ASSESSING THE ROLE OF THE MILITARY IN NATIONAL CYBERSECURITY EFFORTS

A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE
General Studies

by

ANES ZUKIC, CAPTAIN, ARMED FORCES OF BOSNIA AND HERZEGOVINA
BS, Land Forces Military Academy, Ankara, Turkey, 2009

Fort Leavenworth, Kansas
2020

Approved for public release; distribution is unlimited. United States Fair Use determination or copyright permission has been obtained for the use of pictures, maps, graphics, and any other works incorporated into the manuscript. This author may be protected by more restrictions in their home countries, in which case further publication or sale of copyrighted images is not permissible.

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 instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this 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 Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED *(From - To)*
12-06-2020	Master's Thesis	AUG 2019– JUN 2020

4. TITLE AND SUBTITLE

Assessing the Role of the Military in National Cybersecurity Efforts

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Captain Anes Zukic

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The age of expanding globalization created a security environment strongly associated with the information security of the digital world. Cyberspace now is available not only for governments but also to all individuals and all kinds of non-governmental organizations. The cyber domain is creating enormous opportunities for adversaries to conduct actions for their benefits and to harm governments and individuals. Nevertheless, the strategic dynamics of the cyberspace is an opportunity for states to impose their all instruments of national power over their competitors. Fundamentally, societies are becoming more technologically reliant than ever before. The protection of cyber reliant critical information infrastructure is a paramount concern for the whole nation. For any state, integrated and comprehensive approach to security and information management should be based on a whole of government basis. Cybersecurity is becoming a challenge for national security and requires collaboration between governmental and non-governmental entities. A whole of government approach concept will be an act of unity of effort between all stakeholders to maximize a collaborative unity of action to counter cyber threats. The significance of understanding the role of the military in national cybersecurity efforts precisely, capabilities that could be provided throughout the entire process of the national cybersecurity framework, is essential to ensure adequate roles and responsibilities to protect cyberspace. In this thesis, the author discussed the emerging cyber threats, the importance of cybersecurity, and the role of the military within cyber committed countries, and the possibility of national cybersecurity strategy formulation by the military. The objective of this thesis is to determine should Ministry of Defense of BiH leads national cybersecurity efforts.

15. SUBJECT TERMS

Military Role in National Cybersecurity Efforts

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. PHONE NUMBER *(include area code)*
(U)	(U)	(U)	(U)	114	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: Captain Anes Zukic

Thesis Title: Assessing the Role of the Military in National Cybersecurity Efforts

Approved by:

_____, Thesis Committee Chair
Dale C. Eikmeier, MMAS

_____, Member
Randy G. Masten, Ph.D.

_____, Member
Lieutenant Colonel Brandon E. Thrasher, M.S.

Accepted this 12th day of June 2020 by:

_____, Acting Director, Office of Degree Programs
Prisco R. Hernandez, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

ASSESSING THE ROLE OF THE MILITARY IN NATIONAL CYBERSECURITY EFFORTS, by Captain Anes Zukic, 114 pages.

The age of expanding globalization created a security environment strongly associated with the information security of the digital world. The cyber domain is creating enormous opportunities for adversaries to conduct actions for their benefits and to harm governments and individuals. Nevertheless, the strategic dynamics of the cyberspace is an opportunity for states to impose their all instruments of national power over their competitors. Fundamentally, societies are becoming more technologically reliant than ever before. The protection of cyber reliant critical information infrastructure is a paramount concern for the whole nation. For any state, integrated and comprehensive approach to security and information management should be based on a whole of government basis. Cybersecurity is becoming a challenge for national security and requires collaboration between governmental and non-governmental entities. A whole of government approach concept will be an act of unity of effort between all stakeholders to maximize a collaborative unity of action to counter cyber threats. The significance of understanding the role of the military in national cybersecurity efforts precisely, capabilities that could be provided throughout the entire process of national cybersecurity framework is essential to ensure adequate roles and responsibilities to protect cyberspace. In this thesis, the author discussed the emerging cyber threats, the importance of cybersecurity, and the role of the military within cyber committed countries, and the possibility of national cybersecurity strategy formulation by the military. The objective of this research is to determine should Ministry of Defense of BiH leads national cybersecurity efforts.

ACKNOWLEDGMENTS

I want to express sincere gratitude to U.S. Secretary of Defense's International Military Education and Training (IMET) program for enabling the funding of my world-class education in the USA. Likewise, thanks to the Ministry of Defense of Bosnia and Herzegovina for placing its trust and confidence in my abilities to successfully graduate from U.S. Army Command and General Staff College. It was my honor and privilege to be able to serve and represent my country abroad.

Furthermore, I want to thank my Committee Members, Mr. Dale Eikmeier, Dr. Randy Masten, and LTC Brandon Thrasher, for enormous patience, technical support, and tremendous pieces of advice through the process. Thanks for their dedicated part of the time to my thesis. Mainly, I am grateful to Mr. Dale Eikmeier's mentorship, constructive criticism, encouragement, and inspiration for completing my thesis.

I would like to thank my amazing but complicated wife, Imela, for her never-ending mental support, motivation, and understanding. Thanks to my daughter, Najla, for being my source of joy and strength.

In the end, I want to thank all my instructors and classmates from Staff Group 18C, who made my stay at CGSC enjoyable. I would like to hearty thanks to our sponsors from Fort Leavenworth, Leavenworth City, and Kansas City for their support: LTC John Crotzer, Mrs. Shelly Crotzer, Mr. John Bettasso, Mrs. Isabelle Bettasso, Mr.Phil Watlington, Mrs. Nicki Watlington. The time spend in U.S. Army Command and General Staff College was priceless and an experience that made good man better.

Finally, I would like to express warm thanks to the staff of the Graduate Degree Program, Dr. Robert Baumann, Dr. Prisco Hernandez, and Mrs. Ann Chapman.

TABLE OF CONTENTS

PAGE

MASTER OF MILITARY ART AND SCIENCE THESIS APPROVAL PAGE iii

ABSTRACT iv

ACKNOWLEDGMENTS v

TABLE OF CONTENTS vi

ACRONYMS viii

ILLUSTRATIONS x

TABLES xi

CHAPTER 1 INTRODUCTION 1

- Background 1
- The Research Purpose 2
- The Research Question 4
- Assumptions 4
- Definitions 5
- Limitations 9
- Scope and Delimitations 9
- Significance of the Study 10
- Summary 11

CHAPTER 2 LITERATURE REVIEW 12

- Introduction 12
- Background 13
- Defining Cyberspace 16
- Cyberthreats 18
- Understanding Cybersecurity 22
- National Cyber Security Strategies 29
  - National Cyber Security Strategy of the United Kingdom 29
  - National Cyber Strategy of the United States of America 32
  - National Digital Security Strategy of the Republic of France 34
  - National Cybersecurity Strategy of the Republic of Lithuania 36
  - National Cybersecurity Strategy of Estonia 39
- International Strategic Guidance 42
- Bosnia and Herzegovina Cybersecurity Efforts 45

Other Articles Related to the Military's National Cybersecurity Efforts 51
Gaps 52
Summary 53

CHAPTER 3 RESEARCH METHODOLOGY 54

Introduction 54
Conclusion 54
Analysis 55
Summary 59

CHAPTER 4 ANALYSIS 60

Cyber Threats 61
National Cybersecurity 67
Role of the Military in Cyberspace 73
National Cyber Security Strategy 77
Conclusion 80

CHAPTER 5 CONCLUSIONS AND RECOMMENDATIONS 82

Introduction 82
Conclusion 85
Key Findings 89
Recommendations 89
Further Research 91

BIBLIOGRAPHY 92

ACRONYMS

ADM	Army Design Methodology
ATP	Army Techniques Publication
BiH	Bosnia and Herzegovina
CERT	Computer Security Incident Response Team
CERT RS	Computer Security Incident Response Team of the Republic of Srpska
CSIRT	Computer Security Incident Response Team
CoE	Center of Excellence
CSOC	Cyber Security Operations Centre
CGSC	Command and General Staff College
CII	Critical Information Infrastructure
DOD	Department of Defense
DDOS	Distributed Denial-of-Service
DBIR	Data Breach Investigations Report
EU	European Union
ENISA	The European Union Agency for Network and Information Security
EUFOR	European Union Force
FIRST	Forum of Incident Response and Security Team
FNDSS	French National Digital Security Strategy
GCI	Global Cybersecurity Index
GCHQ	Government Communications Headquarters
ITU	International Telecommunication Union
IMET	International Military Education & Training
IT	Information technology

IMOC	Interinstitutional Maritime Operational Center
JP	Joint Publication
LNCSS	Lithuanian National Cybersecurity Strategy
MOD	Ministry of Defense
NATO	North Atlantic Treaty Organization
NCSS	National Cybersecurity Strategy
NICCS	National Initiative for Cybersecurity Careers and Studies
NOCP	National Offensive Cyber Programme
NCS	National Cyber Strategy
OSCE	Organization for Security and Cooperation in Europe
RAFT	Relationship, Actors, Functions, Tensions
RAC BIH	Regulatory Agency for Communications of BiH
SCADA	Supervisory Control and Data Acquisition
TF-CSIRT	Task Force on Computer Security Incident Response Teams
UN	United Nations
U.S.	United States
UK	United Kingdom

ILLUSTRATIONS

PAGE

Figure 1. System Perspective on the Cybersecurity 28

Figure 2. Research Design Concept 56

Figure 3. National Cybersecurity Organization 90

TABLES

PAGE

Table 1. Global Cybersecurity Index for 2018 15

CHAPTER 1

INTRODUCTION

Background

With the expansion of cyberspace in military, political, and economic fields, the need for implementation of defense activities in cyberspace has become a significant part of the defense strategies of many countries. Countries that develop cybersecurity strategies are one step ahead of cyber threats and can maintain an advantage in the new security environment. Cybersecurity is, therefore, critical. With cyber technology becoming a part of daily life, developments, both positive and negative, are changing the security environment. While the concept of information security used to refer only to the protection of printed information, it has become a much broader subject today with the growth of cyberspace and becoming a significant part of daily life. The development of the Internet has opened new doors for individuals who have the opportunity to exploit vulnerabilities, commit cybercrime, and damage the critical information infrastructures of nations.[1] New concepts such as cybersecurity have emerged for the protection of information, and consequently, protective activities have expanded.

Cyberspace security is a new challenge for the state in the national security environment. With the development of cyberspace, cyber-attacks, cybercrime, cyber terrorism, and cyberwar are increasingly threatening peaceful use of cyberspace in areas

[1] International Telecommunications Union, *World Information Society Report 2007* (Geneva, Switzerland: International Telecommunications Union, 2007), 18, accessed 10 August 2019, http://handle.itu.int/11.1002/pub/8020d0d0-acb598bc-en.

whose borders have yet to be clarified. The number of cyber-attacks and cyber-attackers are increasing day by day. These attacks cause significant problems in terms of security of the individuals, institutions, and the country and the reliability of the cyberspace.[2] Providing cybersecurity for the security of nations and protecting critical information infrastructure are the primary challenges in cyber domain. Some states are seeing this field as an opportunity to develop their military capacity. Moreover, some state and non-state actors do not hesitate to use cyber-attacks against the other states or organizations as a method to solve their foreign policy challenges. These processes of cyber conflicts make the national defense in cyberspace, vaguer, and more anarchic than before, forcing the states to abandon traditional security approaches and establish new strategies and security measures.

The Research Purpose

The rapid development of information and the advancement of communication technologies has caused the forming of a new environment called cyberspace. Cyberspace environment consists of interconnections that affect all layers; physical, logical, information, and human.[3] This holistic environment covers not only global or regional, but also national all areas of aspects of political, military, economic, social, information, infrastructure, and physical environment. The emergence of cyberspace

[2] Julian Jang-Jaccard and Surya Nepal, "A Survey of Emerging Threats in Cybersecurity," *Journal of Computer and System Sciences* 80, no. 5 (2014): 80, accessed 10 August 2019, https://doi.org/10.1016/j.jcss.2014.02.005.

[3] David Clark, "Characterizing Cyberspace: Past Present and Future," MIT Computer Science & Artificial Intelligence Lab, 12 March 2010, accessed 13 August 2019, https://projects.csail.mit.edu/ecir/wiki/images/7/77/Clark_Characterizing_cyberspace_1-2r.pdf.

increased the vulnerability of the national security dimensions to attacks from cybercrime, cyber terrorism, and cyberwarfare. The states had to abandon traditional security and establish new strategies and security measures in order to protect critical infrastructure and citizens. This research will address the potential role of the military in ensuring national cybersecurity efforts.

Cyberspace's asymmetrical and multidimensional threats are a higher risk area for the security of states. The conventional national security strategy, with limited borders and primarily controlled by the norms of international law, was not designed for the emerging cyber threat. In this context, the issue of the protection of cyberspace is of specific importance, which involves several intervening and responsible actors that include the numerous departments of the State, public sector, and the citizens. A new security strategy must emerge to replace the conventional security concept with anonymity, where the attack is much simpler than defending, and low cost. According to the securitization approach, it is not limited to military issues and extends to a broader spectrum of threats.[4]

This research aims to increase the overall awareness of the role of the military in national cybersecurity efforts. This paper will try to achieve this by emphasizing the importance of cyber threats in today's world, their effects on critical national infrastructure, and country cyber-defense planning and capabilities. Moreover, this thesis will analyze the military's perspective on operating with intervening and responsible entities in the field of national cybersecurity. Results from the research will be evaluated

[4] Antonia Does, *The Construction of the Maras: Between Politicization and Securitization* Geneva, Switzerland: Graduate Institute Publications, 2013), 17.

and can be the steps for the future development of Bosnia-Herzegovina's military efforts in cyberspace.

The Research Question

The emergence of cyberspace threats prepared the ground for transformations in the perception of security. Cybersecurity is a comprehensive topic that requires analysis in depth. For that reason, the thesis delimits research to understand the military's role in national cybersecurity. The thesis question is concerned with aspects of the role of the military in this domain. The main research question is: Should the Bosnia-Herzegovina Department of Defense lead National Cybersecurity efforts?

Supporting questions are directed to bring clarity to the overall importance of cybersecurity for the protection of national security. Supporting questions are: What are the threats that destabilize national security in the cyberspace environment? What national security components need to be established in order to ensure cybersecurity? What is the role of the military and national departments in the protection of national cyberspace? Is the Department of Defense the best choice to develop a national cybersecurity strategy?

Assumptions

The research assumes that the states delegate cybersecurity efforts primarily to its military. Despite the limited concentration of the qualitative research on the military's role in cybersecurity, the qualitative review will ensure sufficient expressive data for academically satisfactory conclusions in order to enable further research.

Definitions

The definitions section covers the terminology that the researcher uses through this research and the thesis. Terminology is in line with the U.S. definitions to preserve clarity and prevent misunderstanding as the research progresses through the role of the military within national cybersecurity.

Cyberspace. Currently, cyberspace is defined as a global domain within the information environment that consists "of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[5]

Cyberspace attack. The actions are taken in cyberspace that creates noticeable denial effects, such as degradation, disruption, or destruction, in cyberspace or manipulation that leads to denial that appears in a physical domain and is considered a form of fires.[6]

Critical Infrastructure. National critical infrastructures include those assets, systems, and functions vital to national security, economic need, or national public health and safety that rely on computers and networks for their operations.[7] Their breakdown or

---

[5] Joint Chiefs of Staff**,** Joint Publication (JP) 3-12, *Cyberspace Operations* (Washington, DC: Office of the Secretary of Defense, 2018), GL-4.

[6] Ibid.

[7] U.S. General Accounting Office, *Technology Assessment: Cybersecurity for Critical Infrastructure Protection*, GAO-04-321 (Washington DC: U.S. General Accounting Office, 28 May 2004), 3, accessed 13 August 2019, https://www.gao.gov/assets/160/157541.pdf.

annihilation would have a devastating effect on national security, economic security, national public health, or safety.[8]

Cyberspace defense. Set of actions to defeat specific threats that have breached or are threatening to breach the cyberspace security measures, and include actions such as to detect, characterize, counter, and mitigate threats.[9]

Cyberspace security. Set of actions to prevent unauthorized access to exploitation, or damage to computers, electronic communications systems, and other information technology, in order to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.[10]

Defensive cyberspace operations. Missions to protect data, networks, cyberspace-enabled devices, and other systems by defeating on-going or following malicious cyberspace activity.[11]

Offensive cyberspace operations. The set of offensive missions to project power within cyberspace.[12]

---

[8] Cybersecurity and Infrastructure Security Agency, "Critical Infrastructure Sectors," 5 March 2013, accessed 13 August 2019, https://www.cisa.gov/critical-infrastructure-sectors.

[9] Joint Chiefs of Staff**,** JP 3-12, II-16.

[10] Ibid., GL-4.

[11] Ibid.

[12] Ibid., GL-5.

Cyber threat. An activity intended to jeopardize the security of an information system and the information it contains by modifying the availability, integrity, or confidentiality.[13]

Cyber threat actors. Cyber threat actors usually are state, groups, or individuals who, with malicious purpose, aim to take advantage of cybersecurity vulnerabilities, in order to gain unauthorized access to information systems with the end state to access or otherwise affect data, devices, systems, and networks.[14]

Computer Security Incident Response Team (CSIRT). A Computer Security Incident Response Team is an organizational unit or a capability that provides services and support for preventing, detecting, handling, and responding to computer security incidents.[15]

National Cyber Security Strategy. A national cybersecurity strategy is a strategic framework for a nation's approach to cybersecurity in order to intensify the security and resiliency of critical national infrastructures in cyberspace environment.[16]

---

[13] Canadian Centre for Cyber Security, *An Introduction to the Cyber Threat Environment* (Gloucester, ON: Communications Security Establishment Canada, 2018), 2, accessed 16 August 2019, https://cyber.gc.ca/sites/default/files/publications/Intro-to-cyber-threat-environment-e.pdf.

[14] Canadian Centre for Cyber Security, An Introduction to the Cyber Threat Environment, 2.

[15] Forum of Incident Response and Security Teams, "3 The Difference Between a CSIRT and a PSIRT," in "FIRST CSIRT Services Framework," 2019, accessed 16 August 2019, https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1#3-The-Difference-Between-a-CSIRT-and-a-PSIRT.

[16] European Union Agency for Cybersecurity, "National Cybersecurity Strategies," 2019, accessed 17 August 2019, https://www.enisa.europa.eu/topics/national-cyber-security-strategies.

Cyberwarfare. Cyberwarfare refers to a massively coordinated digital assault on a government by another, or by large groups of citizens, to penetrate another nation's computers or networks to cause damage or disruption.[17]

Cyber Terrorism. A computer-based attack aims to persuade government or societies in order to achieve goals that are political, religious, or ideological.[18]

Cyber espionage. A form of cyber-attack aims to steal classified, sensitive data or intellectual property to gain an advantage over a competitive government or nongovernmental entity.[19]

Hacktivism: An infiltration and disruption of a network or website by computer hacking in order to achieve political goals.[20]

Cyber power: the capability to use cyberspace in order to generate advantages and to influence specific occasions in all the operational environments and across the instruments of national power.[21]

---

[17] *USLegal, Cyber Warfare Law and Legal Definition,* n.d., accessed 17 August 2019, https://definitions.uslegal.com/c/cyber-warfare/.

[18] Centre of Excellence Defence Against Terrorism, North Atlantic Treaty Organization, and Public Diplomacy Division, *Responses to Cyber Terrorism* (Washington, DC: IOS Press, 2008), 70.

[19] Martin Libicki, "The Coming of Cyber Espionage Norms" (paper presented at the 9th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 2017), 13, accessed 18 August 2019, https://ieeexplore.ieee.org/document/8240325.

[20] Hossein Bidgoli, *Global Perspectives in Information Security Legal, Social, and International Issues* (Hoboken, NJ: Wiley, 2009), 305.

[21] Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Larry K. Wentz, Stewart H. Starr, and Franklin D. Kramer (Washington, DC: Potomac Books Inc., 2009), 3.

Limitations

The time available for the research is the primary constraint. Scientific researches and government documents regarding cybersecurity that contain the most accurate data might not be publicly available. This fact limits the research on the significant role of the military in the government's cybersecurity efforts. The researcher limits his research to unclassified publicly available major, relevant, cyber defense strategies, and documents by relevant academic, and governmental authorities. The research will not encompass the responsibilities of governmental actors for ensuring cybersecurity for national protection in depth. The research will not cope with the technical issues of cybersecurity.

Scope and Delimitations

Under the limitations section, it was stated that research would not be focused in-depth related to technical military responsibilities in the cyberspace domain. However, it will encompass national cybersecurity strategies and documents of NATO, EU, and ITU member countries. From researching the mentioned countries, the researcher will try to deliver results related to the military's place in national strategies and protecting the critical infrastructure connected with cyberspace. Gained results will try to be incorporated in the recommendation for the future development of the Bosnia-Herzegovina Ministry of Defense's national cybersecurity efforts.

The primary delimitation of this research is that it will only focus on the strategic point of view, not a cyber-expert point of view. The research is restricted to publicly available official reports, strategies, and documents by agencies and governments, case studies, scientific and academic journal articles, and news reports on cyber threats, cyber-

attacks, and the following responses. The research will cover the period only up to 31 December 2019.

Significance of the Study

The emergence of technology emphasized the importance of the cyberspace domain. As a result, the need to defend population, resources, infrastructure, and even borders against cyber-attacks from other states or non-state actors was born.[22] Cybersecurity issues are arising due to three factors: deliberately acting adversaries in cyberspace, a large number of societal functions rely on IT, and the current vulnerabilities of IT systems are an advantage for the adversary.[23] Recognizing the role of the military in establishing cybersecurity for national cyber defense would offer a significant understanding of military cyber capabilities that might offer ways to mitigate dependency on the private sector, or to develop new capabilities in the cyber domain. This research is vital to military organizations that are part of national cybersecurity efforts.

Furthermore, the research will investigate how the BiH MOD acts in the context of national cybersecurity. It is essential to understand this context in order to provide quality knowledge that contributes to ongoing efforts in the cyber domain by enhancing synergy between government entities at the national level. The research discloses the

---

[22] Paul Meyer, "Outer Space and Cyberspace," In *International Cyber Norms: Legal, Policy and Industry Perspectives*, ed. Anna-Maria Osula and Henry Roigas (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2016), 157.

[23] David Clark, Thomas A. Berson, and Herbert S. Lin, *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues* (Washington, DC: National Academies Press, 2014), 9.

importance of the military for defending national cyberspace not only as traditional means of defending but also as leading efforts in establishing the nation's cybersecurity.

Summary

Chapter 1 provided an overview of the problem, the purpose, and significance of the research, as well as assumptions, definitions of terms, scope and limitations, and delimitations that the reader must consider. This study explores the military's role as a nation's component in cybersecurity efforts throughout exemplified cyber strategies and documents. The chapter assesses the meaning of the military in cybersecurity. The first chapter provides insight into the problem and the research question, ensuring the pathway to chapters two and three that further intricate accessible literature and qualitative research process.

CHAPTER 2

LITERATURE REVIEW

Introduction

The purpose of this chapter is to summarize and briefly review the existing literature used in support of the thesis, and in answering the primary and secondary research questions. The focus of the research is on the importance of the military in cybersecurity efforts at the national level. To research the military's role in national cybersecurity activities, a deliberate literature review is required. The literature review aims to recap available literature and sources of information that are relevant to the research questions. The research question is: Should the Bosnia-Herzegovina Ministry of Defense lead National Cybersecurity efforts? Supporting research questions are: What are the threats that destabilize national security in the cyberspace environment? What national security components need to be established in order to ensure cybersecurity? What is the role of the military and national departments in the protection of national cyberspace? Is the Department of Defense the best choice to develop a national cybersecurity strategy?

Moreover, in this chapter, the author discusses literature about cyberspace, cybersecurity, cyber-attacks, national and international cybersecurity strategies, cybersecurity events. The research for this study consisted of three primary sources: government publications and strategic guidance, relevant cybersecurity reports, and articles in the cyberspace domain.

In correlation with the provided background in the second chapter of this thesis, information derived from academic sources will be categorized. The first section of this

chapter consists of cyberspace; second section is cybersecurity; the third section is about cyber-attacks; the fourth section consists of national cyber strategies, the fifth section is international cybersecurity guidance; the sixth section contains documents relevant to the current situation for cybersecurity of Bosnia and Herzegovina, and the last section contains information gained from articles and other electronic sources.

Following supporting research questions, the author provides a short overview of each part based on facts derived from various literature researches. To accurately comprehend the complexity of the research, it is vital to be acquainted with aspects of the cyberspace security environment, cybersecurity, cyberthreats, and military power within the national cyberspace environment. This chapter shows the overview of available literature in open sources, government strategic guidance and publications, reports, articles, and publications of different international institutions. Consequently, the literature review will assist the readers in smooth comprehension about the military's role in national cybersecurity.

Background

It is imperative to emphasize the narrowing of literature review following institutions such as NATO, EU, and ITU. The reason for this delimitation is that European and Euro-Atlantic integration is the future of Bosnia and Herzegovina. Therefore, this background is necessary to understand the author's reason for choosing specific organizations and countries. NATO and the EU have always remained synonymous with the security, development, and stability of all its members and

partners.[24] Because "only a democratic, functional, and sovereign Bosnia-Herzegovina can provide lasting regional stability."[25]

Consequently, this thesis will deal with the functional domain of the military in Bosnia and Herzegovina's cyberspace. EU accession and NATO membership will offer benefits for Bosnia-Herzegovina, EU for Bosnia-Herzegovina socio-economically, and NATO membership for collective security.[26] The Department of Defense of Bosnia and Herzegovina needs to be capable of ensuring the country's security against threats of a national, regional, and international scale and, at the same time, defend the economic and societal assets of the state. This capability means alignment with EU directions and interoperability with NATO. Department of Defense of BiH is one of the institutions that support the commitment of BiH toward Euro -Atlantic integration.

Therefore, in order to use relevant sources for the research topic and to understand cybersecurity efforts of some specific countries that are members of ITU, EU, and NATO, the author used score rate of most cybersecurity committed countries in accordance with International Telecommunication Union (ITU)'s Global Cybersecurity

---

[24] Jabuka, "Brkić: Članstvo u EU i NATO savezu štiti naše posebnosti [Brkić: Membership in the EU and NATO protects our specialties]," 12 August 2019, accessed 11 September 2019, https://www.jabuka.tv/brkic-clanstvo-u-eu-i-nato-savezu-stiti-nase-posebnosti/.

[25] Jasmin Mujanovic, "Jasmin Mujanovic for EWB: Four Theses on Bosnia-Herzegovina's Euro-Atlantic Future," European Western Balkans, 2015, accessed 11 September 2019, https://Europeanwesternbalkans.com/2015/03/16/jasmin-mujanovic-for-ewb-four-theses-on-bosnia-herzegovinas-euro-atlantic-future/.

[26] James O. Thorley, "Is Euro-Atlantic Integration of Bosnia-Herzegovina Good for the EU, NATO and Bosnia-Herzegovina Itself?" (Joint Command and Staff Course of Studies, Canadian Forces College, North York, ON, 2015), 27, accessed 11 September 2019, https://www.cfc.forces.gc.ca/259/290/317/305/thorley.pdf.

Index (GCI) in 2018. GCI is an initiative of the ITU and is a reference that measures the commitment of countries to cybersecurity at a global level.[27]

Table 1 presents the countries from ITU's Global Cybersecurity Index for 2018. Pluses (+) show membership is presented the particular organization, and minuses (-) show there is no membership. This index is important because it shows the commitment of countries to cybersecurity at a global level.

Table 1. Global Cybersecurity Index for 2018

Country	Global Rank	GCI Score	Membership in		
			NATO	EU	ITU
United Kingdom	1	0.931	+	+*	+
United States of America	2	0.926	+	-	+
France	3	0.918	+	+	+
Lithuania	4	0.908	+	+	+
Estonia	5	0.905	+	+	+
Bosnia and Herzegovina	118	0.204	–	–	+

Source: Created by author with information International Telecommunication Union, *Global Cybersecurity Index 2018* (Geneva, Switzerland: International Telecommunication Union, 2018), 16, accessed on 16 September 2019, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf; North Atlantic Treaty Organization, "NATO Member Countries," 16 September 2019, accessed on 16 September 2019 https://www.nato.int/cps/en/natolive/nato_countries.htm; European Union, "Countries," 31 January 2020, accessed 31 January 2020, https://europa.eu/european-union/about-eu/countries_en#tab-0-0; International Telecommunication Union, "List of Member States," 16 September 2019, accessed on 16 September 2019, https://www.itu.int/online/mm/scripts/gensel8.

[27] International Telecommunication Union, "Global Cybersecurity Index," 2019, accessed 15 September 2019, https://www.itu.int/en/ITU-D/Cybersecurity/PAGEs/global-cybersecurity-index.aspx.

There is an evident gap between most committed countries in cybersecurity and BiH. To understand implemented solutions for national cybersecurity literature review of government guidance and strategic will be based on five most committed countries with the GCI's highest score.

Defining Cyberspace

The author, during the research period, found out numerous definitions of cyberspace. However, the author identified the most common and relevant definitions of cyberspace in order to help the reader to understand cyberspace better.

The book Cyberpower and National Security, by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, summarizes related subjects of Cyberspace and Cyberpower and their influence on National Security. This book defines the crucial questions related to building the human capacity to confront cyber challenges, national security concerns, and establishing international partnerships to address cyber issues. Also, analyze cyberwar from economic, technical, political, military, and legal perspectives.

Specifically, in the aforementioned book, Kuehl provides a comprehensive definition of cyberspace: "The cyberspace is a global domain within the information environment whom the distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies."[28]

[28] Kuehl, "From Cyberspace to Cyberpower, 28.

However, another essential definition of cyberspace is asserted by Martin Libicki in his book, *Cyber Deterrence and Cyberwar*. In his book, he deeply explores cyberspace, cybersecurity, cyberattacks, cyber deterrence, and the actions required to protect national cyberspace. Libicki stated that "cyberspace can be defined as an agglomeration of individual computing devices that are connected through a network to each other and the outside world."[29] He also emphasized that cyberspace is a virtual environment that uses information infrastructure, and is independent of land, air, sea, even space.[30]

On the other hand, a more restrictive definition of cyberspace is given by U.S. DoD Joint Publication (JP). DoD's JP 3-12 defines cyberspace as a "domain information environment that consists of the interdependent network of information technology infrastructures and resident data. This domain includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[31]

Taking the above mentioned definitions into consideration, it can be observed that cyberspace is a virtual environment without borders that has anarchical and unconventional characteristics. Cyberspace includes physical elements and virtual domain operations that can produce physical affection.[32] Understanding the cyber

---

[29] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009), 6.

[30] Ibid., 12.

[31] Joint Chiefs of Staff, JP 3-12, GL-4.

[32] Erik Gartzke, Jon Lindsay, and Michael Nacht, "Cross-Domain Deterrence: Strategy in an Era of Complexity" (paper presented at the International Studies Association Annual Meeting, Toronto, Canada, 2014), 98.

environment provides necessary awareness in visualizing the overall situation of structures, objects, and relationships of cyberspace.

Cyberthreats

The European Union Agency for Network and Information Security published its *Threat Landscape Report 2018*, which provides an overview of the most common cyber threats and their trends. This report contains an extensive collection, analysis, and assessment activity of cyber threats in the public domain and covers the period from December 2017 to December 2018.[33] Report advocate nation-states to include cybersecurity into their risk management functions and identify clear strategies to anticipate and respond to crises that can be caused by cyber threats.[34]

J. Rittinghouse and B. Hancock in the *Cybersecurity Operations Handbook* provide extensive guidance on all aspects of operational security of cyberspace, information asset safeguarding, the technical process issues, the operational management issues, and the legal issues.[35] From the perspective of cyber-attacks, authors emphasize proper cybersecurity preparation, which is a determination to have unaffected information systems from cyber threats.[36]

---

[33] European Union Agency for Network and Information Security, *Threat Landscape Report 2018: 15 Top Cyberthreats and Trends* (Athens, Greece: European Union Agency for Network and Information Security, January 2019), 7, accessed 26 September 2019, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018.

[34] Ibid., 124.

[35] John W. Rittinghouse and Bill Hancock, *Cybersecurity Operations Handbook* (Amsterdam, Netherlands: Elsevier Digital Press, 2003), 34.

[36] Ibid., 629.

The study conducted by U.S. the National Intelligence Council, *The Global Trends 2025*, examines "globalization, demography, the rise of new powers, the decay of international institutions, climate change, and geopolitics of energy to generate strategic thinking for future decisionmakers."[37]

This study stressed out that non-military means of warfare, such as cyber, in which adversaries will try to advance their agenda and gain popular support for their cause, will become more prominent in conflicts over the next two decades.[38]

Furthermore, in the report, *Emerging Challenge: Security and Safety in Cyberspace*, authors state that new development and applications of information technology will enable new possibilities for state and non-state actors to commit hostile actions for financial gain, to advance their cause, to disrupt competition, for espionage or gaining economic advantage.[39]

Dr. Steven Bucci, in his report "The Confluence of Cyber Crime and Terrorism," provides functional cyber threat spectrum which presents a group of threats from low to

---

[37] National Intelligence Council, *Global Trends 2025: A Transformed World* (Washington, DC: U.S. Government Printing Office, November 2008), 4, accessed 26 September 2019, https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/2025_Global_Trends_Final_Report.pdf.

[38] Ibid., 91.

[39] Richard O. Hundley and Robert H. Anderson, "Emerging Challenge: Security and Safety in Cyberspace," in *In Athenas Camp: Preparing for Conflict in the Information Age*, ed. John Arquilla and David Ronfeldt (Santa Monica, CA: Rand, 1997), 232, accessed 26 September 2019, https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR880/MR880.ch10.pdf.

high level.[40] Each group has its motivations and the ability to inflict a certain amount of damage. At the low level of the spectrum, individual hackers, small criminal enterprises, may inflict limited damage to individuals, and they are not observed as a significant threat.[41] Medium level threats consist of terrorist use of the internet, cyber espionage, and organized crime.[42] These threats may cause harmful effects on a person, a business, a government, or a region. The threats in a high level of spectrum involve the full power of nation-states and may cause highly significant damage to the state.[43]

The thesis, "Active Cyber Defense: Enhancing National Cyber Defense," examines how active defenses have contributed to traditional warfare, and how some of the concepts can be applied to cyber defense.[44] Author Tiong Wong points out that cyber-attacks have become more sophisticated, pervasive, and exceptionally difficult to trace due to the increasing usage of computers across many sectors such as government, military, industry, and financial sector.[45]

The monograph "Cyber-Attacks, Attribution, and Deterrence: Three Case Studies," by Detlefsen William, assessed the role of a defender's ability to attribute a

---

[40] Steven P. Bucci, "The Confluence of Cyber Crime and Terrorism," Heritage Foundation, 2009, 2, accessed 26 September 2019, https://www.heritage.org/defense/report/the-confluence-cyber-crime-and-terrorism.

[41] Bucci, "The Confluence of Cyber Crime and Terrorism," 2.

[42] Ibid.

[43] Ibid.

[44] Tiong P. Wong, "Active Cyber Defense: Enhancing National Cyber Defense" (Master's thesis, Naval Postgraduate School, Monterey CA, 2011) 1, accessed 26 September 2019, https://calhoun.nps.edu/handle/10945/10713.

[45] Ibid., 7.

cyber-attack and its effect on deterrence.[46] The author expressed that sometimes less powerful states fear to respond to state-originated cyber-attacks because it may cause an escalation of the conflict out of the cyberspace.[47] Also, the author summarized that attribution, the ability to identify attacks, and the appropriate response from responsible governmental entities is critical to defending against and responding to cyber-attacks.[48]

Authors in the book *Cyber War: The Next Threat to National Security and What to Do About* analyze the technical shortcomings of the web, political analysis on the high necessity of cyber defense, and discusses ways of improving the national security situation regarding cyberspace. The authors also give background on previous cyber-attacks such as DDOS attacks on Syria and Estonia. From a cyber-attacks point of view, they emphasized that cyber-attacks have the potential to impact the world's military balance and radically change political and economic relations between nation-states.[49] They also explain three reasons for the possibilities of cyber-attacks: the fault in the design of the Internet, faults in hardware and software, and the online access to critical

[46] William R. Detlefsen, "Cyber Attacks, Attribution, and Deterrence: Three Case Studies" (Monograph, School of Advanced Military Studies, U.S. Army Command and General Staff College, Fort Leavenworth, KS, 2015), 4, accessed 26 September 2019, https://apps.dtic.mil/dtic/tr/fulltext/u2/1001276.pdf.

[47] Detlefsen, "Cyber Attacks, Attribution, and Deterrence, 38.

[48] Ibid., 45.

[49] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins Publishers, 2012), 32.

information infrastructure.[50] The authors point out that a distributed denial-of-service attack is one of the most deliberately cruel methods of cyberwar.[51]

According to gained information from reviewed literature on cyber-attacks thesis summarized that cyber-attacks had threatened the nation's social welfare, national security, and economic stability, and it started to be used as means of persuasion or punishment in foreign policy by states or non-states actors.

Understanding Cybersecurity

Once cyberspace is understood, it is imperative not only to describe threats within but also to establish a foundation for protection from those threats.

Most of the nations are increasingly dependent on the safe and secure cyberspace domain in which new threats are continuously emerging.[52] This dependency is an opportunity for adversaries to target individuals or states and exploit the vulnerabilities of those. Consequently, of these reasons, they are resulting in a focus on cybersecurity. Emerging cyber threats are capable of producing strategic consequences, and the nation-state is required to manage, assess, and protect national cyberspace methodically.[53]

---

[50] Ibid., 39.

[51] Ibid., 56.

[52] Donald J. Trump, *National Cyber Strategy of the United States of America* (Washington, DC: White House, September 2018), 1, accessed 26 September 2019, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

[53] Kenneth Geers, *Strategic Cyber Security* (Tallinn, Estonia: CCD COE Publications, 2011, 15, accessed 26 September 2019, https://ccdcoe.org/uploads/2018/10/2011_Proceedings_0-1.pdf.

It is essential to have persistent resilience for the protection of cyberspace. In the comprehensively researched article, "A Cyber-Security Framework for Development, Defense and Innovation at NATO," represents the significance of cybersecurity as a policy. M. P. Efthymiopoulos states that cybersecurity, as a part of the cross-disciplinary and trans-disciplinary approach, is a strategical-operational framework that is suitable to all levels of socio-political, economic, information technologies, legal, and security-led levels.[54]

Overview of Cybersecurity, published by the International Telecommunication Union (ITU), provides a classification of various cybersecurity threats, an explanation of cyber protection, discussion on risk management, and the importance of education in network protection. In this document, ITU defines cybersecurity as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect and secure the cyber environment."[55]

The European Union Agency for Network and Information Security (ENISA) in the document *Definition of Cybersecurity-Gaps and Overlaps in Standardization*, that aims stakeholders and policymakers, provides an extensive description of proper

---

[54] Marios Panagiotis Efthymiopoulos, "A Cyber-Security Framework for Development, Defense and Innovation at NATO." *Journal of Innovation and Entrepreneurship* 8, no. 1 (2019): 2, accessed 26 September 2019, https://innovation-entrepreneurship.springeropen.com/track/pdf/10.1186/s13731-019-0105-z.

[55] International Telecommunication Union, *Overview of cybersecurity*, ITU-T X.1205 (Geneva, Switzerland: International Telecommunication Union, 2008), 8, accessed 20 October 2019, https://www.itu.int/rec/dologin_pub.asp?lang=s&id=T-REC-X.1205-200804-I!!PDF-E&type=items.

understanding of the term cybersecurity. The document stresses out that cybersecurity shall refer to the security of cyberspace incorporating the principles of confidentiality, integrity, and availability for the reason of relationships and objects within cyberspace; protection of privacy for legal entities; and to address resilience and recovery from cyber-attacks.[56]

The United Kingdom's *National Cyber Security Strategy 2016 to 2021* point out cybersecurity as the protection of internet-connected systems (hardware, software, and related infrastructure), the information stored on them, and the services those systems provide, from unauthorized access, harm or misuse.[57]

On the official website of the U.S. Cybersecurity and Infrastructure Security Agency, the National Initiative for Cybersecurity Careers and Studies (NICCS) Portal's cybersecurity lexicon provides a common understanding of cybersecurity terms for cybersecurity communities both the public and private areas. This portal defines cybersecurity as action, ability or capability, by which information and communications

[56] Charles Brookson, Scott Cadzow, Ralph Eckmaier, Jörg Eschweiler, Berthold Gerber, Alessandro Guarino, Kai Rannenberg, Jon Shamah, and Sławomir Gorniak, *Definition of Cybersecurity-Gaps and Overlaps in Standardisation* (Heraklion, Greece: European Union Agency for Network and Information Security, December 2015), 30, accessed 20 October 2019, https://www.enisa.europa.eu/publications/definition-of-cybersecurity/at_download/fullReport.

[57] United Kingdom Cabinet Office, *National Cyber Security Strategy 2016 to 2021*, London, UK: Her Majesty's Government, 2016), 75, accessed 21 October 2019 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

systems, and the information contained inside is protected and defended against damage, unauthorized use, modification, and exploitation.[58]

In the article *Cybersecurity and Critical Infrastructure Protection*, Lewis James provides a simple yet effective definition of cybersecurity. He states that cybersecurity involves the protection of computer networks and the information they hold within cyber penetration, malicious damage, and disruption.[59]

The resolution, *Creation of a Global Culture of Cybersecurity*, adopted by the UN General Assembly, created a road map for establishing the knowledge and experience for a global culture of cybersecurity that citizens and decision-making mechanisms should acquire.[60] In order to create a global culture of cybersecurity, it requires that all participants address the nine complementary elements.

First, awareness of the need for security of information systems and networks need to be addressed.[61] Second, responsibility for the security of information systems and networks following their roles and responsibilities should be defined.[62] Third,

---

[58] National Initiative for Cybersecurity Careers and Studies, "A Glossary of Common Cybersecurity Terminology." 2019, accessed 21 October 2019, https://niccs.us-cert.gov/about-niccs/glossary#C.

[59] James A. Lewis, "Cybersecurity and critical infrastructure protection." Center for Strategic and International Studies, 2006, accessed 25 October 2019, https://www.csis.org/analysis/cybersecurity-and-critical-infrastructure-protection.

[60] United Nations General Assembly, Resolution 239, *Creation of a Global Culture of Cybersecurity*, A/RES/57/239 (New York: United Nations, 2003), 1, accessed 25 October 2019, https://digitallibrary.un.org/record/482184/files/A_RES_57_239-EN.pdf.

[61] Ibid., 2.

[62] Ibid.

participants should react in a timely and cooperative way to prevent, detect and respond to cybersecurity incidents.[63] Fourth, due to the pervasiveness of information systems and networks in modern societies, participants need to respect the legitimate interests.[64] Fifth, security should be implemented in a way that is consistent with the principles recognized by democratic societies.[65] Sixth, all participants should conduct periodical risk assessments that identify threats and vulnerabilities.[66] Seventh, security should represent an essential element in the planning and design, operation, and use of information systems and networks.[67] Eighth, a comprehensive approach to security management based on risk assessment should be developed.[68] Lastly, participants should examine and evaluate the security of information systems and networks and apply appropriate changes.[69]

Based on definition from the European Union Agency for Network and Information Security (ENISA); cybersecurity, supported with pillars of integrity, confidentiality, availability, privacy, and, resiliency allude to the security of cyberspace, where cyberspace concern to links and relationships between objects that are accessible through a generalized telecommunications network, objects themselves present interfaces

[63] Ibid.

[64] Ibid., 3.

[65] United Nations General Assembly, Resolution 239, 3.

[66] Ibid.

[67] Ibid.

[68] Ibid.

[69] Ibid.

allowing their remote control, remote access to data, or their participation in control actions within that cyberspace.[70]

Inherent understanding of the various systems that encompass the environment is essential to comprehensively be able to visualize system perspective to gain a foundation on what is going on and why.[71] Gaining a system perspective on a complex environment will provide an understanding of interrelated connections and systems.[72]

In order to understand the definition provided by ENISA author based on literature analysis provides a system perspective on cybersecurity using RAFT (Relationships, Actors, Functions, and Tensions) method. The environment is consisting of different systems named actors or objects.[73] Relationship refers to links between systems' actors or objects.[74] Also, every relationship has a purpose or function.[75] Tensions are characteristics of relationships such as supportive, critical, or vulnerable.[76]

In figure 2, actors/objects are defined as people, assets, software, critical information infrastructure (CII), networks, and data. The relationship of those actors/objects is based on access through a telecommunication network, and interconnected lines represent it. Each relationship between actors has a specific purpose,

---

[70] Brookson et al., *Definition of Cybersecurity*, 30.

[71] Dale C. Eikmeier, *From Operational Art to Operational Plans: A Joint Planning Primer*, 9th ed. (Fort Leavenworth, KS: U.S. Army Command and General Staff College, 2012), 17.

[72] Ibid., 18.

[73] Ibid., 17.

[74] Ibid.

[75] Ibid.

[76] Ibid.

such as remote control, intuitive interfaces. The specific purpose of each relationship represents tensions between each actor/object; each of them is supportive to each other, critical for the functioning of the overall system, and vulnerable to cyber threats.

This systematic environment is protected with foundational pillars that are the archetype of relationships between each actor in cyberspace. The comprehensive protection of cyberspace is defined as cybersecurity.

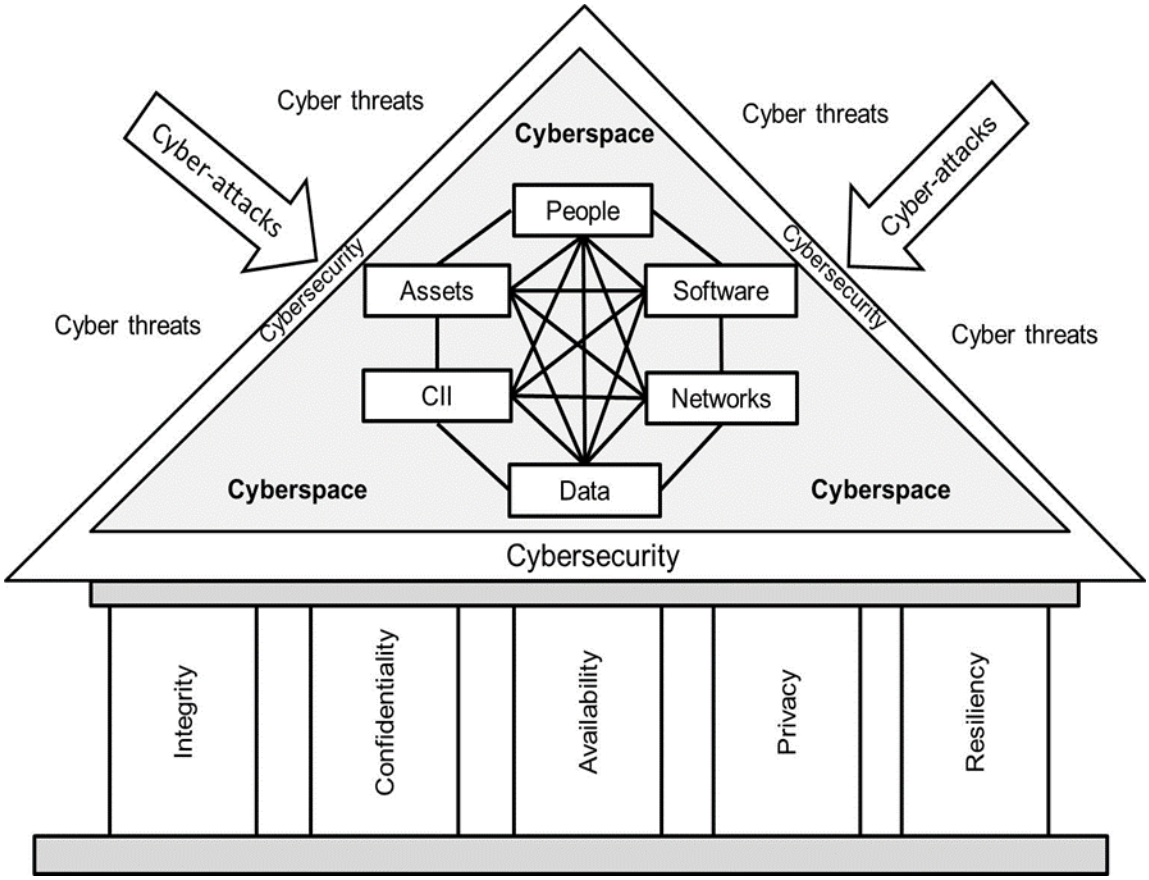

Figure 1. System Perspective on the Cybersecurity

Source: Created by author.

A review of relevant sources points out that cyberspace and information and communications networks have become necessary for society. Ensuring their protection, and resilience are of vital importance Damage to one of these concepts can lead to large-scale economic damage and national security issues. Emerging cyber threats force states to be prepared to protect their society and their economies and to ensure adequate cybersecurity.

National Cyber Security Strategies

National Cyber Security Strategy of the United Kingdom

The United Kingdom's *National Cyber Security Strategy 2016 to 2021* reiterates out the plan to make UK's cyberspace secure and resilient. This strategy aims to reshape the UK's governmental policy by including the public and private sector, civil society, academia, and the wider population.[77] The strategy sets off recommended actions directed to all areas of the economy and society, from departments in government, up to leaders covering industry and the individual citizen.

UK's *National Cyber Security Strategy 2016 to 2021* consists of five sections[78]: 1) assessment of the strategic context that includes current and evolving cyber threats; 2) review of vulnerabilities; 3) UK's government cybersecurity vision in 2021 and key goals in order to achieve the vision, encompassing principles, roles and responsibilities, and government intervention; 4) implementation plan for policy in practice; and 5) assessment of the progress of objectives.

---

[77] United Kingdom Cabinet Office, *National Cyber Security Strategy 2016 to 2021*, 12.

[78] Ibid., 13.

A most crucial aspect of this strategy is the vision of the UK's government and objectives that will enable the achievement of the vision. This strategy sets out a vision to make the UK safe, secure, and resilient against cyber threats in cyberspace environment.[79] Achievement of this vision will be conducted through five main objectives of the strategy.

Defending the UK's Cyberspace: Objective DEFEND of this strategy aims to safeguard resilient UK's networks, information, and systems to cyber-attacks through steps: active cyber defense, secure internet, protected government, and critical national infrastructure, enhancing public behavior, and managing cyber incidents.[80]

Deterring Adversaries: The second objective emphasizes that the UK will use the full spectrum of its capabilities in order to deter and deny adversaries' opportunities through reducing cybercrime, countering hostile foreign actors, preventing terrorism, enhancing sovereign capabilities in offensive cyber and cryptography.[81]

Developing Cyber Capabilities. The third objective DEVELOP stands for acquiring and strengthening the tools and capabilities that the UK requires for the protection of national cyberspace. This objective will be accomplished through strengthening cybersecurity skills, enhancing the development of expertise in cybersecurity, encourage cybersecurity science and technology, and effective horizon scanning.[82]

---

[79] United Kingdom Cabinet Office, *National Cyber Security Strategy 2016 to 2021*, 23.

[80] Ibid., 32.

[81] Ibid., 46.

[82] Ibid., 54.

Justifying Strong International Action. The fourth objective points out the UK's aim to ensure free, open, peaceful, and secure cyberspace by continuing to be a leader in internet governance, opposing data localization, and developing partners' cybersecurity capacities.

Assessing the Progress of the Strategy. The final objective provides the importance of an exhaustive and inclusive set of metrics that will measure the progress of strategy in order to allow annual strategy review to ensure the precise accomplishment of the UK's national goals.[83]

National Cyber Security Strategy 2016-2021stressess out several points related to the military:

In order to improve its intelligence collection and exploitation about adversaries, the Ministry of Defense, will coordinate with international partner agencies and expand its efforts to identify, anticipate, and disrupt hostile cyber activities.[84]

The government will invest in the Ministry of Defense to develop the cybersecurity capabilities in order to be able to respond and disrupt the cyber activities of the adversary.[85]

[83] United Kingdom Cabinet Office, *National Cyber Security Strategy 2016 to 2021*, 66.

[84] Ibid., 28.

[85] Ibid., 35.

The government will increase cyber threat awareness, detection, and reaction capabilities of a Cyber Security Operations Centre (CSOC) that is responsible for protecting MOD's cyberspace.[86]

The government will invest in the National Offensive Cyber Programme (NOCP), which is run by GCHQ and the Ministry of Defense.[87] The government will develop Defense Cyber Academy as a center of excellence for cyber training and exercise across the Ministry of Defense and broader Government.[88]

The government will develop the ability of the Armed Forces to be able to conduct offensive cyber capabilities and maintain the cryptographic capability of the Armed Forces.[89] Armed Forces have to be resilient, have strong cyber defenses, and capable of assisting in national cyber-attack.[90]

National Cyber Strategy of the
United States of America

The *US National Cyber Strategy* (NCS) illustrates the President's goal to establish safe and secure national cyberspace for the interest of the USA and its citizens. The NCS emphasizes cyberspace as a crucial component of America's social, financial,

[86] Ibid., 38.

[87] United Kingdom Cabinet Office, *National Cyber Security Strategy 2016 to 2021*, 51.

[88] Ibid., 56.

[89] Ibid., 51.

[90] Ibid., 10.

institutional, and political aspects.[91] National cybersecurity strategy identifies a full spectrum of actions that are focused on improving the USA's cybersecurity posture.

Mainly, the strategy is structured within four pillars that include several priority actions. The first pillar is to defend the USA by managing cybersecurity to protect networks, systems, functions, and information.[92] This pillar focuses on three essential topics in this domain: securing federal networks and information, securing critical infrastructure, and combating cybercrime and improving incident reporting.

The second pillar is to promote American prosperity by technological ecosystem and developing cyberspace as an engine for the efficient economy and strong domestic innovation.[93] The second pillar focuses on three main topics: 1) fostering a vibrant and resilient digital economy; 2) fostering and protecting united states ingenuity; and 3) developing a superior cybersecurity workforce.

The third pillar is to preserve peace and strength of the United States by identifying, countering, disrupting, degrading, and deterring adversaries in cyberspace.[94] The third pillar describes two main actions: Enhance cyber stability through norms of responsible state behavior, and attribute and deter unacceptable behavior in cyberspace.

The last pillar is to expand the USA's influence abroad in order to preserve open, interoperable, reliable, and secure Internet to strengthen USA interests.[95] The final pillar

---

[91] Trump, *National Cyber Strategy*, 12.

[92] Trump, *National Cyber Strategy*, 15.

[93] Ibid., 23.

[94] Ibid., 29.

[95] Ibid., 33.

identifies two main actions: promote an open, interoperable, reliable, and secure internet, and build international cyber capacity.

National Digital Security Strategy
of the Republic of France

The *French National Digital Security Strategy* (FNDSS) emphasizes the importance of the digital transition of French society, emerging cyber threats that threaten national cyberspace, and extensive strategic objectives to ensure safe national cyberspace.[96] FNDSS stresses out that ensuring France's secure cyberspace will be achieved through five strategic objectives:

Defense of core national interests, the security of national infrastructure, and reaction to cybersecurity crisis.[97] The first objective points out important tasks: possessing scientific, technical, and industrial capabilities, observing security of national information systems, enabling rapid growth of state information systems security, getting ready multilateral cybersecurity organization, and use artificial intelligence for national interests.

Ensuring digital trust, combating cybercrime, and cybermalevolence, and protecting personal data.[98] The second objective identifies several tasks: protecting electronic communication networks, assistance to victims of cybermalevolence, assessing

[96] Manuel Valls, *French National Digital Security Strategy* (Paris, France: National Cybersecurity Agency of France, 2015), 7, accessed 30 October 2019, https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf.

[97] Ibid., 14.

[98] Ibid., 21.

cybercrime, securing privacy and personal information, technical solutions for the public and private sector, and ensuring the Budapest Convention on Cybercrime.

Developing digital security awareness, foundational training, and continuous education.[99] The third objective emphasizes tasks: Raising cyber awareness of French society, incorporating cybersecurity awareness and training on all high education levels, and adaptation of cyber education within businesses.

Developing innovative digital environment and promotion of trusted, secured, capable digital products and services against cyberthreats on an international level.[100] This objective presents tasks: making prominent national and international digital security products and services, cooperation with the private sector, ensuring a safe digital world, public contracting for cybersecurity, exporting French business in the cyber sector.

Advancing in European digital strategic autonomy, and contributing to safe, secure, and free cyberspace.[101] Final objective constitutes of tasks: ensuring plan for European strategic autonomy, strengthening France's international cybersecurity presence, and supporting global cyberspace security.

The French national cyber strategy contains information related to the military: The Ministry of Defense, as one of the competent administrations in the cyber domain, will regularly attend to an Expert Panel for Digital Trust organized by State Secretariat

[99] Valls, *French National Digital Security Strategy*, 26.

[100] Ibid., 31.

[101] Ibid., 38.

for Digital Technology and the National Authority for the Security of Information Systems.[102]

The Ministry of Defense, in cooperation with the National Agency for the Security of Information Systems, will preserve the application of a cyber defense reserve for operational purposes in order to confront major crises in information technology.[103] In 2012 the National Agency for Information Systems Security, in cooperation with the Ministry of Economy, Industry and Digital Technology and the Ministry of Defense, instituted an industrial policy to develop the national fabric of businesses that provide and develop cybersecurity services and products.[104]

In order to have the most secure digital technological products in the world, the competent authorities, such as the Ministry of Defense, should direct its communication efforts concerning the public and private, scientific community, and the innovation centers.[105]

National Cybersecurity Strategy of the Republic of Lithuania

The Programme for the Development of Electronic Information Security (Cyber-Security) for 2011–2019 is the Lithuanian National Cybersecurity Strategy (LNCSS). This strategy aims to regulate the expansion of electronic data through cyberspace with principles of privacy, unity, and obtainability. Also, the strategy points out the protection

---

[102] Ibid., 14.

[103] Valls, *French National Digital Security Strategy*, 17.

[104] Ibid., 31.

[105] Ibid., 33.

of electronic communication networks, information systems, and critical information infrastructure against emerging cyber threats.[106]

In order to accomplish a strategic objective to ensure cybersecurity and security of electronic data in Lithuania, Lithuanian National Cybersecurity Strategy presents three objectives that shall be accomplished:

Safeguarding of information resources that belong to the government.[107] This strategic objective points out important tasks: enhancing monitoring and cooperative efforts of cybersecurity, increasing the quality of regulatory framework for cybersecurity, enlarge and make better security situations for national information infrastructure, advocate the application of cybersecurity projects, and ensure international cooperation in the cybersecurity domain.

Establish an efficient performing of critical information infrastructure.[108] The second strategic objective focuses on the task; functioning of cybersecurity of critical information infrastructure.

Ensuring cybersecurity for Lithuanian cyberspace.[109] The last strategic objective describes main tasks: developing cybersecurity awareness, building up national

---

[106] Lithuanian Information Technology and Communications Department, *The Programme for the Development of Electronic Information Security (Cyber-Security) for 2011–2019*, 1, accessed 30 October 2019, https://www.ird.lt/media/force_download/?url=/uploads/structure/docs/88_3a77a7f83f36364fa7b4a2e38d0c8b76.pdf.

[107] Ibid., 2.

[108] Ibid., 3.

[109] Ibid., 4.

cybersecurity, protecting national cyberspace from cyber threats, strengthen the security of services in cyberspace.

According to this strategy, there are several responsibilities of the Ministry of National Defense of Lithuania, as one of the responsible institutions for implementing cybersecurity program:

MOD of Lithuania should apply national cybersecurity policy.[110] Ministry of Defense of executes cybersecurity projects.[111]

The MOD of Lithuania should participate in cybersecurity events organized by the NATO, EU, and UN and ensure representatives delegated to the NATO Cooperative Cyber Defense Center of Excellence.[112] Also, MOD should cooperate with the CERT services of other states, and conduct identification, analysis and risk assessment of its critical information infrastructure, and to have security requirements for critical infrastructure.[113]

MoD Lithuania should ensure the Cyber Defense Plan for protecting critical information infrastructure and plan for crisis management and preparation of backup infrastructure.[114] Finally, MOD should establish operational and cooperating CERT teams engaged in computer emergency response activities.[115]

---

[110] Lithuanian Information Technology and Communications Department, *The Programme for the Development of Electronic Information Security (Cyber-Security) for 2011–2019*, 7.

[111] Ibid., 10.

[112] Ibid., 11.

[113] Ibid., 12.

[114] Ibid., 13.

[115] Ibid, 15.

National Cybersecurity Strategy
of Estonia

Estonian National Cybersecurity Strategy 2019-2022 is a comprehensive document that lays out long-term vision, goals, priority actions, roles, and responsibilities for the cyber domain, foundation for cybersecurity planning and allocation of resources.[116] This strategy stresses out Estonia's vision in cyberspace to become the most resilient digital society through four essential principles[117]:

The first principle is safeguarding and promotion of rights and freedom in cyberspace. The second principle is empowering socioeconomic growth with rapid digital development and innovative cybersecurity. The third principle is that the basis for the digital ecosystem is the protection of cryptographic solutions. Last principle is digital society will be based on transparency and public trust. Achievement of this vision through this cyber strategy is constructed within four strategic objectives.

Development of maintainable digital society with resilience and readiness.[118] To accomplish the first objective, three ways have been recognized: technological resilience, preparedness for a cyber emergency, inherent leadership, and cohesive community.

[116] Estonian Ministry of Economic Affairs and Communications, *Cyber Security Strategy 2019-2022* (Tallinn, Republic of Estonia: Republic of Estonia, 2019), 7, accessed 31 October 2019, https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf.

[117] Ibid., 10.

[118] Ibid., 40.

Establishing strong and competitive cybersecurity industry, research, and development.[119] This objective will be accomplished through supporting and promoting Estonian cybersecurity research and development and research-based industry.

Becoming a trustworthy and competent international contributor in the cyber domain.[120] The third objective emphasizes two main actions: effective cooperation with strategic international partners, and global promotion of cyber capabilities.

Ensuring talent development and to have a well-educated society about the cyber domain.[121] The last objective is based on two critical actions: empowering cyber awareness through the whole nation, and talent development according to demands.

From the military perspective, the strategy points out some important topics. The main priority of the National Defense Development Plan 2017-2026 is the establishment of real-time cyberspace monitoring, Defense Forces' Cyber Command, and "cyber conscription."[122]

In organizing national cybersecurity organizations, the Ministry of Defense, in collaboration with the Defense Forces, Defense League, and the Foreign Intelligence Service, is responsible for executing activities associated with the military defense part of

[119] Estonian Ministry of Economic Affairs and Communications, *Cyber Security Strategy 2019-2022*, 51.

[120] Ibid., 56.

[121] Ibid., 64.

[122] Ibid., 30.

this strategy, creating cross-sectoral cooperation and coordination mechanisms, and getting uniform reading on the situation.[123]

In order to repel cyber threats and ensure the readiness of government institutions, regular joint cooperative exercises will be organized with the country's political leadership, vital service providers, and structures that ensure military defense. Also, "a uniform situation map of Estonian cyberspace generated in real-time will be developed and shared with all key parties."[124] Estonia will enter into the relevant cyber defense cooperation frameworks with NATO.[125] "Cyber conscription" is a cyber defense educational plan based on talent assessment according to the Küber-Naaskel competition model, which will allow people to complete their military service in the cybersecurity field.[126]

In the old version of the *Estonian Cyber Security Strategy from 2008*, the Ministry of Defense was tasked to develop a Cyber Security Strategy for 2008–2013 in cooperation with the Ministry of Education and Research, Ministry of Justice, Ministry of Economic Affairs and Communications, Ministry of Internal Affairs, and the Ministry of

[123] Estonian Ministry of Economic Affairs and Communications, *Cyber Security Strategy 2019-2022*, 34.

[124] Ibid., 47.

[125] Ibid., 60.

[126] Ibid., 71.

Foreign Affairs.[127] Also, the Ministry of Defense had a leading role in the Cyber Security Strategy Committee.[128]

International Strategic Guidance

As it was stressed in the *Cyber Space Review*, the globally-interconnected digital information and communications infrastructure of cyberspace starts to become the foundation for many sides of modern society.[129] Cyberspace provides critical support to states' economies, civil infrastructure, public safety, and national security.

Being aware of this, the European Union Agency for Network and Information Security in its publication, *Cybersecurity Cooperation: Defending The Digital Frontlines*, stressed the EU Member States should focus their efforts on establishing the effective structure for protection of cyberspace, and be resilient to deal with cyber threats.[130]

---

[127] Ministry of Economic Affairs and Communication, "Cyber Security Strategy Committee, Ministry of Defense, Cyber Security Strategy" (Tallinn Estonia: Republic of Estonia, 2008) 8, accessed 31 October 201, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy.

[128] Ibid., 35.

[129] National Cyberwatch Center, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, DC: United States Executive Office of the President, 2014), 5, accessed 31 October 2019, https://www.nationalcyberwatch.org/ncw-content/uploads/2016/03/Cyberspace_Policy_Review_final-1-1.pdf.

[130] European Union Agency for Network and Information Security, *Cybersecurity Cooperation: Defending the Digital Frontline* (Heraklion, Greece: European Union Agency for Network and Information Security, 2013), 20, accessed 29 October 2019, https://www.enisa.europa.eu/publications/cybersecurity-cooperation-defending-the-digital-frontline/at_download/fullReport.

Nevertheless, the North Atlantic Treaty Organization (NATO) in its Strategic Concept 2010, in which NATO's values and strategic objectives are emphasized, explains the emerging cyber threats can conduct sophisticated cyber-attacks and damage the functioning of government systems, the economy, and critical infrastructure.[131]

The *ITU National Cybersecurity Strategy Guide*, by Dr. Frederick Wamala, explains what composes a national cybersecurity strategy; the standard strategic end states for cybersecurity; how states and stakeholders build cybersecurity capacity, and the factors that influence its implementation of the strategy.[132] The guide describes that countries deal with the national security aspects of cybersecurity strategy in different ways, and cybersecurity strategies usually are the result of the national security strategy.[133] According to guide, some countries named cyber-attacks as a priority, while some prioritized impacts of cyber-attacks on national security, and others developed defense cybersecurity strategy to permit military and intelligence operations.[134]

The guide published by ENISA, *Designing and Implementing National Cyber Security Strategies*, stressed current and emerging cybersecurity threats challenge EU

---

[131] North Atlantic Treaty Organization, *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization* (Lisbon, Portugal: North Atlantic Treaty Organization, 2010), 4, accessed 29 October 2019, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf.

[132] Frederick Wamala, *ITU National Cybersecurity Strategy Guide* (Geneva, Switzerland: International Telecommunication Union, 2012), 5, accessed 30 October 2019, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf.

[133] Ibid., 42.

[134] Ibid., 43.

Member States, forcing them to develop and adapt their cybersecurity strategies continuously.[135] This guide provides useful and practical recommendations to relevant stakeholders on the development, implementation and maintenance of a cybersecurity strategy.[136] It also emphasized that in order to set strategic principles, guidelines, and objectives to mitigate risk related to cybersecurity, national cybersecurity strategies (NCSS) are the main documents of nation-states.[137]

The *National Cyber Security Framework Manual*, published by NATO Cooperative Cyber Defense Centre of Excellence, aims to provide policy-makers with an extensive examination of the relevant factors when managing cybersecurity within national security.[138] It addresses political, strategic, operational, and tactical/technical levels of public policy formulation in order to understand the various features of National Cyber Security.[139] Importantly, it states that NATO nations are making it clear for subjects of NCS and collective cyber defense are interconnected.[140]

---

[135] European Union Agency for Network and Information Security, *NCSS Good Practice Guide: Designing and Implementing National Cyber Security Strategies* (Heraklion, Greece: European Union Agency for Network and Information Security, November 2016), 9, accessed 30 October 2019, https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

[136] Ibid., 11.

[137] Ibid., 5.

[138] Alexander Klimburg, ed., *National Cyber Security Framework Manual* (Tallinn, Republic of Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2012), 17, accessed 30 October 2019, https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf.

[139] Ibid., xv.

[140] Ibid., 183.

The International Telecommunication Union derived the *Global Cybersecurity Index Report* (GCI) to help countries identify sections for improvement in the domain of cybersecurity, and take action to improve their ranking, and raise the overall level of cybersecurity worldwide.[141] The GCI is built on the five pillars of the ITU Global Cybersecurity Agenda: legislative measures, technical mechanisms, organizational structures, capacity-building activities, and cooperative arrangements.[142] To produce the GCI, data collected through an online survey by a group of experts in each nation.[143] According to this report, cybersecurity knowledge should be shared and transferred among various organizations to ensure vital cooperation.[144]

Bosnia and Herzegovina Cybersecurity Efforts

Cyber-attacks are a real and existing threat to BiH and require adequate measures of prevention and cyber protection.[145] Therefore, BiH's institutions must intensify the development of cyber strategy, relevant procedures, techniques, and to provide the necessary human and material resources in the cyber domain.

---

[141] International Telecommunication Union, *Global Cybersecurity Index (CGI) 2018* (Geneva, Switzerland: International Telecommunication Union, 2019), ii, accessed 30 October 2019, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

[142] Ibid., 10.

[143] Ibid., 11.

[144] Ibid., 52.

[145] Safet Music, "Cyber napadi su realna i postojeća prijetnja za BiH [Cyber attacks are real and existing security issue for BiH]," Al Jazeera Balkans, November 2019, accessed 20 November 2019, http://balkans.aljazeera.net/vijesti/cyber-napadi-su-realna-i-postojeca-prijetnja-za-bih.

The document that addresses cybersecurity issues is *Strategy of Bosnia and Herzegovina for Preventing and Combating Terrorism 2015 – 2020*, published in 2015. The strategy identifies the need for protection of critical cyber reliant infrastructure, the establishment of CERT in BiH, and the implementation of international standards in the field of cybersecurity and mechanisms for monitoring and combating the misuse of the Internet for terrorist purposes.[146]

In the *Action Plan for Implementation of the Strategy of BiH for Preventing and Combating Terrorism 2015-2020*, there are several responsibilities and tasks for government entities regarding cybersecurity:

Responsibility for the design and analysis of feasibility studies regarding the better management of cyberspace issues related to terrorism, violent extremism, and hate speech is assigned to the Ministry of Security BiH, the Communications Regulatory Agency of Bosnia and Herzegovina, and entity's Ministries of Internal affairs.

Responsibility for conducting exercises in the domain of possible cyber-attacks is permitted to the Ministry of Security of BiH in cooperation with all relevant institutions in the state.

Responsibility for the development of the analytical report for procurement of IT equipment and obtaining IT equipment for prevention of cyber-attacks on IT infrastructure and misuse of the internet is granted to the Ministry of Security BiH, State

[146] Ministry of Security of Bosnia and Herzegovina, *Strategy of BiH for preventing and Combating Terrorism 2015-2020* (Sarajevo, Bosnia and Herzegovina: Republic of Bosnia and Herzegovina, 2015), 7, accessed 24 November 2019, http://www.msb.gov.ba/dokumenti/strateski/default.aspx?id=12786&langTag=en-US.

Investigation and Protection Agency, Ministry of International Affairs of FBiH and RS, Ministry of Communications and Transports of BiH, Communications Regulatory Agency of Bosnia and Herzegovina, and CERT RS.[147]

The Council of Ministers of Bosnia and Herzegovina has published the strategy for the establishment of CERT in Bosnia and Herzegovina proposed by the Ministry of Security of Bosnia and Herzegovina in 2011.[148] In this strategy, the Ministry of Security of BiH is acknowledged as the leading agency for the establishment of CERT.

After this mentioned strategy, the Council of Ministers of BiH adopted the Decision on Establishment of Computer Emergency Response in March 2017.[149] This decision defines the Ministry of Security of BiH as a responsible agency for the establishment of CERT.

In June 2015, in accordance with Law on Information Security of the Republic of Srpska, the entity's national computer security incident response team (CERT) was

---

[147] Parliamentary Assembly of Bosnia and Herzegovina, *Akcioni plan za provođenje strategije Bosne i Hercegovine za prevenciju i borbu protiv terorizma (2015 – 2020)* [Action Plan for Implementation of Strategy of BiH for Preventing and Combating Terrorism 2015-2020] (Sarajevo, Bosnia and Herzegovina: Republic of Bosnia and Herzegovina, 2015), 7-9, accessed 24 November 2019, https://www.parlament.ba/act/ActDetails?actId=854.8.

[148] Ministry of Security of Bosnia and Herzegovina, *Strategija Uspostave Cert-A U Bosni I Hercegovini* [Strategy for establishment of CERT in Bosnia and Herzegovina] (Sarajevo, Bosnia and Herzegovina: Republic of Bosnia and Herzegovina, 2011, 11, accessed 25 November 2019, http://www.msb.gov.ba/dokumenti/strateski/default.aspx?id=6248&langTag=bs-BA.

[149] Bosnia and Herzegovina Official Gazette, Decision on Establishment of CERT in BiH, 25/17, (Sarajevo, Bosnia and Herzegovina: Republic of Bosnia and Herzegovina, 2017), 5, accessed 25 November 2019, http://www.sluzbenilist.ba/PAGE/akt/g4E0HNrVpsc.

established.[150] CERT RS is a part of the Ministry for Scientific and Technological Development, Higher Education, and Information Society of the Republic of Srpska. CERT RS has a mission of computer security incident prevention, incident response, and general protection of the cyberspace of the Republic of Srpska.[151]

However, the European Commission Progress Report on Bosnia and Herzegovina 2016 brings two main concerns for BiH's cybersecurity efforts. There is an absence of a strategic approach to address cybercrime and cybersecurity. CERT capacities need to be established at the state level and for the Federation entity, while CERT capacities in the Republika Srpska entity need to be increased.[152]

In line with a commitment to establish better national cybersecurity, in 2019, the Ministry of Communications and Transport of BiH in cooperation with Global Cyber Security Capacity Center (GCSCC), undertook a review of the maturity of cybersecurity capacity in Bosnia and Herzegovina. The objective of the cybersecurity capacity review was to enable BiH to gain an understanding of its cybersecurity capacity to develop the

[150] Official Gazette of Republic of Srpska, *Law on Information Security*, No. 70 of 12 July 2011 (Banja Luka, Republika Srpska: Government of Republika Srpska, 2011), 2, accessed 30 November 2019, http://www.podaci.net/_gBiH/propis/Zakon_o_informacionoj/Z-ibezbj03v1170.html.

[151] Republic of Srpska National CERT RS, "About RFC 2350," accessed 30 November 2019, https://certrs.org/en/rfc-2350/.

[152] European Commission, *Commission Staff Working Document: Bosnia and Herzegovina 2016 Report* (Brussels, Belgium: European Union, 2016), 20, 73, accessed 30 November 2019, https://ec.europaeu/neighbourhood-enlargement/sites/near/files/pdf/key_documents/2016/20161109_report_bosnia_and_herzegovina.pdf.

national cybersecurity strategy and to prioritize investment in cyber capacities strategically.[153]

According to this review, the Ministry of Security is leading in the development of the strategy together with the Organization for Security and Cooperation in Europe.[154] On the other hand, the Ministry of Defense has developed its cyber defense strategy to establish secure cyberspace for the own information systems only. The review stated that the Ministry's strategy would help to improve the overall cybersecurity level within the BiH.[155]

The review emphasized that the national and MoD's cybersecurity strategies will be coherent and compatible. The MoD's strategy focuses on four main areas: prevention of cybersecurity incidents, response to cyber incidents; education and cyber awareness-raising with end-users.[156]

Also, the Ministry of Defense developed an action plan to implement the strategy over the next five years and formed a supervisory committee for implementation of the strategy.[157] The review states that by 2021, the MoD intends to establish a secure cyber-environment for the Ministry's network and information systems. The MoD applies a

---

[153] Eva Nagyfejeo and Sarah L. Puello Alfonso, *Cybersecurity Capacity Review Bosnia and Herzegovina* (Oxford, UK: Global Cyber Security Capacity Centre, March 2019), 13, accessed 30 November 2019, http://mkt.gov.ba/dokumenti/informatizacija/ostali_propisi/default.aspx?id=7650&langTag=bs-BA.

[154] Nagyfejeo and Alfonso, *Cybersecurity Capacity Review Bosnia and Herzegovina*, 7.

[155] Ibid., 8.

[156] Ibid., 29.

[157] Ibid., 30.

series of standards that were approved by the ITU and other international organizations.[158]

The document, *Guidelines for a strategic cybersecurity framework in BiH*, was developed in 2019 in cooperation with Organization for Security and Cooperation in Europe (OSCE) Mission to BiH involving all relevant state- and entity-level institutions. This document aims to ensure a strategic and legal framework and competencies, improve procedures and techniques to protect information and communications systems and end-users in BiH's cyberspace.[159]

It represents a strategic framework for establishing an effective cybersecurity system based on the NIS directive, the ENISA Best Practices Guide, positive practices of EU countries, and countries in the region that have adopted national strategies and have established appropriate cyber-attacks response mechanisms.[160]

In line with the international commitment of BiH to join the EU, it is required to align its national cybersecurity efforts with existing cybersecurity legislation and international strategic guidance. In order to comply with the required NATO membership obligations, the MoD should comply with certain standards and procedures required by NATO.[161] Although national cybersecurity experts argue that BiH's complex state

---

[158] Ibid., 74.

[159] Organization for Security and Cooperation in Europe, *Guidelines For a Strategic Cybersecurity Framework* (Sarajevo, Bosnia and Herzegovina: Organization for Security and Co-operation in Europe, 2019), 4, accessed 30 November 2019, https://www.osce.org/mission-to-bosnia-and-herzegovina/438383?download=true.

[160] Ibid., 7.

[161] Presidency of Bosnia and Herzegovina, *The Foreign Policy Strategy of Bosnia and Herzegovina 2018-2023* (Sarajevo, Bosnia and Herzegovina: Republic of Bosnia and

organization and decentralized and complex traditional security management may lead to unsynchronized and inadequate strategical decisions, which further may develop greater complexity in the cybersecurity efforts.[162]

Other Articles Related to the Military's National Cybersecurity Efforts

In the strategy research project, *Defining the DOD Role in National Cybersecurity*, the author examined the approach to leverage the Department of Defense formations, allocation of resources, developing procedures, and establishing industry partnerships along with all other U.S. government stakeholders to extensively improve the national cybersecurity. He concluded that in order to enhance cybersecurity efforts, DoD requires to develop the capacity of cyber expertise and to be part of long-term government strategic investment in cybersecurity.[163]

The article, "Who Should Lead U.S. Cybersecurity Efforts," provides an assessment of different governmental agencies responsible for security. It also examines options and recommendations for the establishment of cybersecurity director similar to the Director of National Intelligence. Most importantly, author Newmeyer Kevin do not

---

Herzegovina, 2018), 8, accessed 30 November 2019, http://www.predsjednistvobih.ba/vanj/default.aspx?id=9555&langTag=en-US.

[162] Sabina Barakovic and Jasmina Barakovic Husic, "'We Have Problems for Solutions': The State of Cybersecurity in Bosnia and Herzegovina." *Information & Security Journal* 32, no. 2 (2015): 3205-19, accessed 30 November 2019, http://defencemanagement.org/system/files/3205_bih_barakovic.pdf.

[163] Mark R. Schonberg, *Defining the DOD Role in National Cybersecurity* (Carlisle Barracks PA: Center for Strategic Leadership, US Army War College, 2013), 28, accessed 30 November 2019, https://apps.dtic.mil/dtic/tr/fulltext/u2/a590756.pdf.

encourage the option of placing the U.S. Department of Defense in charge of national cybersecurity.[164]

It is primarily due to several disadvantages: the legal restrictions of the Posse Comitatus Act on domestic activity by the military; requires regulatory authority and law enforcement powers; deviation from the department's primary mission; challenges in interagency coordination; placing the military in charge of cybersecurity for civilian systems would not be politically viable.

In the article, "The Role of the U.S. Military in Cyberspace," the author stresses out that besides operating and defending its cyberspace military should be prepared to defend the country as a whole. The author states that, in order to do so, the military should effectively cooperate with a cyber relevant international, governmental, and private sector actor. Even though the fact it may be perceived as militarizing cyberspace, the military has essential roles to play in defending the cyber domain.[165]

Gaps

In the course of the development of this paper, the author discovered numerous areas that remain elusive that would facilitate a deeper understanding of this research question. The largest of these instances is the lack of Bosnia and Herzegovina's national cyber policies addressing that address military's strategic objectives. This is further compounded by a lack of relevant documents that specifically identify the role of the

---

[164] Kevin P. Newmeyer, "Who Should Lead US Cybersecurity Efforts?" *Prism: A Journal of the Center for Complex Operations* 3, no. 2 (2012): 126, accessed 30 November 2019, https://apps.dtic.mil/docs/citations/AD1042583.

[165] Suzanne C. Nielsen, "The Role of the US Military in Cyberspace," *Journal of Information Warfare* 15, no. 2 (2016): 35.

military in ensuring national cybersecurity efforts. As a result, it is challenging to address in greater detail the approaches to the military's efforts in national cyberspace.

Summary

The purpose of the literature review is to organize available literature into orderly sections that will empower meaningful examination in the following chapters. Organizing available sources into orderly sections will help the reader to identify answers to supporting questions and develop a course to the main research question. This chapter consisted of seven sub-sections that covered relevant sources in the cybersecurity domain. The number of evaluated sources provides a basic visualization of research and will be expanded in-depth in chapter 4. The author evaluated research areas, regulatory documents, book sections, journal articles, reports, subject matter experts' opinions, and other available and relevant sources of information. From this literature, the author showed the fundamentals of cybersecurity from the perspective of national security.

CHAPTER 3

RESEARCH METHODOLOGY

Introduction

This chapter encompasses the methods used to answer the primary as well as the secondary research questions. The researcher will use the documentation review as the research design. By researching the documentation review and analysis, the author aims at extracting the information as it is, without the additional interpretation of facts provided. This research method will allow for the detailed background analysis of areas of concern by using generic qualitative inquiry. Only already existing information will be used. This research aims to gain a deeper understanding of the military's role in national cybersecurity activities. The research will be shaped by using the Army Design Methodology from Army Techniques Publication (ATP) 5-0.1. ADM is a methodology for applying critical and creative thinking to understand, visualize, and describe complicated, complex problems, and develop approaches to solve them effectively.[166]

Conclusion

The literature presented as part of this analysis is not without its flaws. This is further hindered by the author's inability to access more detailed documents regarding national cybersecurity. This notwithstanding, it does much to illustrate critical takeaways for the reader by the sheer lack of material in certain areas. It also shows that countries committed to cybersecurity, countering emerging cyber threats, and having safe and

[166] Headquarters, Department of the Army, Army Techniques Publication (ATP) 5-0.1, *Army Design Methodology* (Washington, DC: Government Publishing Directorate, July 2015), I-3.

secure cyberspace, developed national cybersecurity strategies that defined the roles and responsibilities of each governmental entity.

Frankly, the material that can be brought to bear on cyber threats, national cybersecurity elements, and BiH cybersecurity efforts is lengthy and well established. This is mainly due to the author's intent to research and organize literature to answer research questions accurately and effectively. The author has struggled to find additional materials on the role of the military in national cybersecurity.

Analysis

The analysis will be based on the author's research design concept based on the idea that a simple method dutifully applied is better than an overly complicated approach. The ADM will assist commanders and planners by defining four main aspects: current state, future state, problems, and operational approach.

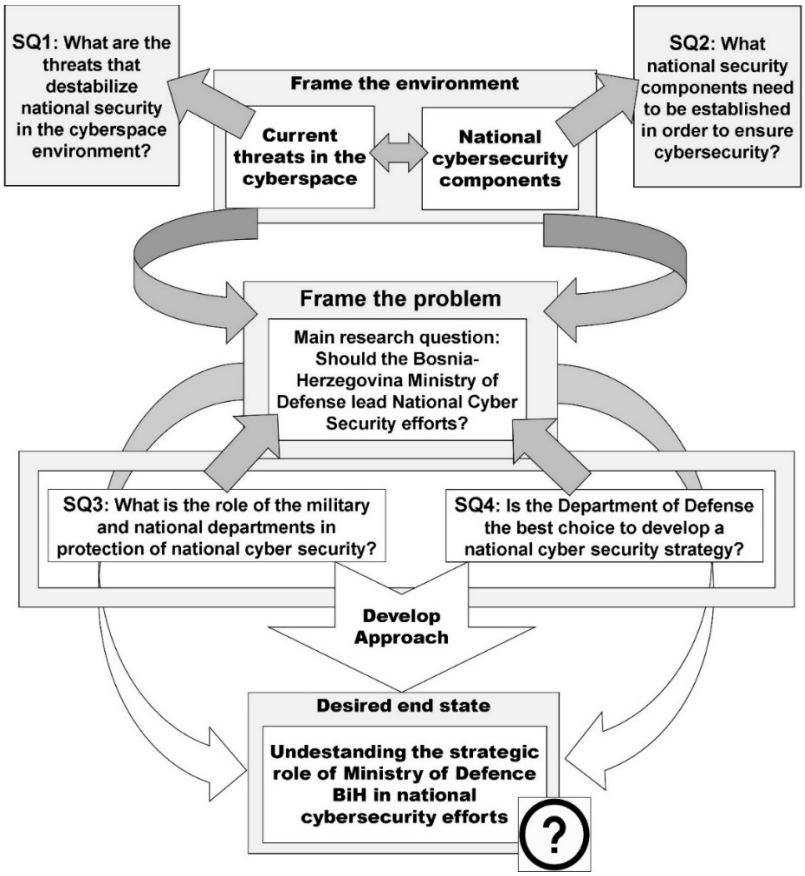

Figure 2. Research Design Concept

Source: Created by author.

In accordance with research questions, the research is organized into five parts overall. First, to develop an understanding of the surrounding environment in cyberspace, the author will frame the environment. Framing the environment will help the author to understand what is going on and why.[167] To ensure data for the first supporting question: "What are the threats that destabilize national security in the cyberspace environment?" the author will collect information regarding current threats in cyberspace.

[167] Headquarters, Department of the Army, ATP 5-0.1, I-4.

Second, after gaining an understanding of threats in cyberspace, the author will analyze national cybersecurity components necessary to protect the national cyber environment. As part of framing the environment, it is required to model the desired end state; secure national cyberspace.[168] With this, the author will provide data for the second supporting question: "What national security components need to be established in order to ensure cybersecurity?" by examining information in the most critical strategic document and organization that the nation-state requires for adequate cybersecurity.

After gaining an initial understanding of a cyberspace environment, and way to protect it adequately, research focuses on efforts to identify and understand the main issue. Identifying and understanding problems are necessary to solve the problem.[169] Related to the main research question: "Should the Bosnia and Herzegovina Ministry of Defense lead National Cyber Security efforts?" the author will frame the problem following background and the purpose of this thesis. In order to provide sufficient data for analysis, this section will be expanded by two additional sections that contain an analysis of the third and fourth supporting questions.

Data for supporting question three: "What is the role of the military and national departments in the protection of national cybersecurity?" will be provided within the analysis of data regarding roles of relevant national agencies in the protection of national cyberspace related to national cybersecurity strategies.

---

[168] Headquarters, Department of the Army, ATP 5-0.1, I-4.

[169] Ibid.

Supporting question four: "Is the Department of Defense best choice to develop a national cybersecurity strategy?" will be clarified by gaining sufficient data on the abilities of relevant states' entities to lead and formulate national strategies.

Finally, through the sections, as mentioned earlier, sufficient and correlative data will be gained, thus allowing analysis for the main research question. It is necessary to answer support questions in order to be able to define those national cybersecurity efforts. In correlation with this main research, the question will be answered in chapter 5. The author stresses that before presenting the main research question, it should be considered the topic will always be a constant debate with various implications from changeable national politics and cyber environment, which requires continuous improvement to assure resiliency.

Understanding the environment and related problem, the author considered an operational approach consists of the broad general actions and means for clarification and achieving the desired end state.[170]

The final stage of this research methodology is concluded and summarized the research in chapter 5. Chapter 5 contains a developed approach to the problem. It provides the answer to the main research question based on the results of the findings and analysis of the thesis. The answer to the main research question will be formulated according to presented national cybersecurity efforts. For each effort, the author will use suitability criteria from strategy evaluation analysis. Suitability is a criterion for evaluating the extent to which a proposed option fits the situation identified in the

[170] Headquarters, Department of the Army, ATP 5-0.1, I-4.

analysis.[171] That is important in order to gain a clear understanding of the organization and its capability to lead each effort. This section also develops proposals, recommendations, and guidance, which may help and optimize probable future solutions for achieving the Ministry of Defense of Bosnia and Herzegovina's strategic cybersecurity objectives in the future.

Summary

The suggested research methodology allows for review and analysis of a variety of material related to the topic sources. The primary objective of the proposed method is to organize a phased study of the questions addressed. The analysis will cover cyberspace, cyber threats, national cybersecurity strategies, international cybersecurity guidance, and relevant research articles. Consequently, the researcher will conduct the general qualitative inquiry to identify standard features of various countries and organizations concerning military efforts within national cybersecurity activities. Finally, the proposed structure leads to an answer to the research questions and will provide recommendations according to analysis. This methodology is feasible, suitable, and will appropriately achieve its research objectives.

[171] Gerry Johnson, Kevan Scholes, and Richard Whittington, *Exploring Corporate Strategy* (London, UK: Prentice Hall, 2006), 365.

CHAPTER 4

ANALYSIS

This chapter addresses the four secondary research questions by discussing cyber threats to the state, required measures, and the role of the military in supporting the state's cybersecurity. It examines the national cybersecurity elements as the basis for national security in cyberspace and how the military encompasses its lines of effort in this domain. Chapter 4 addresses these topics in four primary sections, followed by the chapter summary.

The first section analyzes cyber threats. This section addresses the first secondary question: what are the threats that destabilize national security in the cyberspace environment. It identifies critical threats to the whole nation. It also focuses on their nature and what targets, types of attack, and their purpose. Lastly, this section notes the implications of cyber-attacks on national security.

The second section describes the cybersecurity components. It addresses the second supporting research question: what national security components need to be established in order to ensure national cybersecurity. It contains cyberspace's impact on national security and the need for cybersecurity. It also provides national cybersecurity efforts that are used to answer the main research question.

In the third section, the roles of the military in national cybersecurity were analyzed. It also addresses leading national leading roles as securing or defending, and potential drawbacks.

The fourth section concludes on viability whether the Ministry of Defense should be the best choice to develop a national cybersecurity strategy or not.

Lastly, the summary reviews responses to the four secondary research questions. It encapsulates the military's role in the national cybersecurity protection. This lays the foundation to conclude the research, and it forms the basis for tentative conclusions and the study's response to the primary research question in chapter 5.

Cyber Threats

In evolving expanding cyberspace, governments and organizations are trying to increase their influence in this domain by improving their technological possibilities and capabilities. States that have become more dependent on technology and the internet, the foundation of cyberspace, can be exposed to cyber-attacks. Cyber-attacks target critical infrastructure sectors such as transportation, electricity, education, health, nuclear facilities, agriculture, industry, energy, water, finance, and communications, which are vital for countries. For that reason, countries started to strengthen their national cybersecurity.

Cyber threats and their severity of impact national security are growing by the day.[172] A cyber or cybersecurity threat is a malicious action that aims to damage data, steal data, or disrupt digital life.[173] Malicious action acts as an illegal attempt to harm the computer system or the information on it; using the internet is defined as cyber-attack.[174]

---

[172] National Security Agency, "Understanding the Threat," 2019, accessed 25 December 2019, https://www.nsa.gov/what-we-do/understanding-the-threat/.

[173] Prey Project, "What Are Cyber Threats and What to Do About Them," accessed 25 December 2019, https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/.

[174] *Cambridge Dictionary*, s.v. "Cyberattack," accessed 25 December 2019, https://dictionary.cambridge.org/us/dictionary/english/cyberattack.

Their implications are very high. Cyber-attacks are a severe national security threat that can cause as much harm as a conventional military attack.[175] Many times the cyberspace attacks aim to unauthorized access the system, steal information, breakdown the system, destroy information, and block a system.[176]

On the other hand, they may cause damage to the state's critical infrastructure from miles away, and similar to a missile strike.[177] Cyber threats pose an extensive risk to public health, safety, and prosperity as information technologies are integrated into critical infrastructure and vital national networks.[178] Some reports of cyber-attacks illustrate that the attacks on cyber-reliant critical infrastructures could have a devitalizing effect on national and economic security.[179]

---

[175] Kenneth Mok, "Cyber Threat or Cyber Threat Inflation? – Assessing the Risk to U,S, National Security," *Small Wars Journal* (2019), accessed 25 December 2019, https://smallwarsjournal.com/jrnl/art/cyber-threat-or-cyber-threat-inflation-assessing-the-risk-to-us-national-security.

[176] Rittinghouse and Hancock, Cybersecurity Operations Handbook, 623.

[177] James Lovegrove, "The Implications of Cyber-Attacks on Governments," Diplomatic Courier, 2016, accessed 25 November 2019, https://www.diplomaticourier.com/posts/implications-cyber-attacks-governments.

[178] Daniel R. Coats, *The National Intelligence Strategy of the United States of America* (Washington, DC: U.S. Office of the Director of the National Intelligence, 2019), 13, accessed 29 December 2019, https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf.

[179] Gregory C. Wilshusen, *Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure*, Testimony Before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives (Washington, DC: U.S. Government Accountability Office, July 2011), 11, https://www.gao.gov/assets/130/126702.pdf.

According to the Center for Strategic and International Studies, most attacks targeted government and defense agencies, as well as companies. There have been many cyber-attacks targeting cyber reliant critical infrastructure, including the following:

August 2019. Networks at several Bahraini government agencies and critical infrastructure providers were infiltrated by hackers linked to Iran.[180]

July 2019. State-sponsored Chinese hackers conducted a spear-phishing campaign against employees of three major U.S. utility companies.[181]

April 2018. Cybersecurity researches reveal that North Korean hackers targeted critical infrastructure in seventeen countries using malware.[182]

The landscape report assembled by the European Union Agency for Network and Information Security (ENISA) covers the top fifteen most common types of cyber-attacks in 2018 that have interchangeably been affecting nations.[183] These include malware, web-based attacks, web application, distributed denial of service (DDOS), botnets, phishing, spam, ransomware, insider threats, physical manipulation, exploit kits, data breaches, identity theft, information leakage, and cyber espionage.

---

[180] Center for Strategic and International Studies, *Significant Cyber Incidents List*, 2019, accessed 28 November 2019, 6, https://csis-prod.s3.amazonaws.com/s3fs-public/200504_Cyber_Attacks.pdf?0M9lsdHhOXhw.BahGk5hYXgDtEWrs6x9.

[181] Ibid., 7.

[182] Ibid., 17.

[183] European Union Agency for Network and Information Security, *UNISA Threat Landscape Report 2018: 15 Top Cyberthreats and Trend*, Heraklion, Greece: European Union Agency for Network and Information Security January 2019, 7, accessed 30 November 2019, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018.

The four major categories of cyber threats to national security, whether they are associated with state or non-state factors, are cyberwar, economic espionage, cybercrime, and cyber-terrorism.[184]

The Verizon Data Breach Investigations Report (DBIR) found that of the most common cyber-attacks in 2018, 52 percent were caused by external hacking, and 33 percent by social engineering.[185] Cyber-attacks are not only targeting critical information systems, but also the person operating the computer. As a human factor, the lack of awareness or negligence regarding cybersecurity is emerging as one of the prominent causes of security incidents leading to the dramatic consequence for organization and government.[186]

There are two types of cyber-attacks: targeted and untargeted. Targeted cyber-attack is a dedicated attack with the purpose to inflict damage on a specific user, organization, or company.[187] It aims to gain access to critical data covertly and cause more damage. The intent of such an attack is for financial gain, industrial espionage,

---

[184] Joseph S. Nye, Jr., "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly* 5, no. 4 (Winter 2011): 21.

[185] Verizon, "2019 Data Breach Investigations Report," 2019, 2, accessed 30 December 2019, https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf.

[186] Janine Kremling and Amanda M. Sharp Parker, *Cyberspace, Cybersecurity, and Cybercrime* (Thousand Oaks, CA: SAGE Publications, 2017), 184.

[187] Aditya K. Sood, Richard J. Enbody, and Peter Loshin, *Targeted Cyber Attacks: Multi-Staged Attacks Driven by Exploits and Malware* (Waltham, MA: Syngress, 2014), 3.

stealing intellectual property, disrupting the system's process, political influence, and attack a nation's critical infrastructure.[188]

Untargeted cyber-attack is an attack that does not attack a specific designated target. It aims to generate a high amount of losses by affecting multiple computers.[189]

JP 3-12 Cyberspace Operations emphasizes the biggest challenges of the cyber threat is anonymity (connecting particular cyber-persona to action), and its borderless nature.[190] However, sometimes they might be well-coordinated with multi phases.[191]

Usually, a cyber-attack delivers malicious computer code. In order to be successful in its attack, adversary exploits a vulnerability in the system, gain access, and then deliver a payload to penetrate the system.[192]

For example, in November 2008 malware attack was conducted on the U.S. Department of Defense computer systems. The attacks targeted military computer systems and infected the U.S. Central Command. Due to this attack, the use of external computer flash drives on military computers was banned in U.S. Armed Forces.[193]

---

[188] Sood, Enbody, and Loshin, *Targeted Cyber Attacks: Multi-Staged Attacks Driven by Exploits and Malware*, 2.

[189] Luis Ayala, *Cybersecurity Lexicon*, vol. 158 (Berkeley, CA: Apress, 2016), 43.

[190] Joint Chiefs of Staff**,** JP 3-12, I-12.

[191] Curtis St. Michel and Sarah Freeman, "Consequence-Based Resilient Architectures," in *Industrial Control Systems Security and Resiliency: Advances in Information Security*, ed. Craig G. Rieger Indrajit Ray, Quanyan Zhu, and Michael A Haney, vol. 75 (Cham, Switzerland: Springer, 2019), 17.

[192] Susan Davis, *NATO in the Cyber Age: Strengthening Security and Defense, Stabilizing Deterrence*, Brussels, Belgium: NATO Parliamentary Assembly, 2019, 3.

[193] Julian E, Barnes, "Pentagon computer networks attacked," *Los Angeles Times*, 2008, accessed 27 December 2019, https://www.latimes.com/archives/la-xpm-2008-nov-28-na-cyberattack28-story.html.

Also, in December 2015, three utility companies in Ukraine were hit by malicious cyber-attack that began with phishing and targeted SCADA systems. In the same year, the Israel National Electricity Authority suffered damage from cyber-attack. Those two significant attacks caused a power outage for several hours in both countries.[194]

However, they may cause worse consequences, such as an example of an autistic 17-year-old college student, from the UK, hanged himself after receiving a ransomware scam.[195]

Some essential characteristics of cyber-attacks were identified during analysis. It is challenging to recognize the attacks. Most cases were recognized too late. It is complicated to identify and track the actor that carried out the attack. Cyber-attacks are low cost for the attacker. Politically motivated cyber-attacks are a national security issue. Espionage activities that otherwise involved high costs and risks become much easier when using cyber-attacks.

Answering supporting research question: what are the threats that destabilize national security in the cyberspace environment? According to analysis, threats that destabilize national security in cyberspace are those that implicit on the nation's critical information infrastructure's computer control systems. They are mostly caused

---

[194] Stuart Collins, "Cyber-Attacks: Critical Infrastructure," Global Risk Dialogue, *Allianz Global Corporate and Specialty* 1 (Summer/Fall 2016): 15, 14-29, accessed 27 December 2019, https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/grd/AGCS-GRD-1-2016-EN.pdf.

[195] John Leyden, "Panicked teen hanged himself after receiving ransomware scam email," The Register, 2015, accessed 29 November 2019, https://www.theregister.co.uk/2015/01/23/autistic_teen_joseph_edwards_ransomware_scam_suicide_tragedy/.

intentionally with the purpose of physical damage, economic losses, and psychological trauma.

Their impediments to national security are characterized as paralyzing the state's decision-making system; causing massive public panic; the collapse of critical national infrastructure.[196] Considering the devastating characteristic of cyber threats toward national security would require a severe approach involving all stakeholders of the state to commit efforts in ensuring safe and secure cyberspace.

National Cybersecurity

With the technological developments in recent years, geographical restrictions have disappeared, and electronic services have become the center of our lives. The business world, community life, public services, national security infrastructures of nations depend on the operation of information technologies, and critical infrastructures. In today's world, where cyber threats become widespread, the integrity and confidentiality of information flowing on critical infrastructures become essential. Since society becomes more dependent on information technologies, it makes the protection and usability of these critical infrastructures a national interest. Thus, cybersecurity is regarded as a horizontal and strategic national issue affecting all levels of society.

---

[196] Athina Karatzogianni, *Cyber Conflict and Global Politics* (London, UK: Routledge, 2010), 84; Maria Bada, "The Social and Psychological Impact of Cyberattacks," in *Emerging Cyber Threats and Cognitive Vulnerabilities*, ed. Vladlena Benson and John McAlaney (San Diego, CA: Elsevier, 2019); Ryan Zatolokin and Joe Morgan, "Cybersecurity for Critical Infrastructure," *Security Magazine*, June 2019, accessed 29 December 2019, https://www.securitymagazine.com/articles/90268-cybersecurity-for-critical-infrastructure.

The National Cybersecurity should be provided at a national level and updated in coordination in line with the demands coming from the public and private sector, taking into consideration the developing technology, changing conditions, and requirements.

To ensure reasonable information security, infrastructural protection, and cyberspace security for a nation require coordinated and comprehensive approaches that incorporate public-private sector efforts.[197] Ensuring the openness of the Internet and fundamental values is the main challenge of cybersecurity policymaking today.[198]

Increasing cyber threats that states face drives their national security efforts to make cybersecurity priority effort. This priority employs specific techniques and procedures in order to be ensured. Thus, mitigating all risks in cyberspace, a government should ensure all stakeholders be part of a systemic approach to national security. Cybersecurity needs shared responsibilities among different stakeholders; and facilitation of collaboration.[199] Because of the cyberspace connection to critical infrastructure, all

---

[197] Barack Obama, The Comprehensive National Cybersecurity Initiative (Washington, DC: White House, 2010), 5, accessed 29 December 2019, https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative.

[198] Organization for Economic Co-operation and Development, *Security Policy Making a Turning Point: Analyzing a New Generation of National Cybersecurity Strategies for the Internet Economy* (Paris, France: Organization for Economic Co-operation and Development, 2012), 12, accessed 29 December 2019, http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf.

[199] Mariarosaria Taddeo, "Is Cybersecurity a Public Good?" *Minds and Machines* 29 (October 2019): 351, accessed 30 December 2019, https://link.springer.com/content/pdf/10.1007/s11023-019-09507-5.pdf.

strategic means of a country must be adaptable and flexible in confronting the issues in the cyber environment effectively.[200]

In accordance with the analysis and effective strategic means for cybersecurity is a National Cyber Security Strategy (NCSS). It is a strategic tool that establishes a range of national objectives and priorities in order to improve the security and resilience of national infrastructures and services.[201] NCSS provides a strategic framework for a nation's approach to cybersecurity integrated with the nation's national interest. Joint Publication (JP) 3-0, Joint Operations, defines strategy as "an idea or set of ideas of the ways to employ the instruments of national power in a synchronized and integrated fashion to achieve national, multinational, and theater objectives."[202]

An example of a successful approach in developing resilient national cybersecurity is an Estonia. In 2007 Estonia was a victim of politically-motivated cyber-attack, with that Estonia looked for the best course of action and sough international support to mitigate cyber threats.[203] Consequently, in 2008 the Estonian Ministry of

---

[200] Quigg, Michael, Juan Lopez, Mason Rice, Michael Grimaila, and Benjamin Ramsey, "Cyberspace and Organizational Structure: An Analysis of the Critical Infrastructure Environment," in *Critical Infrastructure Protection X: 10th IFIP WG 11.10 International Conference, ICCIP 2016, Arlington, VA, USA, March 14-16, 2016, Revised Selected Papers*, ed. Mason Rice and Sujeet Shenoi, (Cham, Switzerland: Springer, 2016), 22.

[201] European Network and Information Security Agency, *National Cyber Security Strategies: Setting the course for national efforts to strengthen security in cyberspace* (Brussels, Belgium: European Network and Information Security Agency, 2012), 4.

[202] Joint Chiefs of Staff, Joint Publication (JP) 3-0, *Joint Operations* (Washington, DC: Office of the Secretary of Defense, January 17, 2017), GL-15.

[203] Emilio Iasiello, "Cyber attack: A dull tool to shape foreign policy" (paper presented at the 5th International Conference on Cyber Conflict (CYCON), Tallinn,

Defense published National Cyber Security Strategy addressing implementing measures in reducing cyber threats vulnerability in the nation as a whole.[204] Estonia successfully changed its security perspective and aligned national efforts to develop an effective national cyber strategy for a comprehensive approach to protecting the state's critical infrastructure.

International Telecommunication Union defines critical infrastructure as "the key systems, services, and functions whose disruption or destruction would have a weakening impact on public health and safety, commerce, and national security."[205] ITU emphasized that CI consists of the state's interests. Usually, critical infrastructure includes domain as health, water, transport, communications, government, energy, food, finance, and emergency services sectors. Most of the state's critical infrastructures rely on cyberspace and the information and communication technologies that enable it. So, cyberspace and the information and communication technologies together are critical information infrastructure (CII). The CII operates and controls the critical sectors and their physical assets.[206] CII is considered as the entities and infrastructures that process, store, and exchange information required to provide the services that are crucial to a nation's

---

Estonia, 2013), 5, accessed 29 December 2019, https://ieeexplore.ieee.org/document/6568392.

[204] Ministry of Economic Affairs and Communications, *Cyber Security Strategy*, 3.

[205] Frederick Wamala, *The ITU National Cybersecurity Strategy Guide* (Geneva, Switzerland: International Telecommunication Union, 2012), 25, accessed 30 November 2019, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf.

[206] Ibid.

existence.[207] CII is controlled by SCADA (Supervisory Control and Data Acquisition). SCADA is a computer control system that is used to monitor and control plant processes.

Therefore, for a state, cyberspace is a strategic domain, thus securing it is a strategic objective. Cybersecurity is a strategic domain because the complexity and interconnectedness of CII across critical sectors make it hard to predict the outcome of a cyber-attack.

This strategic importance of cyberspace was recognized by over seventy countries that adopted their national cybersecurity strategies as the preferred and most effective mechanism for reducing risks and responding to cyber threats related to the ICT infrastructure.[208] Justifying the need for cyber strategy might be summarized as threat mitigation, risk reduction, preventive measures, effective response, and building capacity. Motives behind the development of the National Cyber Security Strategy according to fifty-four countries are reducing cyber threats, economic security, requirements by other policy instruments, strengthening national resiliency, political imperatives, lawful mandates, protecting state secrets, strengthening diplomacy, and increasing the country's image.[209]

---

[207] Bernhards Blumbergs, *Technical Analysis of Advanced Threat Tactics Targeting Critical Information Infrastructure*, Cyber Security Review (NATO Cooperative Cyber Defence Centre, 2014), 1, accessed 29 December 2019, https://ccdcoe.org/uploads/2018/10/2014-Technical-Analysis-of-Advanced-Threat-Tactics-Targeting-Critical-Information-Infrastructure.pdf.

[208] Cristin Flynn Goodwin and J. Paul Nicholas, *Developing a National Strategy for Cybersecurity: Foundations for Security, Growth, and Innovation* (Redmond, WA: Microsoft Corporation, 2013), 3.

[209] Azmi, Riza, William Tibben, and Khin Than Win, "Motives behind Cyber Security Strategy Development: A Literature Review of National Cyber Security

Answering the second supporting research question: What national security components need to be established in order to ensure cybersecurity? In accordance with the analysis, national cybersecurity requires two main components: NCSS strategy and strategic cybersecurity framework. National Cyber Security Strategy that has elements of ends, ways, and means. "Whereas ends are the objectives or goals sought. Means are the resources available to follow the objectives. Ways are methods that describe how one organizes and applies the resources."[210] Every meaningful national cyber strategy, NCSS has a foundation on its national interests; to reduce the cyber threat, ensure the state's welfare, and improve resiliency, and at the same time relevant international guidance. Based on strategic objectives from NCSS, the cybersecurity framework provides guidelines for action plans. This strategic framework ensures the implementation of strategic objectives from NCSS. The process represented in the framework is a national cybersecurity effort for secure cyberspace.

OSCE Mission to BiH, following BiH's realistic needs and international commitments in the area of cybersecurity, developed Strategic Cybersecurity Framework for Bosnia and Herzegovina. This document contains strategic objectives and activities that will lead national efforts to a productive and enforceable strategic cybersecurity

---

Strategy" (paper presented at Australasian Conference on Information Systems, Wollongong, Australia, 5-7 December 2016), 5.

[210] Robert H. Dorff, "A Primer in Strategy Development," in *U.S. Army War College Guide to Strategy*, ed. Joseph R. Cerami and James F. Holcomb (Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, 2001), 11.

management and secure cyberspace.[211] Strategic objectives represented in this framework will be used for answering the main research question.

The strategic objectives of strategic cyber security framework in Bosnia and Herzegovina includes:

A. The harmonization and development of cybersecurity legislation;
B. Secured Information and Communication Systems;
C. Raising the Awareness and Knowledge of Cybersecurity;
D. Functional entities for Securing, Strengthening and Improving Cyber Security;
E. Enhancing Security and Resilience of Information and Communication Systems;
F. Enhanced Capacity to Combat Cybercrime;
G. Effective Cyber Security Co-operation established in International, Regional and National Frameworks;
H. Capacity Built to Respond to Crisis Adequately;
I. Public-Private Partnership Established.[212]

The strategic dynamics of the cyber world will provide numerous opportunities for states' national interests and to maximize their power within their resilient capabilities. Thus, strategic cybersecurity and national security will be layered with suitable means and appropriate ways to follow up embodied objectives.

Role of the Military in Cyberspace

Establishing resilient cybersecurity is also the responsibility of the military. The military can cooperate with the other stakeholders and professionals to create awareness and provide secure cyberspace through the provision of resilient and robust capabilities.

---

[211] Organization for Security and Cooperation in Europe, *Guidelines for a Strategic Cybersecurity Framework in Bosnia and Herzegovina* (Sarajevo, Bosnia and Herzegovina: Organization for Security and Cooperation in Europe, 2019), 7, accessed 15 December 2019, https://www.osce.org/mission-to-bosnia-and-herzegovina/438383?download=true.

[212] Ibid., 9.

Capabilities include detecting, defending, responding, and preventing from cyber-attacks. Those capabilities apply to military systems and networks and allow the military to use them on battlefields and to defend their systems from enemies during peacetime.

Self-imposed strict rules the driving military to target only military targets. However, cyber-attacks may have potentially devastating effects on foreign nations, in case they are used out of purpose, whereas only political and diplomatic ramifications would stop the military. In the environment without self-imposed borders course deviation may occur, and no one can stop the military from inflicting foreign state's security.[213]

The analysis shows that the ministries of defense have a framework for responding to cyber-attacks against their information systems and networks. Responding to cyber-attacks through its cybersecurity capabilities and measures like developing resiliency, strengthening the information collection, investigation of incidents, analysis, and developing a realistic cyber training environment to enhance response capabilities.

For example, in October 2017, a total number of thirty-seven successful cyber-attacks conducted in order to compromise sensitive military and defense data belonging to the U.K. Ministry of Defense.[214] Vulnerabilities in network protocols could allow attackers to infect even mobile phones with malware or intercept their communications.

---

[213] Paul Szoldra, "Here's how the US military is beating hackers at their own game," Tech Insider, 2016, accessed 29 November 2019, https://amp.insider.com/us-military-cyberwar-2016-5.

[214] Alexander J, Martin, "MoD Secrets Exposed in Dozens of Cyber Security Breaches," October 2018, accessed 30 December 2019, https://news.sky.com/story/mod-secrets-exposed-in-dozens-of-cyber-security-breaches-11524076.

Whatsoever, it is not enough to have only cybersecurity measures in place. The Cadets CyberFirst program, of Ministry of Defense cadet organizations and the UK National Cyber Security Centre, will equip over 2,000 cadets a year with the skills and expertise to become future leaders in this emerging industry.[215] This investment in expert personnel capacities was enhancing long term cyber resiliency.

Some agencies are responsible for national protection, including prevention, mitigation, and recovery from cyberattacks. Like the FBI in the U.S.A., under the umbrella of the U.S. Department of Justice, it has responsibility for investigation and enforcement. The Department of Defense, including US Cyber Command, is in charge of national defense. In the U.S., various military branches have their cyber units.

Some countries gave authority to the military to be leading in their cybersecurity efforts but from the point of cyber defense. The cyber defense represents the part of the defense strategy under the responsibility of the ministry in charge of defense issues.[216]

Several examples represent actors in charge of cyber defense issues: The Albanian Ministry of Defense created the Interinstitutional Maritime Operational Center (IMOC) for developing cyber defense capability.[217] The Austrian Ministry of Defense cited cybersecurity as a significant component and priority of Austria's defense strategy

---

[215] UK Ministry of Defense, "Defence Secretary reveals new generation of 'cyber cadets,'" September 2018, accessed 30 December 2019, https://www.gov.uk/government/news/defence-secretary-reveals-new-generation-of-cyber-cadets.

[216] Darko Galinec, Darko Možnik, and Boris Guberina, "Cybersecurity and Cyber Defence: National Level Strategic Approach," *Automatika* 58, no. 3 (March 2017): 282.

[217] James A. Lewis and Katrina Timlin, *Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization* (Geneva, Switzerland United Nations Institute for Disarmament Research, 2011), 5.

in its 2008 White Book.[218] The Ministry of Defense of Columbia is the lead agency for National CERT, and cyber strategy. However, legislative, judicial, and international matters are handled by the respective agencies.[219] In 2008 an Estonian national cybersecurity strategy was drafted by the Cyber Security Strategy Committee, chaired by the Ministry of Defense in cooperation with the Ministry of Foreign Affairs, the Ministry of Internal Affairs, the Ministry of Education and Research, the Ministry of Justice and the Ministry of Economics.[220]

The Malaysian Ministry of Defense implements IT security policy to protect the government and businesses from cyberattacks and avoid harmful economic impact.[221] Evolving cyber threats are proliferating at a dramatic rate. However, there are two main challenges regarding dependency on the military. State that depends too heavily on the military for cybersecurity will feel decreasing incentives for the private sector to develop longer-term solutions.[222] Second, the risk of militarizing cybersecurity would be considered a bad political decision.[223]

On the other hand, from the perspective of serious crisis management, the military's capability plays an essential role. Thus, the cyber crisis may refer to time

---

[218] Lewis and Timlin, *Cybersecurity and Cyberwarfare*, 5.

[219] Ibid., 9.

[220] Ibid., 10.

[221] Ibid., 16.

[222] Ian Wallace, "The Military Role in National Cybersecurity Governance," Brookings Institutions, December 2013, accessed 30 December 2019, https://www.brookings.edu/opinions/the-military-role-in-national-cybersecurity-governance/.

[223] Ibid.

pressure, a severe threat, and a high level of uncertainty.[224] This domain, for sure, requires more deliberate research and analysis showed that cyber incidents would cause a crisis in the state in the same manner as natural disasters. That said, in the Netherlands, the multi partnership model between all stakeholders in-country is very successful in cybersecurity and cooperation-assistance during the crisis.[225] The Netherlands MoD CERT is first in line to aid civilian authorities in times of crisis.

Answering the third supporting research question: what is the role of the military and national departments in the protection of national cybersecurity? Depending on the state's legal constitution, MOD may play a significant role in leading the national cybersecurity efforts or through its cyber resilience ability to defend from cyber threats. In some cases, the military's supreme effort may have an exciting challenge like to be considered as the militarization of cyberspace. On the other hand, it may provide strategic support in developing legislations and lead cyber incident management.

Likewise, ensuring a role in national cybersecurity due to its military nature would be clear. The developing strategy may need to go through its ability to do so and experience in it.

National Cyber Security Strategy

Through analysis of data in chapter 4, sufficient information gained in order to answer the fourth research question.

---

[224] Sergei Boeke, *First Responder or Last Resort? The role of the Ministry of Defense in national cyber crisis management in four European countries* (Leiden, Netherlands: Universiteit Leiden, 2016), 5.

[225] Ibid., 47.

In accordance with BiH Defense Law, MoD BiH has competent objectives regarding the development of strategic documents:[226] a) ensuring and maintenance of defense capacity in order to ensure the protection of sovereignty, territorial integrity, political independence and international subjectivity of BiH, b) developing, review, and updating of the defense policy, c) formulating and approval of policies and regulations in terms of organization, administration, training, equipping, and use of the Armed Forces of BiH.

In the *Defense Planning Policy*, MOD BiH is responsible for developing defense policy, a framework for defense planning, and cooperate with Armed Forces BiH in the development of Military Strategy.[227]

Strategies are shaped during the development process. If structured well, a strategy formulation process ensures decisionmakers to evaluate the political, security, and budgetary environments, also identify choices for an organization, weight risks, opportunities, and trade-offs and the best course of action for the future.[228] MOD BiH, within its internal procedures, uses the process that identifies the national interests of

---

[226] House of Representatives of BiH, Parliamentary Assembly, Law on Defense of BiH, Sarajevo, (5 October 2005), 13, accessed 30 December 2019, http://www.mod.gov.ba/files/file/zakoni/Zakon-o-odbrani-bs.pdf.

[227] Ministry of Defense of Bosnia and Herzegovina, *Defence Planning Policy*, 2009, 6, accessed 30 December 2019, http://www.mod.gov.ba/dokumenti/interni_dokumenti/Politika%20odbrambenog%20planiranja%20-%20Bosanski%20jezik.pdf.

[228] Mark Cancian, Rick McPeak, Melissa Dalton, John Schaus, Colin McElhinny, Andrew Metrick, Hijab Shah, William Arnest, Stephanie Hartley, Alexa Hopkins, and Aftan Snyder, *Formulating National Security Strategy: Past Experience and Future Choices* (Washington, DC: Center for Strategic and International Studies, 2017), x.

Bosnia and Herzegovina, challenges and risks to the national security of BiH, defense objectives, defense strategy, own forces, friends and allies, and assessment and funding priorities.[229]

It should be clear that MoD BiH, without government-driven documents developed its cyber defense strategy. The MoD's strategy focuses on four main areas: prevention of cybersecurity incidents, response to cyber incidents; education and cyber awareness-raising with end-users.[230] By its initiative, MOD BiH started to develop its resiliency in cyberspace. Also, the Ministry of Defense developed an action plan to implement the strategy in the next five years and formed a supervisory committee for implementation of the strategy.[231] The review states that by 2021, the MOD intends to establish a secure cyber-environment for the Ministry's network and information systems. MOD applies a series of standards that were approved by the ITU and other international organizations.

Answering forth supporting research question is the MOD best choice to develop a national cybersecurity strategy. Correlating to data-driven from analysis, most of the countries delegate cyber strategy development to its MOD, and MOD BiH should develop national cybersecurity strategy due to its ability to develop strategies, and

---

[229] Ministry of Defense of BiH, Defense White Paper of BiH, 2005, 5, accessed 30 December 2019 http://www.mod.gov.ba/files/file/dokumenti/defense/engwhitebook.pdf.

[230] Eva Nagyfejeo and Sarah L Puello Alfonso, *Bosnia and Herzegovina Cyber Security Capacity Review: Bosnia and Herzegovina* (Oxford, UK: Global Cyber Security Capacity Centre, March 2019), 29, accessed 26 December 2019, http://mkt.gov.ba/dokumenti/informatizacija/ostali_propisi/default.aspx?id=7650&langTag=bs-BA.

[231] Ibid., 30.

strategic documents that are in line with national efforts, and presents ends, ways, and means.

Conclusion

This chapter answers the four supporting questions. From the analysis of data, it is evident that there is a continuous expansion of cyber threats and its opportunities within cyberspace. Cyberspace is a reality in which subversive practices are emerging. In the generation of expanding information and knowledge, cyberspace's physical dimensions are distinct, borderless, and not comparable to land, air, sea dimensions.

Thus, the normal functioning of state's societies in cyberspace, and protecting cyber-reliant critical infrastructure, is only possible with effective strategic cybersecurity framework. Most committed countries in today's world established presented their cyber commitment with the developing national cybersecurity strategy. It is the principal and most crucial segment of reliable and resilient national cybersecurity.

To ensure commitment in cybersecurity, it requires alignment, and systematization with the international framework, most relevant regulations, and legal initiatives. International cooperation and collaboration are a fundamental principle of commitment to the cybersecurity. It allows to frame and to craft national regulations, strategic documents, and strategies accordingly with required standards.

In those documents' roles and responsibilities of various government entities would be stated. Because adequate cybersecurity, threat prevention, and combating cyber threats require the intervention and cooperation of several entities within the country.

In this chapter, four different topics have been analyzed. First, cyber threats and their impacts on national security presented. Second, the essential requirements to ensure

national cybersecurity pointed out. Next, the role of the military in ensuring cybersecurity for national security analyzed. Finally, an analysis of the military's role in formulating national cybersecurity strategy was presented.

Chapter 5 will provide a conclusion and discuss a recommendation based on all information and research complied throughout this review, to best answer the primary research question.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

Introduction

The age of expanding globalization created a security environment strongly associated with the information security of the digital world. The cyber domain is creating enormous opportunities for adversaries to conduct actions for their benefits and to harm governments and individuals. Nevertheless, the strategic dynamics of the cyberspace is an opportunity for states to impose their all instruments of national power over their competitors. Fundamentally, societies are becoming more technologically reliant than ever before. The protection of cyber reliant critical information infrastructure is a paramount concern for the whole nation. For any state, integrated and comprehensive approach to security and information management should be based on a whole of government basis.

Cybersecurity is a dilemma for national security and requires collaboration between governmental and non-governmental entities. A whole of government approach concept will be an act of unity of effort between all stakeholders to maximize a collaborative unity of action to counter cyber threats. The significance of understanding the role of the military in national cybersecurity efforts, specifically, capabilities that could be provided throughout the entire process of national cybersecurity framework is essential to ensure adequate roles and responsibilities to protect cyberspace.

This study attempted to develop a response for the primary research question: should the Ministry of Defense of BiH lead national cybersecurity efforts. This primary research question relied on four secondary research questions that have been answered in

chapter 4. The secondary research questions induced the study to view cyberspace as a distinctive actor of the borderless environment in which BiH needs to ensure reliable national cybersecurity. As a result, chapter 4 described destabilizing threats of national cyberspace, and the state's required sufficient efforts to protect it, and sought to determine ways the military underpin the national cybersecurity.

With gathered and analyzed data, the study promptly answered the main question from the perspective of the suitability of MOD BiH as a strategic option for national cybersecurity efforts. The study addressed the suitability of existing capability of MOD BiH for the accomplishment of strategic objectives of BiH's National Cyber Security efforts:

Strategic objective 1. Systematic development of cybersecurity strategic legislations and documents. It is suitable for the MOD to design and develop a cybersecurity strategy. The MOD can develop legislation and national strategy in coordination with Joint Staff of Armed Forces.

Strategic objective 2. Ensure secure Information and Communication systems. Defining security measures for all service providers would not be suitable, for MOD by itself since it requires expertise for different state's social domains. Deep collaboration requires coordination and support from the Personal Data Protection Agency in Bosnia and Herzegovina and BiH's Ministry of Communications and Transport.

Strategic objective 3. Cyber awareness-raising and cybersecurity education. Partial suitability of MOD has been found since BiH's internal public educational structure is divided into entities' levels within the Ministry of Educations on each entity level. It would be very extensively challenging to develop and execute programs

regarding for all citizens. MOD BiH's Peace Support Operations Training Centre, in cooperation with BiH's Agency for the training of security forces, may provide training and education for security forces and law enforcement.

Strategic objective 4. Establishment of authority for National Cyber Security. In accordance with the Decision of Council of Ministers of BiH on the Establishment of Computer Emergency Response, it is the responsibility of the Ministry of Security of Bosnia and Herzegovina to establish National CERT. MOD BiH is not a suitable option. On the other hand, MOD BiH's cybersecurity center, for protection of its own IC infrastructure, would be the functional body within the organizational structure of National CERT.

Strategic objective 5. Secure and resilient IC systems. Suitability of MOD BiH as an option cannot be considered due to the legal responsibility of the Regulatory Agency for Communications of BiH (RAC BiH). The RAC BiH as the main provider of licenses for this structure prescribes requirements for protection. MOD BiH applies required protection and control measures for its infrastructure.

Strategic objective 6. Developing cybercrime capacity. Due to its responsibilities prescribed in BiH's defense law and national legislations, MOD BiH is not suitable for this option. Law enforcement institutions are responsible for investigating and prosecuting cybercrime in BiH.

Strategic objective 7. International, Regional, and National Cybersecurity cooperation. The membership in the UN, NATO, OSCE, the CoE, FIRST, TF-CSIRT, and other organizations enforce commitment to fulfilling their cybersecurity requirements. Since some of the memberships requires extensive technical expertise in

cybersecurity, MOD BiH represents a partially suitable option with the capability to participate in strategic defense cooperation within NATO, OSCE, EUFOR, other countries' military cyber organizations, and military cyber exercises, training, and conferences.

Strategic objective 8. Building a competent capacity to respond to the national cybersecurity crisis. Dealing with cybersecurity protection of states' critical infrastructure requires national authority, such as National CSIRT, to be in place. With the capability to observe, identify, report, and manage cyber incidents of its infrastructure MOD BiH is a partially suitable option.

Strategic objective 9. Technical Public-Private Partnership. The fulfillment of this objective requires technical expertise in order to be the state's leading authority to establish cooperation with the private sector. Therefore, MOD might not be a suitable strategic option. However, to maintaining and developing its infrastructure, MOD BiH should develop a partnership with the national private industrial sector in the domain of cybersecurity development.

Conclusion

Based on research analysis MOD BiH is not a suitable option to lead national cybersecurity efforts but still may provide strategic support within its capabilities.

Despite some moderate shortfalls in the ability to secure BiH's IT systems, nation's cyberspace, or information communication systems, fight cybercrime, and ensure nation's public-private cooperation MOD BiH with its distinct capabilities is well aligned to support BiH's cybersecurity objectives. With that said, MOD's unique capabilities to formulate policies and strategies, provide a shared understanding on the

cyber environment, initiate cyber awareness, and combined international efforts stand out strategic military contribution to the BiH. Its limited budgetary circumstances and mildly unpopular public viewpoint are an irregular feature of its strategic capabilities, although may considerably decrease possibilities for more cybersecurity contribution.

Emerging cyber threats are the most pervasive threats that cause insidious harm to the state's critical infrastructure.[232] To deter cyber threats, it requires to have an effective perimeter defense, an all-round defense, for critical infrastructure as a nation's strongpoints. Because cybersecurity is a global problem that significantly exceeds the capabilities of any single governmental entity, it should be known that the government's cybersecurity efforts with an inadequate strategic cybersecurity framework, and dispersed and uncoordinated national authorities, are doomed to failure.[233]

After a thorough examination of a variety of references and data, this thesis reveals that MOD BiH is not suited to lead the national cybersecurity efforts. Furthermore, cyber threats are an issue of national security. Responsibility to protect the nation's cyberspace should not be delegated to a single entity in government. There are several reasons why MOD BiH is not a suitable option: a) military's leading of nation's cybersecurity efforts may appear as a sort of military campaign, b) Bosnia and Herzegovina's society may have a public perception of the militarization of cyberspace, c) for MOD BiH, attracting and retaining sufficient cybersecurity experts may not be financially feasible, d) the centrality of MOD BiH is not a politically viable option, e)

---

[232] Walter Gary Sharp, Sr., "The Past, Present and Future of Cybersecurity," *Journal of National Security Law and Policy* 4, no. 13 (2010): 13.

[233] Ibid., 25.

MOD BiH may encounter overload with its mission since cybersecurity is broader than the military.

Nevertheless, MOD BiH is capable of translating BiH's state interests into Strategic Directions. In the current analyzed situation, MOD BIH is responsible for defending and protecting its networks. Although MOD BiH developed its cybersecurity strategy. In order to make the national and MoD's cybersecurity strategies to be coherent and compatible, it requires mutual collaboration between all governmental entities of BiH. In regards to this, to achieve a mutual collaboration thesis suggests the establishment of the National Cybersecurity Directorate.

Establishing directorate would help to mitigate existing overlapping responsibilities and improve the state's strategic cybersecurity vision.[234] The directorate would allow combining the existing cyber capabilities of each entity in the BiH.

This directorate would bring several benefits for BiH national cybersecurity efforts. MOD BiH would be able to contribute to its capabilities and developed cybersecurity strategy greatly. It would be combined among many ministries in BiH. The memorandum of understanding to exchange personnel, the collaboration between all stakeholders would be extended with technical expertise in the cyber domain. The legal structure would be solidified, and bureaucracy decreased. Beside BiH's relevant ministries, it would also include private sector representatives.

---

[234] U.S. Government Accountability Office, *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented: Report to Congressional Addressees* (Washington, DC: U.S. Government Accountability Office, 2013) 4.

Establishing national cybersecurity directorate, BiH shows its commitment to cybersecurity as an integrated and comprehensive whole of government approach. A whole of government approach is a concept in which the government draws together relevant state's stakeholders vital to the success of national cybersecurity by maximizing coordination and collaboration to achieve a unified effort.[235]

To achieve this unified effort, the cybersecurity directorate should be established as administrative organizations within the Ministry of Security of BiH. The administrative bodies established by the BiH's law are with operational independence and established to perform tasks within their competence, managed by directors, and financed from the budget of BiH institutions.[236]

The BiH's cybersecurity directorate as a mission would have to determine the cybersecurity measures to be taken by public and private institutions and organizations to approve the prepared cybersecurity plans, programs, reports, procedures, principles, and standards and to ensure their implementation and coordination. In general, the more

---

[235] Jason L. Percy and Terry A. Fellows Jr., "A Whole of Government Approach for National Security" (master's thesis, Naval Postgraduate School, Monterey, CA, 2009), 45.

[236] Parliamentary Assembly of Bosnia and Herzegovina, Law on The Directorate for Coordination of Police Bodies and on Agencies for Support to the Police Structure of Bosnia And Herzegovina are administrative organizations within the Ministry of Security of BiH, Sarajevo, 2008, 1, accessed 30 December 2019, http://www.dkpt.ba/Dokumenti/propisi_i_dokumenti_Zakoni_1%20Zakon%20o%20direkciji%20za%20koordinaciju%20policijskih%20tijela_Zakon%20o%20direkciji%20za%20koordinaciju%20policijskih%20tijela%20i%20o%20agencijama%20za%20podrsku%20policijskoj%20strukturi%20BiH.pdf.

centralized the leading structure BiH has, the greater the BiH's ability to achieve unity of effort.[237]

Key Findings

Research noticed that growing cyberspace, and its impact on the state's security, forcing governments to apply adequate collective national security measures, including all stakeholders in the country to mitigate the damage from adversary cyber actions.

Emphasizing growing importance to protect critical infrastructures of the country from cyber-attacks stressed out increasing the military's role in supporting the national cybersecurity efforts through its cyber capabilities both on the battlefield and supporting resources to protect its critical infrastructure in peacetime.

Recommendations

Based on research and analysis I recommend the development of National Cybersecurity Software. Extensive and focused cooperation with the national relevant private sector in the domain of cybersecurity is required to develop national cybersecurity software that will protect critical information systems within the state.

Based on the analysis, I recommend a centralized National Cyber Structure. Through defined clear national standards, guidelines, and regulations develop a centralized agency to coordinate and manage counter cyber measures in order to ensure security and resiliency of the nation's critical infrastructure.

---

[237] U.S. Department of Defense, Joint Publication Law on The Directorate for Coordination of Police Bodies and on Agencies for Support to the Police Structure of Bosnia: Multinational Operations, 01 March 2019, accessed 26 November 2019, II-17.

Having a leading element in the command structure may also be characterized by an integrated state's cyber relevant stakeholders. Integrating the staff enables the directorate to bring expertise to other ministries. The recommended structure will enable synchronization, coordination, and integration of all relevant state entities to ensure unity of effort.[238] Failure to accomplish unity of effort can cost the lives of BiH citizens, create political instability, and jeopardize BiH's cybersecurity efforts.

Considering BiH's internal state organization and existing cybersecurity capabilities, building a centralized agency to confront cyber threats could be structured as a civil-military organization. Based on that study recommended structure is as follows.

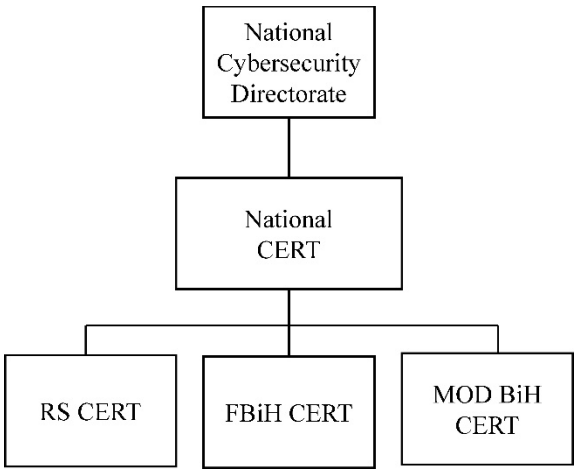

Figure 3. National Cybersecurity Organization

Source: Created by author.

Roles and responsibilities are open for further discussion and may include:

[238] Joint Chiefs of Staff, JP 3-0, I-8.

National cybersecurity directorate would be responsible to 1) prepare and update strategic cybersecurity documents; 2) coordinate cybersecurity between CERTs; 3) evaluate cybersecurity activities; 4) assist in the preparation of cybersecurity regulations.

National CERT should be responsible for analyzing threats, reducing vulnerabilities, and providing cyber threat warning, and coordinating incident response.

CERT of the Republic of Srpska should continue to coordinate, prevent, respond, and protect cyberspace of RS and provide strategic technical assistance in efforts for establishing National CERT. CERT of the Federation of Bosnia and Herzegovina should be responsible for coordinating, preventing, responding, and protect cyberspace of the Federation of BiH. MOD BiH CERT should be responsible for the protection of its critical infrastructure and development of cyber defense capabilities.

Further Research

The comprehensive study of Bosnia and Herzegovina on public interest on becoming a cybersecurity operator in MOD. This can be achieved by using quantitative research. Information from this would benefit from understanding future cybersecurity investments. Also, it may refine possible skill sets of operators and bring uncover solutions.

BIBLIOGRAPHY

Akhgar, Babak, Andrew Staniforth, and Francesca Bosco. *Cyber Crime and Cyber Terrorism Investigators Handbook*. Waltham, MA: Syngress Publishing, 2014.

Ayala, Luis. *Cybersecurity Lexicon*. Berkeley, CA: Apress, 2016.

Azmi, Riza, William Tibben, and Khin Than Win. "Motives behind Cyber Security Strategy Development: A Literature Review of National Cyber Security Strategy." Paper presented at Australasian Conference on Information Systems, Wollongong, Australia, 5-7 December 2016.

Bada, Maria. "The Social and Psychological Impact of Cyberattacks." In *Emerging Cyber Threats and Cognitive Vulnerabilities*, edited by Vladlena Benson and John McAlaney. San Diego, CA: Elsevier, 2019.

Barakovic, Sabina, and Jasmina Barakovic Husic. "'We Have Problems for Solutions': The State of Cybersecurity in Bosnia And Herzegovina." *Information & Security Journal* 32, no. 2 (2015): 1-24. Accessed 30 November 2019. http://defence management.org/system/files/3205_bih_barakovic.pdf.

Barnes, Julian E. "Pentagon computer networks attacked." *Los Angeles Times*. 2008. Accessed 27 December 2019. https://www.latimes.com/archives/la-xpm-2008-nov-28-na-cyberattack28-story.html.

Bidgoli, Hossein. *Global Perspectives in Information Security Legal, Social, and International Issues*. Hoboken, NJ: Wiley, 2009.

Blumbergs, Bernhards. *Technical Analysis of Advanced Threat Tactics Targeting Critical Information Infrastructure*. Cyber Security Review. NATO Cooperative Cyber Defence Centre, 2014), 1. Accessed 29 December 2019. https://ccdcoe.org/ uploads/ 2018/10/2014-Technical-Analysis-of-Advanced-Threat-Tactics-Targeting-Critical-Information-Infrastructure.pdf.

Boeke, Sergei. *First Responder or Last Resort? The role of the Ministry of Defense in national cyber crisis management in four European countries*. Leiden, Netherlands: Universiteit Leiden, 2016.

Bosnia and Herzegovina Council of Ministers. *Strategy of Bosnia and Herzegovina for Preventing and Combating Terrorism 2015-2020*. Sarajevo: Ministry of Security of Bosnia and Herzegovina, 2015. Accessed 27 December 2019. http://msb.gov. ba/PDF/STRATEGIJA_ZA_BORBU_PROTIV_TERORIZMA_ENG.pdf

Brookson, Charles, Scott Cadzow, Ralph Eckmaier, Jörg Eschweiler, Berthold Gerber, Alessandro Guarino Guarino, Kai Rannenberg, Jon Shamah, and Sławomir Gorniak. *Definition of Cybersecurity-Gaps and Overlaps in Standardisation.* Heraklion, Greece: European Union Agency for Network and Information Security, December 2015. Accessed 20 October 2019. https://www.enisa.europa.eu/publications/definition-of-cybersecurity/at_download/fullReport.

Bucci, Steven P. "The Confluence of Cyber Crime and Terrorism," Heritage Foundation, 12 June 2009. Accessed 26 September 2019, https://www.heritage.org/defense/report/the-confluence-cyber-crime-and-terrorism.

Cambridge Dictionary. New York: Cambridge University Press, 2019. Accessed 25 December 2019. https://dictionary.cambridge.org/us/dictionary/english/cyberattack.

Canadian Centre for Cyber Security. *An Introduction to the Cyber Threat Environment*. Gloucester ON: Communications Security Establishment Canada, 2018. Accessed 16 August 2019. https://cyber.gc.ca/sites/default/files/publications/Intro-to-cyber-threat-environment-e.pdf.

Cancian, Mark, Rick McPeak, Melissa Dalton, John Schaus, Colin McElhinny, Andrew Metrick, Hijab Shah, William Arnest, Stephanie Hartley, Alexa Hopkins, and Aftan Snyder. *Formulating National Security Strategy: Past Experience and Future Choices*. Washington, DC: Center for Strategic and International Studies, 2017.

Center for Strategic and International Studies. *Significant Cyber Incidents List*. 2019. Accessed 28 November 2019. https://csis-prod.s3.amazonaws.com/s3fs-public/200504_Cyber_Attacks.pdf?0M9lsdHhOXhw.BahGk5hYXgDtEWrs6x9.

———. *Global Cyber Strategies Index*. Washington, DC: Center for Strategic International Studies, 2019.

Centre of Excellence Defence Against Terrorism, North Atlantic Treaty Organization, and Public Diplomacy Division. *Responses to Cyber Terrorism* (Washington, DC: IOS Press, 2008.

Choucri, Nazli. *Cyberpolitics in International Relations*. Cambridge, MA: The MIT Press, 2013.

Clark, David D., Thomas A. Berson, and Herbert undefined Lin. *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues*. Washington, DC: National Academies Press, 2014.

Clark, David. “Characterizing Cyberspace: Past Present and Future.” MIT Computer Science and Artificial Intelligence Lab. 12 March 2010. Accessed 13 August 2019. https://projects.csail.mit.edu/ecir/wiki/images/7/77/Clark_Characterizing_cyberspace_1-2r.pdf.

Clarke, Richard A. and Robert K. Knake. *Cyber War-The Next Threat to National Security and What to Do About It*. New York: Harper Collins Publishers, 2010.

Coats, Daniel R. *The National Intelligence Strategy of the United States of America*. Washington, DC: U.S. Office of the Director of the National Intelligence, 2019. Accessed 29 December 2019. https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf.

Collins, Stuart. “Cyber-Attacks: Critical Infrastructure.” Global Risk Dialogue. *Allianz Global Corporate and Specialty* 1 (Summer/Fall 2016): 14-29. Accessed 27 December 2019. https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/grd/AGCS-GRD-1-2016-EN.pdf.

Cybersecurity and Infrastructure Security Agency. “Critical Infrastructure Sectors.” 5 March 2013. Accessed 13 August 2019. https://www.cisa.gov/critical-infrastructure-sectors.

Davis, Susan. *NATO in the Cyber Age: Strengthening Security and Defense, Stabilizing Deterrence*. Brussels, Belgium: NATO Parliamentary Assembly, 2019.

Denning, Dorothy E. “Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy.” In *Networks and Netwars: The Future of Terror, Crime, and Militancy*, edited by John Arquilla and David Ronfeldt, 239-288. Santa Monica, CA: RAND Corp, 2001.

Detlefsen, William R. “Cyber Attacks, Attribution, and Deterrence: Three Case Studies.” Monograph, School of Advanced Military Studies, U.S. Army Command and General Staff College, Fort Leavenworth, KS, 2015. Accessed 26 September 2019. https://apps.dtic.mil/dtic/tr/fulltext/u2/1001276.pdf.

Does, Antonia. *The Construction of the Maras: Between Politicization and Securitization*. Geneva, Switzerland: Graduate Institute Publications, 2013.

Dorff, Robert H. “A Primer in Strategy Development.” In *U.S. Army War College Guide to Strategy*, edited by Joseph R. Cerami and James F. Holcomb, 11-18. Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, 2001.

Duffield, John S. “NATO’s Functions After the Cold War.” *Political Science Quarterly* 109, no. 5 (1994-1995): 764.

Efthymiopoulos, Marios Panagiotis. “A Cyber-Security Framework for Development, Defense and Innovation at NATO.” *Journal of Innovation and Entrepreneurship* 8, no. 1 (2019): 1-26. Accessed 26 September 2019. https://innovation-entrepreneurship.springeropen.com/track/pdf/10.1186/s13731-019-0105-z.

Eikmeier, Dale C. *From Operational Art to Operational Plans: A Joint Planning Primer*. 9th ed. Fort Leavenworth, KS: U.S. Army Command and General Staff College, 2012.

European Commission. *Commission Staff Working Document: Bosnia and Herzegovina 2016 Report*. Brussels, Belgium: European Union, 2016. Accessed 30 November 2019. https://ec.europaeu/neighbourhood-enlargement/sites/near/files/pdf/key_documents/2016/20161109_report_bosnia_and_herzegovina.pdf.

European Network and Information Security Agency. *National Cyber Security Strategies: Practical Guide on Development and Execution*. Athens, Greece: European Union Agency for Cybersecurity, 2012.

———. *National Cyber Security Strategies: Setting the course for national efforts to strengthen security in cyberspace*. Brussels, Belgium: European Network and Information Security Agency, 2012.

European Union Agency for Cybersecurity. “National Cybersecurity Strategies.” 2019. Accessed 17 August 2019. https://www.enisa.europa.eu/topics/national-cyber-security-strategies.

European Union Agency for Network and Information Security. *Cybersecurity Cooperation: Defending the Digital Frontline*. Heraklion, Greece: European Union Agency for Network and Information Security, 2013. Accessed 29 October 2019. https://www.enisa.europa.eu/publications/cybersecurity-cooperation-defending-the-digital-frontline/at_download/fullReport.

———. *NCSS Good Practice Guide: Designing and Implementing National Cyber Security Strategies*. Heraklion, Greece: European Union Agency for Network and Information Security, November 2016. Accessed 30 October 2019. https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

———. *Threat Landscape Report 2018: 15 Top Cyberthreats and Trends* (Athens. Greece: European Union Agency for Network and Information Security. January 2019). Accessed 26 September 2019. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018.

———. *UNISA Threat Landscape Report 2018. 15 Top Cyberthreats and Trend*. Heraklion, Greece: European Union Agency for Network and Information Security, January 2019. Accessed 30 November 2019. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018.

Forum of Incident Response and Security Teams. “3 The Difference Between a CSIRT and a PSIRT.” In “FIRST CSIRT Services Framework.” 2019. Accessed 16 August 2019. https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1#3-The-Difference-Between-a-CSIRT-and-a-PSIRT.

Galinec, Darko, Darko Možnik, and Boris Guberina. “Cybersecurity and Cyber Defence: National Level Strategic Approach.” *Automatika* 58, no. 3 (March 2017): 273-86.

Geers, Kenneth. “Cyberspace and the Changing Nature of Warfare.” Keynote speech, Research and Technology Organisation Symposium, Information Assurance for Emerging and Future Military Systems, Ljubljana, Slovenia, 13 October 2008. Accessed 25 August 2019. http://www.blackhat.com/presentations/bh-jp-08/bh-jp-08-Geers/BlackHat-Japan-08-Geers-Cyber-Warfare-Whitepaper.pdf.

———. *Strategic Cyber Security*. Tallinn, Estonia: CCD COE Publications, 2011. Accessed 26 September 2019. https://ccdcoe.org/uploads/2018/10/2011_Proceedings_0-1.pdf.

Global Cyber Security Capacity Centre. “Cybersecurity Capacity Review Bosnia and Herzegovina.” Bosnia and Herzegovina Ministry of Communications and Transport. 2019. Accessed 30 November 2019. http://www.mkt.gov.ba/dokumenti/informatizacija/ostali_propisi/default.aspx?id=7650&langTag=bs-BA.

Goodwin, Cristin Flynn, and J. Paul Nicholas. *Developing a National Strategy for Cybersecurity: Foundations for Security, Growth, and Innovation*. Redmond, WA: Microsoft Corporation, 2013.

Headquarters, Department of the Army. Army Techniques Publication 5-0.1. *Army Design Methodology*. Washington, DC: Government Publishing Directorate, July 2015.

Herzog, Stephen. “Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses.” *Journal of Strategic Security* 4, no. 2 (2011): 49-60.

Horowitz, Michael. *A Common Future? NATO and the Protection of the Commons*. Chicago Council Trans-Atlantic Paper Series No. 3. Chicago: Chicago Council on Global Affairs2010.

Hundley, Richard O., and Robert H. Anderson. “Emerging Challenge: Security and Safety in Cyberspace.” In *In Athenas Camp: Preparing for Conflict in the Information Age*, edited by John Arquilla and David Ronfeldt, 231-252. Santa Monica, CA: RAND, 1997. Accessed 26 September 2019. https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR880/MR880.ch10.pdf.

Iasiello, Emilio. “Cyber-attack: A dull tool to shape foreign policy.” Paper presented at the 5th International Conference on Cyber Conflict (CYCON), Tallinn, Estonia, 2013. Accessed 29 December 2019. https://ieeexplore.ieee.org/document/6568392.

———. “Is Cyber Deterrence an Illusory Course of Action?” *Journal of Strategic Security* 7, no. 1 (2014): 54-67.

International Telecommunication Union. *Overview of Cybersecurity*. ITU-T X.1205. Geneva, Switzerland: International Telecommunication Union, 2008. Accessed 20 October 2019. https://www.itu.int/rec/dologin_pub.asp?lang=s&id=T-REC-X.1205-200804-I!!PDF-E&type=items.

———. *World Information Society Report 2007* Geneva, Switzerland: International Telecommunications Union, 2007. Accessed 10 August 2019. http://handle.itu.int/11.1002/pub/8020d0d0-acb598bc-en.

Jabuka. “Brkić: Članstvo u EU i NATO savezu štiti naše posebnosti [Brkić: Membership in the EU and NATO protects our specialties].” 12 August 2019. Accessed on 11 September 2019. https://www.jabuka.tv/brkic-clanstvo-u-eu-i-nato-savezu-stiti-nase-posebnosti/.

Jang-Jaccard, Julian, and Surya Nepal. “A Survey of Emerging Threats in Cybersecurity.” *Journal of Computer and System Sciences* 80, no. 5 (2014): 973-93. Accessed 10 August 2019. https://doi.org/10.1016/j.jcss.2014.02.005.

Johnson, Gerry, Kevan Scholes, and Richard Whittington. *Exploring Corporate Strategy*. London, UK: Prentice Hall, 2006.

Joint Chiefs of Staff. Joint Publication 3-12. *Cyberspace Operations*. Washington, DC: Office of the Secretary of Defense.

Joint Communication to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions. “Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.” European External Action Service. 2013. Accessed 15 August 2019. http://www.eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf.

Karatzogianni, Athina. *Cyber Conflict and Global Politics*. London, UK: Routledge, 2010.

Klimburg, Alexander, ed. *National Cyber Security Framework Manual*. Tallinn, Republic of Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2012. Accessed 30 October 2019. https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf.

Kremling, Janine, and Amanda M. Sharp Parker. *Cyberspace, Cybersecurity, and Cybercrime*. Thousand Oaks, CA: SAGE Publications, 2017.

Kuehl, Daniel T. “From Cyberspace to Cyberpower: Defining the Problem.” In *Cyberpower and National Security*, edited by Franklin D. Starr, Stuart H. and Wentz, Larry, 3-23. Washington, DC: Potomac Books Inc., 2009.

Lewis, James A. “Cybersecurity and critical infrastructure protection.” Center for Strategic and International Studies, 2006. Accessed 25 October 2019. https://www.csis.org/analysis/cybersecurity-and-critical-infrastructure-protection.

Lewis, James A., and Katrina Timlin. *Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization*. Geneva, Switzerland United Nations Institute for Disarmament Research, 2011.

Leyden, John. “Panicked teen hanged himself after receiving ransomware scam email.” The Register. 2015. Accessed 29 November 2019. https://www.theregister.co.uk/2015/01/23/autistic_teen_joseph_edwards_ransomware_scam_suicide_tragedy/.

Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND, 2009.

———. “The Coming of Cyber Espionage Norms.” Paper presented at the 9th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 2017. Accessed 18 August 2019. https://ieeexplore.ieee.org/document/8240325.

Lovegrove, James. “The Implications of Cyber-Attacks on Governments.” Diplomatic Courier. 2016. Accessed 25 November 2019. https://www.diplomaticourier.com/posts/implications-cyber-attacks-governments.

Luiijf, Eric, Kim Besseling, and Patrick de Graaf. “Nineteen National Cyber Security Strategies.” *International Journal of Critical Infrastructures* 9, no. 1/2 (2013): 3-31.

Martin, Alexander J. “MoD Secrets Exposed in Dozens of Cyber Security Breaches.” October 2018. Accessed 30 December 2019. https://news.sky.com/story/mod-secrets-exposed-in-dozens-of-cyber-security-breaches-11524076.

Meyer, Paul. “Outer Space and Cyberspace.” In *International Cyber Norms: Legal, Policy and Industry Perspectives*, edited by Anna-Maria Osula and Henry Roigas, 155-169. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2016.

Ministry of Economic Affairs and Communication. “Cyber Security Strategy Committee, Ministry of Defense, Cyber Security Strategy. Tallinn Estonia: Republic of Estonia, 2008. Accessed 31 October 2020. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy.

———. *Cyber Security Strategy 2019-2022*. Tallinn, Republic of Estonia: Republic of Estonia, 2019. Accessed 31 October 2019. https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf.

Ministry of Security of Bosnia and Herzegovina. *Strategija Uspostave CERT-a u Bosni i Hercegovini* [Strategy for establishment of CERT in Bosnia and Herzegovina]. Sarajevo, Bosnia and Herzegovina: Republic of Bosnia and Herzegovina, 2011. Accessed 25 November 2019. http://www.msb.gov.ba/dokumenti/strateski/default.aspx?id=6248&langTag=bs-BA.

———. *Strategy of BiH for preventing and Combating Terrorism 2015-2020*. Sarajevo, Bosnia and Herzegovina: Republic of Bosnia and Herzegovina, 2015. Accessed 24 November 2019. http://www.msb.gov.ba/dokumenti/strateski/default.aspx?id=12786&langTag=en-US.

Mok, Kenneth. "Cyber Threat or Cyber Threat Inflation? – Assessing the Risk to U.S. National Security." *Small Wars Journal* (2019). Accessed 25 December 2019. https://smallwarsjournal.com/jrnl/art/cyber-threat-or-cyber-threat-inflation-assessing-the-risk-to-us-national-security.

Mujanovic, Jasmin. "Jasmin Mujanovic for EWB: Four Theses on Bosnia-Herzegovina's Euro-Atlantic Future." European Western Balkans. 2015. Accessed 11 September 2019. https://Europeanwesternbalkans.com/2015/03/16/jasmin-mujanovic-for-ewb-four-theses-on-bosnia-herzegovinas-euro-atlantic-future/.

Mušić, Safet, and Anesa Agović. "Online Radicalisation–Security Challenge That Endures." Paper presented at the Third Sarajevo International Conference on Social Sciences, Sarajevo, Bosnia and Herzegovina, 27-30 April 2017.

Mušić, Safet. "Cyber napadi su realna i postojeća prijetnja za BiH [Cyber-attacks are real and existing security issue for BiH]." Al Jazeera Balkans, November 2019. Accessed 20 November 2019. http://balkans.aljazeera.net/vijesti/cyber-napadi-su-realna-i-postojeca-prijetnja-za-bih.

Nagyfejeo, Eva, and Sarah L Puello Alfonso. *Bosnia and Herzegovina Cyber Security Capacity Review: Bosnia and Herzegovina*. Oxford, UK: Global Cyber Security Capacity Centre, March 2019. Accessed 26 December 2019. http://mkt.gov.ba/dokumenti/informatizacija/ostali_propisi/default.aspx?id=7650&langTag=bs-BA.

National Cyberwatch Center. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. Washington, DC: United States Executive Office of the President, 2014. Accessed 31 October 2019. https://www.nationalcyberwatch.org/ncw-content/uploads/2016/03/Cyberspace_Policy_Review_final-1-1.pdf.

National Initiative for Cybersecurity Careers and Studies. "A Glossary of Common Cybersecurity Terminology." 2019. Accessed 21 October 2019. https://niccs.us-cert.gov/about-niccs/glossary#C.

National Intelligence Council. *Global Trends 2025: A Transformed World*. Washington. DC: U.S. Government Printing Office, November 2008. Accessed 26 September 2019. https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/2025_Global_Trends_Final_Report.pdf.

National Security Agency. "Understanding the Threat." 2019. Accessed 25 December 2019. https://www.nsa.gov/what-we-do/understanding-the-threat/.

Newmeyer, Kevin P. "Who Should Lead US Cybersecurity Efforts?" *Prism: A Journal of the Center for Complex Operations* 3, no. 2 (2012): 115-123. Accessed 30 November 2019. https://apps.dtic.mil/docs/citations/AD1042583.

Nielsen, Suzanne C. "The Role of the US Military in Cyberspace." *Journal of Information Warfare* 15, no. 2 (2016): 27-38.

North Atlantic Treaty Organization. *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization.* Lisbon, Portugal: North Atlantic Treaty Organization, 2010. Accessed 29 October 2019. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf.

Nye, Jr., Joseph S., "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly* 5, no. 4 (Winter 2011): 18-38.

O'Reirdan, Michael. "Why Bother with Best Practices? Or Why Global Collaboration is Faster (and More Effective) Than a Speeding Bullet." Cyber Security, New Europe (Special Edition). 2011. Accessed 25 August 2019. http://www.scribd.com/doc/56702531/Cyber-Security-2011.

Obama, Barack. The Comprehensive National Cybersecurity Initiative. Washington, DC: White House, 2010. Accessed 29 December 2019. https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative.

Official Gazette of Republic of Srpska. *Law on Information Security*. No. 70 of 12 July 2011. Banja Luka, Republika Srpska: Government of Republika Srpska, 2011. Accessed 30 November 2019. http://www.podaci.net/_gBiH/propis/Zakon_o_informacionoj/Z-ibezbj03v1170.html.

Organization for Economic Co-operation and Development. *Security Policy Making a Turning Point: Analyzing a New Generation of National Cybersecurity Strategies for the Internet Economy*. Paris, France: Organization for Economic Co-operation and Development, 2012. Accessed 29 December 2019. http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf.

Organization for Security and Cooperation in Europe. *Guidelines for a Strategic Cybersecurity Framework in Bosnia and Herzegovina*. Sarajevo, Bosnia and Herzegovina: Organization for Security and Cooperation in Europe, 2019. Accessed 15 December 2019. https://www.osce.org/mission-to-bosnia-and-herzegovina/438383?download=true.

Parliamentary Assembly of Bosnia and Herzegovina. *Akcioni plan za provođenje strategije Bosne i Hercegovine za prevenciju i borbu protiv terorizma (2015. - 2020)* [Action Plan for Implementation of Strategy of BiH for Preventing and Combating Terrorism 2015-2020]. Sarajevo, Bosnia and Herzegovina: Republic of Bosnia and Herzegovina, 2015. Accessed 24 November 2019. https://www.parlament.ba/act/ActDetails?actId=854.

Percy, Jason L., and Terry A. Fellows Jr. "A Whole of Government Approach for National Security." Master's thesis, Naval Postgraduate School. Monterey, CA, 2009.

Presidency of Bosnia and Herzegovina. *The Foreign Policy Strategy of Bosnia and Herzegovina 2018-2023*. Sarajevo, Bosnia and Herzegovina: Republic of Bosnia and Herzegovina, 2018. Accessed 30 November 2019. http://www.predsjednistvobih.ba/vanj/default.aspx?id=9555&langTag=en-US.

Prey Project. "What Are Cyber Threats and What to Do About Them." Accessed 25 December 2019. https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/.

Quigg, Michael, Juan Lopez, Mason Rice, Michael Grimaila, and Benjamin Ramsey. "Cyberspace and Organizational Structure: An Analysis of the Critical Infrastructure Environment." In *Critical Infrastructure Protection X: 10th IFIP WG 11.10 International Conference, ICCIP 2016, Arlington, VA, USA, March 14-16, 2016, Revised Selected Papers*, edited by Mason Rice and Sujeet Shenoi, 3-25. Cham, Switzerland: Springer, 2016.

Republic of Srpska National CERT RS. "About RFC 2350." Accessed 30 November 2019, https://certrs.org/en/rfc-2350/.

Ritchie, Hannah, and Roser Max. "Natural Catastrophes." Our World in Data. 2018. Accessed 26 September 2018. https://ourworldindata.org/natural-catastrophes.

Rittinghouse, John W., and Bill Hancock, *Cybersecurity Operations Handbook*. Amsterdam, the Netherlands: Elsevier Digital Press, 2003.

Schonberg, Mark R. *Defining the DOD Role in National Cybersecurity*. Carlisle Barracks PA: Center for Strategic Leadership, US Army War College, 2013. Accessed 30 November 2019. https://apps.dtic.mil/dtic/tr/fulltext/u2/a590756.pdf.

Smajic, Mirza, Sead Turcalo, and Emir Vajzovic. "Euro-Atlantic Integration of Bosnia And Herzegovina: Internal Challenges and Foreign Influences." Paper presented at Security Forum 12th Annual International Conference, Banska Bystrica, Slovakia, 2019.

Sood, Aditya K., Richard J. Enbody, and Peter Loshin. *Targeted Cyber Attacks: Multi-Staged Attacks Driven by Exploits and Malware*. Waltham, MA: Syngress, 2014.

St. Michel, Curtis, and Sarah Freeman. "Consequence-Based Resilient Architectures." In *Industrial Control Systems Security and Resiliency: Advances in Information Security*, edited by Craig G. Rieger Indrajit Ray, Quanyan Zhu, and Michael A Haney, 17-28. Vol. 75. Cham, Switzerland: Springer, 2019.

Szoldra, Paul. "Here's how the US military is beating hackers at their own game." Tech Insider. 2016. Accessed 29 November 2019. https://amp.insider.com/us-military-cyberwar-2016-5.

Taddeo, Mariarosaria. "Is Cybersecurity a Public Good?" *Minds and Machines* 29 (October 2019): 349-354. Accessed 30 December 2019. https://link.springer.com/content/pdf/10.1007/s11023-019-09507-5.pdf.

Thorley, James O. "Is Euro-Atlantic Integration of Bosnia-Herzegovina Good for the EU, NATO and Bosnia-Herzegovina Itself?" Joint Command and Staff Course of Studies, Canadian Forces College, North York, ON, 2015. Accessed 11 September 2019. https://www.cfc.forces.gc.ca/259/290/317/305/thorley.pdf.

Tiong P. Wong, "Active cyber defense: enhancing national cyber defense." Master's thesis, Naval Postgraduate School, Monterey CA, 2011. Accessed 26 September 2019, https://calhoun.nps.edu/handle/10945/10713.

Trump, Donald J. *National Cyber Strategy of the United States of America*. Washington, DC: White House, September 2018. Accessed 26 September 2019. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

U.S. Government Accountability Office. *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented: Report to Congressional Addressees*. Washington, DC: U.S. Government Accountability Office, 2013.

UK Ministry of Defense. "Defence Secretary reveals new generation of 'cyber cadets,'" September 2018. Accessed 30 December 2019. https://www.gov.uk/government/news/defence-secretary-reveals-new-generation-of-cyber-cadets.

United Kingdom Cabinet Office, *National Cyber Security Strategy 2016 to 2021*, London, UK: Her Majesty's Government, 2016), 75. Accessed 21 October 2019 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

United Nations General Assembly. Resolution 239, Creation of a Global Culture of Cybersecurity, A/RES/57/239. New York: United Nations, 2003. Accessed 25 October 2019. https://digitallibrary.un.org/record/482184/files/A_RES_57_239-EN.pdf.

US Legal, n.d. Accessed 11 November 2019. https://definitions.uslegal.com/c/cyber-warfare.

Valls, Manuel. *French National Digital Security Strategy*. Paris, France: National Cybersecurity Agency of France, 2015. Accessed 30 October 2019. https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf.

Verizon. "2019 Data Breach Investigations Report." 2019. Accessed 30 December 2019. https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf.

Wallace, Ian. "The Military Role in National Cybersecurity Governance." Brookings Institutions. December 2013. Accessed 30 December 2019. https://www.brookings.edu/opinions/the-military-role-in-national-cybersecurity-governance/.

Walter Gary Sharp, Sr. "The Past, Present and Future of Cybersecurity." *Journal of National Security Law and Policy* 4, no. 13 (2010): 13-16.

Wamala, Frederick. *ITU National Cybersecurity Strategy Guide*. Geneva, Switzerland: International Telecommunication Union, 2012. Accessed 30 October 2019. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurity StrategyGuide.pdf.

Wilshusen, Gregory C. *Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure*. Testimony Before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives. Washington, DC: U.S. Government Accountability Office, July 2011. https://www.gao.gov/assets/130/126702.pdf.

Zatolokin, Ryan, and Joe Morgan, "Cybersecurity for Critical Infrastructure," *Security Magazine*, June 2019. Accessed 13 August 2019, https://www.securitymagazine.com/articles/90268-cybersecurity-for-critical-infrastructure.