NATIONAL AND INTERNATIONAL CYBERSECURITY STRATEGIES OF THE UNITED STATES: A SECURITIZATION ATTEMPT?

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF SOCIAL SCIENCES
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY
DUYGU KÜÇÜKAYDIN

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN THE DEPARTMENT OF
INTERNATIONAL RELATIONS

JUNE 2016

Approval of the Graduate School of Social Sciences

_____

Prof. Dr. Meliha Altunışık

Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

_____

Prof. Dr. Özlem Tür

Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

_____

Assist. Prof. Dr. Tuba Ünlü Bilgiç

Supervisor

Examining Committee Members

Assoc. Prof. Dr. Bestami Sadi Bilgiç	(İpek University, IR)	_____
Assist. Prof. Dr. Tuba Ünlü Bilgiç	(METU, IR)	_____
Assist. Prof. Dr. Şerif Onur Bahçecik	(METU, IR)	_____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last name : Duygu Küçükaydın

Signature :

ABSTRACT

NATIONAL AND INTERNATIONAL CYBERSECURITY STRATEGIES OF THE UNITED STATES: A SECURITIZATION ATTEMPT?

Küçükaydın, Duygu

MS., Department of International Relations
Supervisor: Assistant Professor Dr. Tuba Ünlü Bilgiç

June 2016, 193 pages

This thesis aims to explore how cybersecurity has become a national security issue for the United States. It will analyze the issue by trying to answer the question of whether this process, which started with the Clinton Administration, is a successful 'securitization.' In this line, this thesis, firstly, tries to conceptualize the cyberspace as a new domain for international politics through examining its rise in the information age. Then, it emphasizes the major debates between cyber-pessimists and cyber-skeptics concerning the effects of cyberspace on major security concepts such as warfare, power, attack, offense-defense balance and security dilemma. In the light of this conceptualization, the thesis will try to answer the research question through concentrating on both internal and international cybersecurity strategies of the last three presidents, namely of Bill Clinton, George W. Bush and Barack Obama. At the domestic level, it analyzes securitization of the issue and the policymaking process which involves the main bureaucratic agencies of the US. At international level, it examines evolution of the bilateral and multilateral cybersecurity strategies.

Keywords: Cyberspace, Cybersecurity, National Security, the United States, Securitization

ÖZ

AMERİKA BİRLEŞİK DEVLETLERİ'NİN ULUSAL VE ULUSLARARASI SİBER GÜVENLİK STRATEJİLERİ: GÜVENLİKLEŞTİRME HAREKETİ?

Küçükaydın, Duygu

Yüksek Lisans, Uluslararası İlişkiler Bölümü
Tez Yöneticisi: Yardımcı Doçent Doktor Tuba Ünlü Bilgiç

Haziran 2016, 193 sayfa

Bu tezin amacı, siber güveliğin nasıl bir Amerikan ulusal güvenlik meselesi olarak ele alındığını incelemektir. Bu çalışma, ele aldığı dönem itibariyle, Clinton döneminde başlayan sürecin başarılı bir güvenlikleştirme hareketi olup olmadığı sorusunu cevaplamaya çalışır. Bu amaç doğrultusunda, öncelikle siber alana ait kavramlar siber alanın bilgi çağında yükselişi kapsamında incelenir. Daha sonra, siber pesimistler ve siber kuşkucular arasındaki güvenlik kavramları temelinde devam eden ana tartışmalara değinilir. Ardından bu kavramlar ışığında, üç Amerikan başkanı yönetimindeki – Clinton, Bush ve Obama- ulusal ve uluslararası siber güvenlik stratejilerine odaklanılarak tezin araştırma sorusuna cevap aranır. Ulusal düzlemde siber alanın güvenlikleştirilmesi ve politika geliştirme süreci ana bürokratik organlar dahilinde incelenir. Uluslararası düzlemde ikili ve çoklu siber güvenlik stratejilerinin gelişimi incelenir.

Anahtar Kelimeler: Siber Alan, Siber Güvenlik, Ulusal Güvenlik, Amerika Birleşik Devletleri, Güvenlikleştirme Teorisi

To Mr. Love and Jr. Love

ACKNOWLEDGEMENTS

First and foremost, I wish to express my sincere gratitude to Assistant Professor Doctor Tuba Ünlü Bilgiç. Her constructive and academic criticism helped me to conclude this thesis. I will always remember and appreciate her irreplaceable academic assistance and intellectual support for my thesis as well as her patience and kindness. In all means, without her support, writing this thesis would not have been possible.

Also, I would like to thank to examining committee members, Associate Prof. Dr. Bestami S. Bilgiç and Assistant Prof. Dr. Şerif Onur Bahçecik for their valuable contributions and comments to my thesis.

I wish to thank my friends and colleagues, particularly Nesrin Koç, Alp Eren Topal, Funda Kelahmetoğlu and Yasemin Küçükaydın for their continuous support and encouragement.

And last but not least I am heavily indebted to my family and most notably to my husband İsmail Küçükaydın for his love, patience and continuous support and contributions both spiritually and materially. Without them, this study could not have been complete.

TABLE OF CONTENTS

PLAGIARISM iii
ABSTRACT iv
ÖZ vi
DEDICATION vii
ACKNOWLEDGEMENTS viii
TABLE OF CONTENTS ix
LIST OF ABBREVIATIONS xii
CHAPTER
1 INTRODUCTION 1
1.1 The Statement of the Problem 2
1.2 Methodology 7
1.3 Organization of the Study 8
2 CYBERSPACE AND INTERNATIONAL RELATIONS: THEORY and PRACTICE 12
2.1 Broadening Concept of Security: Cybersecurity and the Copenhagen School 13
2.2 A Journey towards Cyber World 16
2.3 Cyber Optimists, Cyber Skeptics and Cyber Pessimists: Main Debates on Cyberspace and Cybersecurity 26
2.4 Capabilities in the Cyberspace: Cyber Power and Offense-Defense Balance 35
2.5 Conclusion 42
3 CLINTON ERA: YEARS OF BURGEONING 44

3.1 Introduction 44
3.2 Foreign Policy Framework of the Clinton Administration.....44
3.3 Burgeoning of Cybersecurity 49
3.3.1 Causes of Burgeoning.....50
3.3.1.1 Vulnerability and Risk Assessment of Threats to Critical Infrastructure 50
3.3.1.2 Economic Interests.....52
3.3.2 Cyber Incidents of 1990s and the 'First Cyberwar'.....56
3.4 Building-up Cybersecurity Strategy in Domestic Politics.....59
3.4.1 Role of the Department of Defense 60
3.4.2 Role of the Presidency 66
3.4.3 Role of the Legislative Efforts.....71
3.5 Building-up International Cybersecurity Strategy.....73
3.6 Conclusion.....75
4 BUSH ERA: CYBERSECURTIY IN THE SHADOW OF TERRORISM.....77
4.1 Introduction 77
4.2 Foreign Policy Framework of the Bush Administration 78
4.3 Developing Cybersecurity Strategy and Proliferation of Cyberterrorism Discourse in Domestic Politics.....81
4.3.1 Role of the Department of Homeland Security 83
4.3.2 Role of the Department of Defense 87
4.3.3 Role of the President.....94
4.3.4 Role of the Legislative Efforts.....98
4.3.5 Role of the Non-Governmental Organizations and Agencies 100
4.4 An International Attempt? 103
4.5 Conclusion.....107
5 OBAMA ERA: INCREASING EFFORTS.....109

5.1 Introduction 109
5.2 Foreign Policy Framework of the Obama Administration 110
5.3 Increasing Efforts on Enhancing National Cybersecurity Strategy 112
5.3.1 Role of the Presidency 113
5.3.2 Role of the Department of Homeland Security 125
5.3.3 Role of the Department of Defense 131
5.3.4 Role of the Legislative Efforts 135
5.4 Towards an International Cybersecurity Strategy? 142
5.4.1 US-Russia: Strategic Game under the Roof of International Organizations 148
5.4.2 US-China: A Cyber Cold War? 150
5.5 Conclusion 155
6 CONCLUSION 157
REFERENCES 163
APPENDICES
APPENDIX A: TURKISH SUMMARY 180
APPENDIX B: TEZ FOTOKOPİSİ İZİN FORMU 193

LIST OF ABBREVIATIONS

CNCI	Comprehensive National Cybersecurity Initiative
CSIS	Center for Strategic and International Studies
DoS	Denial of Service
DDoS	Distributed Denial of Service
DHS	The Department of Homeland Security
DoD	The Department of Defense
NATO	North Atlantic Treaty Organization
PDD	Presidential Decision Directive
PPD	Presidential Policy Directive
UN	The United Nations
US	The United States
USCYBERCOM	The United States Cyber Command

CHAPTER 1

INTRODUCTION

The United States (US) has been the main target of cyber intrusions with a gradually increasing level on daily basis.[1] To make it more clear, it was reported by the US General Accounting Office that number of cyber incidents reached 67,168 in 2014 with an increase of 1,121% which was almost thirteen times higher than it had been in 2006 with 5,503 cyber incidents.[2] Inspired by the ever-growing new threats from cyberspace, this thesis aims to address cybersecurity policy of the US by analyzing its response to this emerging virtual domain at national and international levels.

In the information age, the popularity of cyberspace and cybersecurity have been increasing day by day as the world gets more and more connected by the Internet based networks, software, hardware and other digital tools. Cyberspace is now an integral part of political life which affects the whole system of military, economy, intelligence, public service, and so on. Moreover, cyber domain, with its inherent actors and networks, is crucial in the digital age because it has profound impact on national welfare and influence on international arena through the use of new technologies for economic and political purposes. The effects of this growing domain may be observed

---

[1] For statistics on daily digital attacks: Norse Corp, http://map.norsecorp.com/#/ (Accessed on 28.04.2016)

[2] "Cybersecurity Actions Needed to Address Challenges Facing Federal Systems," *U.S. Government Accountability Office*, April 22, 2015, http://www.gao.gov/assets/670/669810.pdf

through vulnerability assessments, threat perceptions, and responsive security strategies of both public and private sectors of states. Therefore, information technology revolution represents another major point that affects referent objects and threats.

In accordance with the innovations brought about by the information age and the rapid evolution of cyberspace, which makes cybersecurity a vital and central problematic in security studies, this thesis will concentrate on the cybersecurity policies and strategies of the United States, and their international repercussions. The research question will be: How cybersecurity is dealt with as a national security issue in the US and what kind of measures and strategies have been developed at the domestic and international levels?

1.1 The Statement of the Problem

Security studies is quite popular within the wider discipline of international relations since it covers a wide range of thematic issues from societal to state level. Furthermore, these themes are not static, but subject to rapid change due to critical developments, which also makes it a dynamic area of research.

In the Cold War period, the international world faced multi-faceted challenges of nuclear strategy and threats coming from nuclear weapons. The end of the Cold War in 1991 and the rise of terrorism in the 2000s represent recent critical developments. In post-Cold War period, for instance, the traditional concepts of referent objects and threats have changed in that now states are not considered as the only principal referent object; there is an observed diversification of referent objects and threats. In other words, the end of the Cold War has opened a new phase which includes a new set of threats and vulnerabilities towards recently emerging actors and traditional actors. In addition to environmental, humanitarian, and economic issues, the late 1990s and the first decade of the millennium have seen the rise of terrorism or in particular war on terrorism as a central concern.

However, concerns of the era are not limited to the war on terrorism. From the 1990s onwards and especially in the second half of the 2000s, securing information and technology in the digital age, as well as sustaining security of physical space and cyberspace from cyber threats have become an important and also controversial part of security studies. Its importance stems from the claims that cyberspace has initiated a new phase in security studies with its different characteristics. In other words, it is argued that cyberspace poses particular challenges to security policy and strategy of actors with the emergence of new vulnerabilities based on cyber threats. These challenges are derived from unique characteristics of cyberspace and results of cyber attacks which are not pre-defined.

The thematic progress in the security studies, the effects of the new world order with the end of the Cold War and the impact of the ascending cyberspace on this order may be observed through the examination of policies and strategies of one of the world's leading powers, the US. In time, ever-expanding and evolving nature of cyberspace has become more and more clear in the US. To illustrate, one of the critical strategic documents of the Bush Administration *The National Strategy to Secure Cyberspace*, which was released on February 14, 2003 with the aim of identifying cyberspace and strategic objectives, admitted that:

> Our economy and national security are fully dependent upon information technology and the information infrastructure. At the core of the information infrastructure upon which we depend is the Internet, a system originally designed to share unclassified research among scientists who were assumed to be uninterested in abusing the network. It is that same The Internet that today connects millions of other computer networks making most of the nation's essential services and infrastructures work. These computer networks also

> control physical objects such as electrical transformers, trains, pipeline pumps, chemical vats, radars, and stock markets, all of which exist beyond cyberspace.[3]

Bush displayed the importance of information age by showing the critical position of the information infrastructure. In addition to presidential statements, analogies with historically critical cases like Pearl Harbor and Enigma-Ultra were used to highlight the importance of the cybersecurity. In 2008, the report of Center for Strategic and International Studies (CSIS) *Securing Cyberspace for the 44th Presidency*, which was prepared for defining the roles of the new presidents, stressed the growing concerns regarding the cyberspace by asserting:

> Many people know the story of Ultra and Enigma. Enigma was the German military encryption machine in the World War II; Ultra was the British Program to crack the German codes. The British, through a combination skill, luck and perseverance, were able to collect and decrypt sensitive German military communications and essentially become part of German military network. This gave them immense advantage and made allied success more rapid and assured. The outcome of an invisible struggle between Britain and Germany in a precursor to cyberspace gave one side an immense advantage. The United States in similar situation today, but we are not playing the role of the British. Foreign opponents, through a combination skill, luck and perseverance, were able to penetrate poorly protected US computer networks and collect immense quantities of valuable information. […] These potential opponents have not hesitated to avail themselves of the opportunities presented by poor cybersecurity. America's failure to protect cyberspace is one of the most urgent national problems facing the new administration that will take office January 2009. It is, like Ultra and Enigma, a battle fought mainly in the shadows. It is a battle we are losing.[4]

---

[3] George W. Bush, *The National Strategy to Secure Cyberspace* (Washington, DC, 2003), p.vii. https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

[4] Commission on Cybersecurity for the 44th Presidency, *Securing Cyberspace for the 44th Presidency* (Washington, DC, 2008), p.11. http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

On several occasions, Leon Panetta, Secretary of Defense of the US between July 2011 and February 2013, tried to make the US public be aware of the dangers from cyberspace by stating:

> Cyberspace is the new frontier, full of possibilities to advance security and prosperity in the 21st century. And yet, with these possibilities, also come new perils and new dangers. The Internet is open. It's highly accessible, as it should be. But that also presents a new terrain for warfare. It is a battlefield of the future where adversaries can seek to do harm to our country, to our economy, and to our citizens. […] An aggressor nation or extremist group could use these kinds of cyber tools to gain control of critical switches. They could, for example, derail passenger trains or even more dangerous, derail trains loaded with lethal chemicals. They could contaminate the water supply in major cities or shutdown the power grid across large parts of the country. The most destructive scenarios involve cyber actors launching several attacks on our critical infrastructure at one time, in combination with a physical attack on our country. Attackers could also seek to disable or degrade critical military systems and communication networks. The collective result of these kinds of attacks could be a cyber Pearl Harbor; an attack that would cause physical destruction and the loss of life. In fact, it would paralyze and shock the nation and create a new, profound sense of vulnerability.[5]

These analogies are critical in terms of defining the extent and the nature of cyber threats since threats from cyberspace are tried to be identified on the same ground with the striking cases. These analogies demonstrate how cyberspace and cybersecurity have become one of the trending topics in security studies, and how they have shaped threat perceptions of states.

In accordance with the rhetorical evolution of cybersecurity, enhancing cybersecurity and capabilities in cyberspace have been integrated into the national security strategies of the US beginning from the Clinton Administration. This thesis aims to scrutinize

---

[5] "Secretary Panetta's Speech About Cybersecurity," *Council on Foreign Relations*, 2012, http://www.cfr.org/cybersecurity/secretary-panettas-speech-cybersecurity/p29262.

responses by the American administrations to threats emanating from the virtual domain, cyberspace, targeting one of the most important actors of the international politics, the United States. Cyberspace is in the security agenda of not only the US; many other nations are gradually defining their strategies towards cyberspace.[6] However, this thesis concentrates on the US politics because of this country's dominant position in international politics as it sets primary examples for other actors to follow. In other words, it is more likely for the US to have the leading role on the issue of cybersecurity. The perspective of the US on this evolving topic will be crucial to understand the kind of national and international strategies.

Studies regarding the cyberspace cannot offer extensively rigorous argumentation rather it can be defined as provisional.[7] However, despite this nascent characteristic of cyberspace, there is a growing need to study to interpret the ongoing effects of cyberspace on national politics, to explain the strategies, and to predict future effects of the issue on the general picture of the international politics and security studies. It is critically important to explore these effects since there has emerged new pillar of power based on information, and new kinds of non-traditional threats with the inclusion of non-state actors. On the other hand, negligence about importance of cyber domain in recent international politics does not seem meaningful while cyberspace is accepted as a new domain for security studies by policymakers. While actors of international politics try to enhance their capabilities in cyberspace, underestimation of the

---

[6] Alexander Klimburg, ed., *National Cybersecurity Framework Manual* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence), pp.53-55. https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf. (Accessed on 13.11.2015)

[7] Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security* 38, no. 2 (2013), p.8.

cyberspace could create strategic vulnerabilities in security studies even if cyberspace does not bring overtly violent consequences.

This study as a hypothesis argues that the US response to increasing level of cyber threats is diversified at national and international levels in the light of a securitization move. At national level, which implies a gradual increase in the securitization move, there are more attempts to have consistent and comprehensive strategies in order to prevent or to decrease damage from cyber attacks. At international level, the level of securitization is almost non-existent because there are limited efforts for international cybersecurity strategy to keep strategic use of cyberspace at maximum.

1.2 Methodology

To illustrate effects and challenges of cyberspace, specific definitions and debates regarding the cyberspace will be examined by relying on secondary sources consisting of a selection of books and journal articles. In order to analyze evolution of cybersecurity as national security issue, mainly primary sources will be utilized. Concerning presidential attitudes and strategies, governmental documents such as hearings, bills, policy statements and other federal documents will be used. Online sources and articles from the major newspapers will also be used. They will be critical in comparing the policies and strategies of the three consecutive presidential administrations.

The research approach is the qualitative analysis of mainly the primary documents primarily. Primary documents will help to analyze strategies towards cybersecurity at bureaucratic, national and international levels starting from presidency of Bill Clinton.

In order to supplement explanatory power of the qualitative analysis of the primary documents, securitization theory of the Copenhagen School will be utilized. The securitization theory will allow interpreting the policy statements of the each presidential administration. It will make it easier to understand the evolution of

cybersecurity as a national security issue by tracing the process of labeling the referent objects, the existential threat, the speech act, the securitization move and finally the securitization, if there is an act of securitization. Moreover, with the categorization of the main concepts of securitization theory at national level, it will be consistent to compare it with the development of international cybersecurity strategies.

Regarding the qualitative analysis, a causal mechanism will be proposed between X, the cause and Y, the outcome. X in this thesis is malicious activities of various actors in cyberspace. In causal mechanism, main role belongs to the government with its entities that try to produce either offensive or defensive strategies at national and international levels. The outcome, Y, can be reached by utilizing the securitization theory. At national level, the US has applied the risk-based strategies such as imposing sanctions and developing law enforcement mechanism to take preventive measures since there is a securitization move concerning national security based on vulnerabilities. At international level, in the absence of a decisive securitization move, the US has utilized from more opportunity-based strategies to launch offensive actions and to keep its prestigious status by developing bilateral relationships with emerging cyber powers like China and Russia, and more comprehensive relations can be pinpointed within the structure of the international organizations.

Based on these assumptions, combination of the qualitative analysis of the primary documents and the securitization theory will help to serve more clear and consistent argument at national and international levels.

1.3 Organization of the Study

In order to explain the causal mechanism between malicious use of cyberspace and its effects on the US national and international strategies, this study will first present a brief introduction of the broadened security concept and the Copenhagen School and then, focus on examining position of cyberspace in the field of International Relations

(IR). Therefore, Chapter 2 proceeds with an analysis of the relationship between cyberspace and international relations. In order to be able to answer the research question of this thesis, it is necessary to begin with the concepts and the definitions of the cyberspace, as they have many differences as well as similarities when cyberspace is compared to traditional domains. In this chapter, mainly, the concepts of cyber war, cyber weapon, cyber attacks, cyber threat, and cyber power will be examined in detail along with the division of the literature on cyberspace. In the examination of main concepts, I will refer to three main points of view in literature which are cyber optimists, cyber pessimists and cyber skeptics. The division among them derives from their position on the effects of technology revolution and information technologies on politics. This chapter will help to analyze the evolution of cyberspace as a security issue for the US by indicating the critical features and main debates regarding the cyberspace.

As time constraint of this study suggests examination of presidential actions will start with the 42nd President of the United States, Bill Clinton and end up with the 44th President of the United States, Barack Obama. In the following three chapters, the evolution of cyberspace as a national security issue will be detailed along with the policies, strategies and responses towards threats emanating from cyberspace. In each of these chapters, position of cyberspace and cybersecurity in general policy framework will be analyzed for each presidential term. Then, the national and international efforts of the main bureaucratic agencies to establish cybersecurity strategy will be displayed by referring to the main concepts of the securitization theory. Critical cases of the each presidential term will be used to show their effects on growing awareness of cybersecurity.

In detail, as cybersecurity is an issue that implies strategies of military, technical and intelligence personnel of the administration it requires multilayered examination of decision-making process. In this sense, each presidential term will be examined

chronologically, in order to explain the process and results of policies and strategies of the US towards cybersecurity. But, this presidential examination will essentially involve deep insight of the position of bureaucratic agencies though presidential considerations which are generally accepted as the main determinant of strategies. Since every bureaucracy has its own subculture due to organizational system of the US, their positions should be examined one by one in each term. That is why positions and interactions of executive, military and legislative branches of government are included as critical securitizing actors. To compare and to contrast the influence of bureaucratic agencies on strategy for cybersecurity, there are two sub-questions to answer:

- What is the role of the agency on cybersecurity?
- What are the actions or the strategies of agency to secure cyberspace?

Thus, in the third chapter, as it examines the Clinton Administration as years of burgeoning of cybersecurity, the reasons behind the rise of cybersecurity during this period will be considered. In the following chapter, for Bush term, it will be shown how cybersecurity was linked with the war on terrorism. In the fifth chapter, increasing efforts of the Obama Administration will be explained as more decisive efforts for a successful securitization in order to take necessary measures concerning national security.

The last chapter, conclusion, will be based on the comparison of three presidential terms through the qualitative analysis of the primary resources and securitization theory. It will be suggested that although it was not a direct and successful securitization in the beginning, there have been effects of securitization moves regarding the paradoxes of cyberspace which offer both risks and vulnerabilities through emerging threats and opportunities as it can be used for strategic purposes. In terms of domestic cybersecurity strategies, there is a stronger securitization move as the three presidents have worked to develop some extraordinary measures by defining

existential threats and referent objects. Contrary to national line, in international domain, securitization move is weaker as it will allow the US to benefit from the strategic advantages of the cyberspace which lets actors pursue offensive actions in cyberspace to complement physical actions.

CHAPTER 2

CYBERSPACE AND INTERNATIONAL RELATIONS: THEORY and PRACTICE

Information revolution or information age has produced new terms and subjects for any field that touches upon technology. Therefore, security studies have been affected from these major developments. In this line, this chapter will start with the examination of broadened security concept and securitization theory of the Copenhagen School. Before the discussion of the main concepts of cyberspace and literature review, this chapter will first address the evolution of cyberspace in the light of the information revolution. What do we mean by the information age? What is cyberspace? What are the components of cyberspace? How does it relate with international relations and security studies? These are the four major questions that will be answered during this chapter.

Then, the available literature on cyberspace will be covered, prior to a detailed discussion of the effects of cyberspace on politics. New terminology of this new domain will allow us to underline its difference from traditional terms of war, weapons, power, attack, security and also to emphasize their similarities. This will help produce a clearer argument. Therefore, in order to analyze positions in literature and to serve a consistent argument, it is important to define the terms of cyberspace by providing its technical definition and emphasizing its significance for the security studies and from the perspective of strategy-planning and policy-making process of the US.

2.1 Broadening Concept of Security: Cybersecurity and the Copenhagen School

Security is one of the important and controversial concepts addressed by the mainstream IR theories. Defining the concept of security may require answering several questions such as: Whose security? What are the threats? What kind of measures should be taken? As the answers to these questions may change in accordance with the issue, the definition of the security may be vague. Yet, some offer a general definition of security. For instance, according to Arnold Wolfers, 'security' as an aspired value for a nation means "the absence of threats to acquired values" in an objective sense and "the absence of fear that such values will be attacked" in a subjective sense.[8] These objective and subjective nature of security are measured by the ability of nation which refers to its possessions of power. To put it differently, traditionally, security may be defined as absence of military threat which is based on the relationship between power and politics from a realist perspective. This definition was exposed to challenge with the end of the Cold War and the disappearance of the Soviet Union. It was argued that the challenge stemmed from the relatively decreasing importance of the military power and so military threat.[9] In parallel to this, non-military threats were expected to be a critical part of the security studies.[10] In addition to the new threats, it was also expected and realized that not only the states and national security will be subject of these threats, but also there will other objects. Therefore, military statecraft might not be an effective mean to achieve security.

---

[8] Arnold Wolfers, *Discord and Collaboraiton: Essays on International Politics* (Baltimore: The Johns Hopkins University Press, 1965), p.150.

[9] David A. Baldwin, "Security Studies And The End Of The Cold War," *World Politics* 48 (1995), p.118.

[10] Ibid., p.118.

The challenges to the concept of security may be observed empirically. Since the end of the Cold War, there have been many themes in security studies: economic and social problems such as industrial development and poverty, environmental degradation and global warming, international migration, health problems, terrorism, and so on. Among the broadened dimensions of security studies, cybersecurity should be inserted in the information age regarding the rapid evolution of the cyberspace.

In the field of cybersecurity, there is a discussion around theoretical stagnation which means mainstream IR theories are avoiding from the study of cyberspace as underlined by Lucas Kello.[11] In this regard, it is important to merge theory and practices to prevent the growing gap in the field of cybersecurity.[12] In doing so, securitization would offer the best framework to explain evolution of cybersecurity because realist and liberal paradigms may see cyberspace and cybersecurity as an exaggerated case.

As security issues grow in variety that threats from traditional domains should not be taken as the only security problem; it would be better to consider threats that arise from non-traditional spheres as in the case of cyberspace. In the framework of the Copenhagen School, there are different types of referent objects from five sectors that are military, political, environmental, economic and societal. This means not only the states but also identity or survival of nature could be referent objects. The widening analysis makes securitization a quite popular model within security studies.

Barry Buzan, as a prominent figure of the Securitization Model, sees security as a 'self-referential practice'. According to him, "the issue becomes a security issue through language, not necessarily because a real threat exists but because the issue is presented

---

[11] Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," p.12.

[12] Ibid., p.12.

as such a threat."[13] It means that security is not something out there; it is a result of a certain process which is defined as *speech act*.[14] Ole Weaver, another leading scholar of the Copenhagen School, explains security as "it is by labelling something a security issue that it becomes one."[15]

In its theoretical framework, for a successful securitization there are some paths to follow up which can be defined as *securitization move*. According the scholars of the Copenhagen School, at first there should be an *existential threat* that is determined and served by the *securitizing actor*.[16] There should be *referent objects* that are threatened by this existential threat. Final unit of the securitization analysis is the functional actors that are influential in the security sectors of securitization through *speech act*.[17] For instance, from the perspective of the analysis of this study, if the referent object is state, its operational capability in cyberspace is defined as the national priority by securitizing actors who are generally the political leaders and the government. Finally, to have a successful securitization, there should be measures which are defined as emergency or extraordinary against the existential threat.[18] In general, the extraordinary measures may be applied when the audience is convinced by the securitizing actor.[19]

---

[13] Barry Buzan, Ole Weaver, and Jaap De Wilde, eds., *Security: A New Framework for Analysis* (London: Lynnie Rienner Publishers, 1998), p.24.

[14] Ibid., p.26.

[15] Ole Weaver, "Aberystwyth, Paris, Copenhagen: New Schools in Security Theory and the Origins between Core and Periphery" (Montreal: ISA Conference, 2004), p.13.

[16] Buzan, Weaver, and De Wilde, *Security: A New Framework for Analysis*, p.25.

[17] Ibid., p.36.

[18] Ibid., p.26.

[19] Ibid., p.26.

For a securitizing actor, it is important to get support of the public because when he takes the extraordinary measures against existential threat, the audience should be persuaded. Therefore, for a full successful securitization a securitization move which refers to the definition of threat is important together with the persuasion of the audience.[20] In the process of convincing the audience, speech act has gained importance with the promotion of Ole Weaver. For him, security can be seen as a speech act where referent objects and existential threats are signified mostly by the promotion of securitizing actors.[21] Here, effectiveness of reports, statements of the politicians, media, news and official documents should not be ignored.

Therefore, it is helpful to analyze referent object which is tried to be secured from existential threat and role of securitizing actor by exploring speech act during the securitization move, and the measures taken to solve the security problem by using securitization theory. This perspective perfectly fits with the issue in cybersecurity since it neither denies anarchical international system nor limits existential threats by military ones. Moreover, securitization will help complement the causal chain.

2.2 A Journey towards Cyber World

Information age may be defined as inclusion of "the growing presence of certain technical devices and tools in society that allow the much more rapid communication of information and knowledge."[22] Moreover, it is also defined as a process of transition

---

[20] Ibid., p.25.

[21] Ole Weaver, "Securitization and Desecuritization," in *On Security*, ed. Ronnie D. Lipschutz (New York: Columbia University Press, 1995), p.55.

[22] Nico Stehr, "Theories of the Information Age," in *Historical Developments and Theoretical Approaches in Sociology* 2, ed. Charles Crothers (Oxford: EOLSS Publishers, 2010), p.376.

from industrial age to information age.[23] In the very beginning, it should be underlined that neither information and communication technology nor all other related networked systems –including the Internet- do not come out of a clear blue sky. It is a man-made process in its innovation and development. Once technological developments occurred, these have been disseminated in social, political, economic, cultural areas in individual level and state-level and then in global level.

How did it begin? The information revolution is associated with the promising digital technological innovations of 1960s.[24] This period started with the realization of the ARPANET (The Advanced Research Projects Agency Network) project which can be defined as the base of the Internet. In the beginning, it was a project of the US Department of Defense which was originally invented to speed up the communication within the US administration in the Cold War period with military purposes.[25] The invention and then commercialization of the Internet in 1990s have accelerated this process. Then, it continued with the integration of new innovations such as software, the Internet and finally network based critical infrastructures to digital technologies. Among all these innovative developments, today, the Internet is regarded as the key indicator of this worldwide revolution and as the main cause of cyber insecurity.[26]

What are the roles of these developments for public? The Internet as one of the main catalyzer of this revolution dates back to birth of ARPANET in 1965. Although it was

---

[23] Yannis Veneris, "Modelling the Transition from the Industrial to the Informational Revolution," *Environment and Planning A* 22, no. 3 (1990): 399–416.

[24] Emmanuel C. Lallana and Margaret N. Uy, *The Information Age* (UNDP Asia-Pacific Development Information Programme, 2003), p.5. http://www.unapcict.org/ecohub/resources/the-information-age.

[25] "The Invention of the Internet," History, http://www.history.com/topics/inventions/invention-of-the-the Internet (Accessed on 13.04.2016)

[26] Kristin M. Lord and Travis Sharp, *America's Cyber Future: Security and Prosperity in the Information Age*, Centre for a New American Security, (Washington, DC, 2011), p.20.

not a public project in its invention period, after a while, it became a common public service with the invention of 'world wide web' in the beginning of 1990s.[27] This global network is referred as a medium of communication and commerce.[28] For the US, the functioning of this digital network has vital significance in functioning of economic, military and social services.[29] For instance, a cyber attack on the military networks through the Internet can disrupt either communication or navigation systems of military.[30] Any disruption of the Internet or related infrastructures may lead a great economic cost since it is estimated that the contribution of the Internet to annual GDP is about $2 trillion according to a report of the White House in 2009.[31] Moreover, it is an inseparable part of everyday life as well as political life. It can be observed in the spread of access of the Internet which could be understood from the table below that compare and contrast the Internet access.

The advent of the Internet and transmission of it into public usage can be seen as fundamental factor that revolutionized information age. Although developed world have the advantage of technologic advances, world in total has doubled the Internet access.[32] By this way, people take the advantage of web-based services from e-learning to e-commerce. On the other hand, the growing public usage of the Internet has been

---

[27] Klimburg, *National Cybersecurity Framework Manual*, p.2.

[28] Lallana and Uy, *The Information Age*, p.9.

[29] Lord and Sharp, *America's Cyber Future: Security and Prosperity in the Information Age*, p.7.

[30] Ibid., p.7.

[31] Executive Office Of The President Council, National Economic Policy, Office Of Science And Technology, *A Strategy For American Innovation: Driving Towards Sustainable Growth And Quality Jobs*, 2009, p.5, https://www.whitehouse.gov/sites/default/files/microsites/ostp/innovation-whitepaper.pdf.

[32] International Telecommunication Union, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx (Accessed on 15.05.2016)

increasing the variety of actors. In other words, widespread use of the Internet means that your adversary can be a teenager or a housewife as well as more familiar actors of IR. The variety of actors and widespread of use of the Internet make more and more people available to pursue an attack in cyberspace. With all these factors, cyberspace became a popular term.

Cyberspace which does not have constant and universal definition may be seen as an umbrella term that imposes new features to traditional concepts such as power, attack, threat, and security. At first glance, terms include *cyber*- prefix looks like as parts of a science-fiction book or a science-fiction movie for many. But, it is not a delusion. Cyberspace is popularized within the stories and books of an American-Canadian novelist, William Gibson.[33] However, although origin of the term favors this standing, currently it is a vital part of everyday life as well as political life. As it is open to daily observation, almost everybody is able to access and to use these technologies. Appearance of cyberspace in popular novels and emphasis on digital revolution and cyber domain in several Hollywood movies and TV-series are good examples of its acceptance in daily life.

As it does not have a common definition, there can be slightly different definitions of cyberspace either by limiting it to computers and the Internet networks or by expanding it beyond digital technologies. For many organizations and scholars there are only three main components of cyberspace which are computer networks, the Internet and critical infrastructures. Lucas Kello defines cyberspace by separating three related parts which are the Internet, the world wide web, and cyber archipelago which includes computer

---

[33] "Cyberspace," http://techterms.com/definition/cyberspace; Thomas Jones, "William Gibson: Beyond Cyberspace," *The Guardian*, September 21, 2011, http://www.theguardian.com/books/2011/sep/22/william-gibson-beyond-cyberspace.

systems.[34] As an example to organizations, International Telecommunication Union (ITU) defines cyberspace as "systems and services connected either directly to or indirectly to the Internet, telecommunications and computer networks."[35] Even this limited definition causes a ground for new vulnerabilities. In this line, it emphasizes cyberspace as a critical component of national security since malicious use of cyberspace could cause wide range of security breaches for a state.[36]

Cyberspace is also defined as "an operational domain, characterized by the use of electronics and electromagnetic spectrum to create, store, modify, and exchange information via networked information systems and associated physical infrastructures."[37] The linkage with national security and its operational characteristics lead one of the main security authorities of the US, the Department of Defense (the DoD) to define cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processes and controllers."[38] The relatively broad definition of the DoD may be widened as follows:

---

[34] Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," p.17.

[35] "ITU National Cybersecurity Strategy Guide," *International Telecommunication Union* (Geneva, 2011), p.5. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf.

[36] Ibid., p.5.

[37] Franklin D. Kramer and Larry K. Wentz, "Cyber Influence and International Security," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Virginia: Potomac Books, Inc., 2009), p.344.

[38] Joint Chief of Staff, *The National Military Strategy for Cyber Operations* (Washington, DC, 2006), p.ix. http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf.

> More ecosystem than machine, cyberspace is a bioelectronics environment that is literally universal, it exists everywhere there are telephone vires, coaxial cables, fiber-optic lines or electromagnetic waves. This environment is "inhabited" by knowledge, including incorrect ideas, existing in electronic form. It is connected to the physical environment by portals which allow people to see what's inside, to put knowledge in, to alter it, and to take knowledge out. Some of these portals are one-way (e.g. television receivers and television transmitters); others are two-way (e.g. telephones, computer modems). […] The key is software, a special form of electronic knowledge that allows people to navigate through the cyberspace environment and make its contents understandable to the human senses in the form of written language, pictures and sound. People are adding to cyberspace -- creating it, defining it, expanding it -- at a rate that is already explosive and getting faster. Faster computers, cheaper means of electronic storage, improved software and more capable communications channels (satellites, fiber-optic lines) -- each of these factors independently adds to cyberspace. But the real explosion comes from the combination of all of them, working together in ways we still do not understand.[39]

As this research deals with the cybersecurity strategies of the US, this thesis will accordingly use this broad definition of cyberspace. In other words, cyberspace in this thesis has also a broad meaning because the national security of the US is not only threatened by 'online' attacks that come from computers connected to the Internet. According to this detailed definition, any strategy for cybersecurity may stem from vulnerabilities of any component of cyberspace.

In addition to definitions of cyberspace, significant characteristics of cyberspace should be explored in depth by comparing and contrasting its characteristics with those of traditional domain because the adaptation to the information age creates a paradox regarding the cyberspace. The paradox implies that increasing dependency upon digital technologies via high-speed communication networks, the Internet, and all other

---

[39] Esther Dyson, "Cyberspace and the American Dream: A Magna Carta for the Knowledge Age," *The Information Society* 12, no. 3 (1994), p.296.

networked systems presents an increasing level of vulnerabilities. November of 1988 could be accepted as one of the turning point for cybersecurity timeline to observe and to predict vulnerabilities since it is the time of discovery of a computer worm, Morris, which is called by its launcher Robert Morris, a graduate student. Although this worm does not have a malicious intention,[40] uncontrolled spread and disruptive impact of the worm on several systems due to bugs in the code demonstrated how these types of attacks would damage operation of systems with its unique characteristics.

One of the prominent scholars of cyber politics, Nazli Chouchri, Professor of Political Science at Massachusetts Institute of Technology, points out seven features of cyberspace which are *temporality, physicality, permeation, fluidity, participation, attribution* and *accountability*.[41] Temporality in cyberspace means that actions take place 'near instantaneity' other than 'conventional temporality'.[42] Physicality refers to performing over the geographical and physical location.[43] Permeation means "penetrating boundaries and jurisdictions" while fluidity means "sustaining shifts and reconfigurations."[44] These characteristics are accompanied by attribution and accountability which together reduce the responsibility for an action in cyberspace through unauthenticated acts.[45] All these differentiate cyberspace from other domains – air, land and sea-.

---

[40] Larry Seltzer, "The Morris Worm: The Internet Malware Turns 25," *ZDNet*, 2013, http://www.zdnet.com/article/the-morris-worm-the Internet-malware-turns-25/.

[41] Nazli Choucri, "Co-Evolution of Cyberspace and International Relations : New Challenges for the Social Sciences, " (Montreal: World Science Forum, 2013), p.3.

[42] Ibid., p.3.

[43] Ibid., p.3.

[44] Ibid., p.3.

[45] Ibid., p.3.

These are the driving factors that distinguish cyberspace from traditional domains which is not prone to instantaneous changes and attacks in a geographically bordered sovereignty with responsibility and easier identification of more akin actors in case of a conflict. To put it differently, cyberspace is a new domain that is beyond sovereignty and control of political and physical boundaries of states in contrast to air, land and sea.[46] When compared to traditional spheres, the most distinctive features of cyberspace that set this virtual domain apart from real world are its dark side of attribution of actions and rapidity. The DoD, from a military perspective, also classifies the key features of cyberspace as *man-made domain, technical innovation, volatility, information movement, and speed*.[47] Technical innovation and man-made domain refer to the dynamic characteristics of the cyberspace which require 'more comprehensive response to extraordinary incidents' with a continuing effort.[48] Similar to physicality, information movement also means the characteristics of cyber incidents which are beyond boundaries of states.[49] Volatility anticipates operations in cyberspace to be less effective due to the instantaneous changes in the domain whereas speed of cyber attacks makes them more valuable in terms of effectiveness.[50] These characteristics mean that cyber attacks and threats are beyond physicality thanks to its speed, and it is very easy to attack since the relative cost is very low due to low barriers of entry and attribution problem that prevent to identify the attacker. Furthermore, it could be said

---

[46] Franz-Stefan Gady and Greg Austin, *Russia, The United States, and Cyber Diplomacy: Opening the Doors* (New York, 2010), p.1. http://www2.ewi.info/sites/default/files/ideas-files/USRussiaCyber_WEB.pdf.

[47] Joint Chief of Staff, *The National Military Strategy for Cyber Operations*, p.4.

[48] Ibid., p.4.

[49] Ibid., p.4.

[50] Ibid., p.4.

that these features make states and non-state actors equal in entry and in identification by offering both of them the grey zone which is stemmed from the attribution problem.

These different and unique characteristics of cyberspace are generally based on its man-made structure which makes it very open to rapid changes. Gregory Rattray as a part of military wing argues that:

> Cyberspace is unique in that the interactions are governed by hardware and software that is manmade, so the "geography" of cyberspace is much more mutable than other environments. Mountains and oceans are hard to move, but portions of cyberspace can be turned on and off with the flick of a switch; they can be created or "moved" by insertion of new coded instructions in a router or switch.[51]

Nonetheless, we can see a great similarity with traditional spheres in addition to all these relatively new characteristics of cyber domain. It may be argued that anarchical nature of the politics in cyberspace does not change since there is still no higher authority. Moreover, there is growing level of uncertainty due to attribution problem which means the authentication of the aggressor is almost impossible in cyberspace. It also prevents development of any direct punishment and enforcement mechanism. The anarchical nature of cyberspace and uncertainty require the examination of the relationship between national security and cyberspace.

Myriam Dunn Cavelty and Elgin M. Brunner who are the important scholars in the field of cybersecurity argue that information revolution makes the information strategically important and brings the issue of vulnerabilities, particularly of critical

---

[51] Gregory Rattray, "An Environmental Approach to Understanding Cyberpower," in *Cyberpower and National Security*, ed. Franklin D. Kramer and Stuart H. Starr (Virginia: Potomac Books, Inc., 2009), p.256.

infrastructures due to the characteristics of the new domain.[52] They also set the relationship between national security and information revolution by asserting dependence of critical infrastructures of economy, military and civilians on the information infrastructure.[53] Therefore, they emphasize on the changes in the dimensions of the 'networked security' when compared to conventional national security. The emphasis is mainly on the varied actors in cyberspace together with the extra-territorial characteristics of the emerging threats in cyberspace. Firstly, the actors in cyber domain are more diversified which means they are not limited by nation-states, but also non-state actors utilize from cyberspace.[54] Secondly, security threats of cyberspace are beyond sovereign boundaries of nation-states, so they are not only understood territorially, but also extra-territorially.[55] With respect to these changes and characteristics, it may be understood that security practices of states regarding cyberspace may be different from traditional domains. This is mainly stemmed from actors' variety including states and non-states and extraterritoriality in a networked anarchical system.

The rapid evolution of cyberspace and emergence of its unique characteristics have affected the world globally. This effect may be mainly observed through examining the security agenda of states and the debate on literature which is based on these differences and similarities between cyberspace and traditional domains.

---

[52] Myriam Dunn Cavelty and Elgin M. Brunner, "Introduction: Information, Power and Security- An Outline of Debates and Implications," in *Power and Security in the Information Age : Investigating the Role of the State in Cyberspace*, ed. Myriam Dunn Cavelty, Victor Mauer, and Sai Felicia Krishna-Hensel (Hampshire: Ashgate, 2007), p.11.

[53] Ibid., p.11.

[54] Ibid., p.56.

[55] Ibid., p.56.

2.3 Cyber Optimists, Cyber Skeptics and Cyber Pessimists: Main Debates on Cyberspace and Cybersecurity

The available literature on cyber peril can be divided into three main categories as cyber optimists, cyber skeptics and cyber pessimists. The reason of this division lies in positive, neutral and negative interpretations of the impact of the digital revolution on international politics. Probability and effectiveness of cyber war, results of the cyber attacks, and functionality of cyber weapons are the main themes that cause controversy between skeptics and pessimists.

Cyber optimists whose emphasis is more on liberal effects of cyberspace may be distinguished from the main debate between skeptics and pessimists who have controversial arguments about its effects. Even though this thesis mainly focuses on the discussion among pessimists and skeptics from security perspective, primary arguments of cyber-optimists will also be explained briefly. Cyber optimists mainly deal with the democratic characteristics of cyberspace such as freedom, transparency, flow of information, which are all promoted by the technology revolution, in particular with the rise of the Internet.[56] These are also reasons of their optimism since they create positive political impact on societies and states. For instance, Michael Margolis and David K. Resnick claim that "the Internet might facilitate the particular style of democratic politics favored by activists, a style that, unlike that of traditional political parties, does not concentrate on voting and elections."[57] Very similar to this argument, Richard Davis argues that the Internet as an important communication tool uphold 'public input

---

[56] Adrian Athique, *Digital Media and Society: An Introduction* (Cambridge: Polity Press, 2013); Manuel R. Torres Soriano, "The Internet as a Driver of Political Change: Cyber-Pessimists and Cyber-Optimists," *Revista Del Instituto Español de Estudios Estratégicos* 1 (2013): 332–52.

[57] Michael Margolis and David K. Resnick, *Politics as Usual: The Cyberspace `Revolution'* (London: SAGE Publications Inc., 2000), p.17.

and direct democracy'.[58] The revolutions that are promoted by the use of digital tools as in the case of the Arab Spring are the main empirical evidence of positive impact for optimists.[59]

Yet the main debate stems from the division between the cyber skeptics and cyber pessimists. A group of scholars in literature that can be named as cyber skeptics claims that almost nothing has changed with the technology revolution.[60] They try to show exaggeration of the security of the cyber domain mainly on warfare, on security, and thus on international politics.

Means of war and the impact of cyberspace on traditional warfare are the central issues between the skeptics and pessimists. Although cyberspace is taken into account as a new domain of warfare mainly by pessimists[61], cyber skeptics ignore the effects of cyberspace on war.[62] Thomas Rid is one of the main representatives of skepticism. His perspective is based on the impossibility of cyber war which lacks criteria of war that is developed by Carl von Clausewitz in his popular work *On War*. For Clausewitz, there are three main criteria of war which are its violent character, its instrumentality and its political nature, and there are no major cyber incidents that meet these criteria

---

[58] Richard Davis, *The Web of Politics: The Internet's Impact on the American Political System* (New York: Oxford University Press, 1999), p.175.

[59] Torres Soriano, "Internet as a Driver of Political Change: Cyber-Pessimists and Cyber-Optimists"; William Dutton, *Society on the Line: Information Politics in the Digital Age:* (Oxford University Press, 1999).; European Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, (Brussels: 2013), http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf.

[60] Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," pp.9-12.

[61] Andrea Locatelli, *The Offense/ Defense Balance in Cyberspace* (Milano, 2013), http://www.ispionline.it/sites/default/files/pubblicazioni/analysis_203_2013.pdf.

[62] Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," p.10.

together.[63] Based upon lack of these criteria and an empirical example of an act which may be called as cyber war, Rid underlines the improbability of cyber war.[64] Erik Gartzke also joins in this argument by touching upon temporary and short-term characteristics of damage in cyberwarfare, so that the inability of the cyber weapons as instruments to finalize a political action.[65] Adam Liff who tries to figure out capabilities of cyber weapons concludes that they will not change the rules of the game since they could not be classified as absolute weapons.[66] In other words, although skeptics do not ignore the existence and increasing usage of cyber weapons, for them these weapons can only be used to weaken an economic or military system through sabotage; to weaken the authority or order by subversion; to gather secret information like espionage.[67] None of them carry out the characteristics and criteria of Clausewitzian framework of war, so that the skeptics downgrade the cyber danger. Furthermore, all the skeptics may provide their arguments by arguing that as yet, there have been no major cases of cyber war which could be called as 'war'. Both Rid and Gartzke argue that neither the structure of warfare nor the effectiveness conventional attacks during war is transformed with the rise of the weapons from cyberspace. In other words, even if cyber attacks may bring the expected political results, they will not

---

[63] Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012), pp.7-8.;Thomas Rid, "Cyberwar and Peace," *Foreign Affairs*, 2013, https://www.foreignaffairs.org/articles/2013-10-15/cyberwar-and-peace.

[64] Rid, "Cyber War Will Not Take Place," p.10.

[65] Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38, no. 2 (2013), p.57.

[66] Adam P. Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," *Journal of Strategic Studies* 35, no. 3 (June 29, 2012), p.426.

[67] Rid, "Cyber War Will Not Take Place," pp.16-27.

be able to substitute conventional weapons or conventional warfare.[68] As they are skeptical about the extent of the cyber danger, it could be said that skeptics do not expect changes in security strategies of actors. Contrary to skeptics, pessimists emphasize the possible challenges on political behavior of actors and on security studies caused by the rise of the cyberspace.

Cyber pessimists are generally aware of the effects of cyber weapons on warfare, and they attract attention to the dangers from cyber attacks.[69] Lucas Kello and Nazli Choucri as members of Exploration in Cyber International Relations (ECIR) at Massachusetts Institute of Technology (MIT) considered as the leading scholars of the pessimist side since they mainly underline the influence of the cyberspace on international politics and so on international security. For instance, Kello accepts the effects of cyber weapons on war, however, by arguing that unique characteristics of cyber weapons and cyber attacks need to be interpreted differently from traditional Clausewitzian framework of war.[70]

Cyber attack can simply be defined as use of malicious codes against any types of electronic or networked systems by wide range of actors including individuals, groups, states, and non-state actors to any of these varied actors through different motivations.[71] These attacks may turn into a cyber conflict or a cyber war which is defined as "the unauthorized penetration by, on behalf of, or in support of, a government into another nation's computer or network, or any other activity affecting a computer system, in which the purpose is to add, alter, or falsify data, or cause the disruption of or damage

---

[68] Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," p.63.

[69] Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," p.23.

[70] Ibid., p.22.

[71] Ibid., p.19.

to a computer, or network device, or the objects a computer system controls[72]" as a broader version, but it does not necessarily mean that all cyber attacks turns into cyber war.

Attacks in cyberspace are not unique. They can be classified in terms of their vulnerabilities and scale. Moreover, there are many ways in cyberspace to attack or to disturb your opponent therefore there is no single and definite tool used as cyber weapons. There are many ways to attack in cyberspace by using various cyber weapons including denial of service, malware, website defacement.[73] Web defacement aims to change the website which may cause a disruption in activities of the website.[74] Malwares such as viruses, worms, spywares and Trojans that are almost familiar to everyone who uses communication technologies are generally designed for exploitation of data.[75] Denials of Service (DoS) and more seriously Distributed Denials of Service (DDoS) that originates from various locations are more comprehensive type of web defacement which tries to prevent access to networked-system by controlling malware which is used to attack.[76] In addition to cyber attack, there are also other types of offensive activities such as cyber exploitation, cyber espionage, and cyber sabotage.

---

[72] Richard A. Clarke and Robert K. Knake, *Cyber War : The Next Threat to National Security and What to Do About It* (New York: Ecco, 2010), p.227.

[73] Thiong Pern Wong, "Active Cyber Defense: Enhancing National Cyber Defense" (Naval Postgraduate School, 2011), http://calhoun.nps.edu/bitstream/handle/10945/10713/11Dec%255FWong%255FT.pdf?sequence=1. (Accessed on 29.06.2015)

[74] Ibid.; "FBI Warns of Fake Govt Sites, ISIS Defacements," *Krebs on Security*, http://krebsonsecurity.com/2015/04/fbi-warns-of-fake-govt-sites-isis-defacements/.(Accessed on 29.06.2015)

[75] "Glossary," *McAfee*, http://home.mcafee.com/virusinfo/glossary. (Accessed on 29.06.2015)

[76] Wong, "Active Cyber Defense: Enhancing National Cyber Defense.";"Denial of Service (DoS)," *Trend Micro*, http://www.trendmicro.com/vinfo/us/security/definition/denial-of-service-dos. (Accessed on 29.06.2015)

Cyber exploitation is defined as "penetration of an adversary's computer system for the purpose of exfiltrating data."[77] Cyber espionage is a type of cyber exploitation which intends to penetrate the system to capture strategic political, military or economic information.[78] Cyber sabotage is "a deliberate attempt to weaken or destroy an economic or military system."[79] For pessimists, all these offensive activities from cyberspace pose serious threats for national security even though there is no critical example of cyber war.[80]

All of the cases of cyber incidents (e.g., the DDoS attacks in Estonia in 2007, disruption of Georgian computer systems during Russian-Georgian war of 2008, and Stuxnet worm on Natanz nuclear facility in Iran[81]) are categorized as either cyber attacks or as other types of offensive cyber actions. From the perspective of skeptics, these actions do not have striking points in terms of national and international security because it is argued that cyber attacks have only limited and indirect instrumentality in actualizing political goals.[82] In other words, attacks from cyberspace can be effective only if they are supplemented by conventional attacks to create a long-term physical damage especially on physical space.[83] However, it should be noted that effects of cyber attacks are not limited by indirect damage.

---

[77] Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," p.20.

[78] Ibid., p.20.; Nadav Morag, *Cybercrime, Cyberespionage, and Cybersabotage: Understanding Emerging Threats* (Colorado, 2014), http://www.coloradotech.edu/~/media/CTU/Files/ThoughtLeadership/cybercrime-white-paper.ashx.

[79] Rid, "Cyber War Will Not Take Place," p.16.

[80] Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," p.22.

[81] Ibid., p.22.

[82] Rid, "Cyber War Will Not Take Place," p.22.

[83] Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," p.59.

Cyber pessimists underline the direct and the indirect effects of cyber attacks in order to show the significance of cyber attacks. One can observe the direct effects of cyber attacks easily on the target machine or network, while indirect effects may be observed in the system that is composed of these machines or networks.[84] It means that the effects of cyber attacks are not limited to cause damage on cyberspace. They can cause economic, social and other damage in facilities like electric grid or nuclear power[85] which increases the need to enhance national security of critical infrastructures. In this line, pessimists speculatively urge on hazardous results and damage from cyber attacks for example in case of destroying one of the main critical infrastructures of a nation like power grid of electricity.[86] For them, this is another example of indirect effects since it generates feeling of national insecurity. Therefore, in addition to the problem of protection of critical infrastructure, there is also problem of feeling of insecurity which interpreted as indirect psychological consequence of cyber attacks.[87]

Together with the direct and indirect effects of cyber attacks, some of the distinctive features of cyber attacks and cyber weapons make them more striking in terms of security for cyber pessimists. Cyber weapons can be defined as arms and instruments of cyber domain that causes non-kinetic disruption on adversary's systems by decreasing its operational capability.[88] It can be argued that particularly remote and speed attacks

---

[84] Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," p.19.

[85] Ibid., p.19. ; Herbert Lin, "Joining Cybercrime and Cyberterrorism: A Likely Scenario," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Washington: Georgetown University Press, 2012), pp.57–68.

[86] Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," p.23. ; Richard Clarke, "War From Cyberspace," *National Interest*, no. November/December (2009): 31–37.

[87] Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," p.23.

[88] James P. Farwell and Rafal Rohozinski, "The New Reality of Cyber War," *Survival* 54, no. 4 (2012): 107–20.

in cyber domain by these new weapons differs them from conventional attacks.[89] These are caused by the characteristics of physicality, temporality and attribution of cyberspace as they are identified by Choucri. In terms of physicality, the geographical distance and physical barriers do not matter to operate capabilities in cyberspace.[90] In terms of temporality and attribution, a few seconds is enough to attack your target in cyberspace without the risk of identification.[91] These are the main features of cyber attacks that bring about new strategic security challenges for states since they enable wide range of actors to pursue offensive activities in cyberspace.

Similar to cyber attacks, the most important feature of cyber weapons is their relatively lower cost. This enables non-state actors as well as states to pursue cyber attacks as the participation characteristics of cyberspace suggest. Furthermore, relatively cheaper costs of cyber weapons and their undiscovered nature also call for new strategies and policies for states.

However, the cruciality of these features is not agreed upon by skeptics. Instead, they result in controversial interpretations in terms of cyber attacks. For skeptics, neither attribution problem nor low level of entry barrier do not bring any challenges for states since they still have plenty of offensive and defensive capabilities even in cyber domain compared to relatively weaker actors.[92] That is because cyber attacks and cyber weapons can be effective only at strategic and tactical level which may be used to

---

[89] Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," pp.410-416.

[90] Ibid., pp.410-416.

[91] Ibid., pp.410-416.

[92] Ibid., pp.410-416.

complement any action in traditional domains rather than pursuing a pure war at cyber domain, so that they do not transform the nature of conventional attacks and weapons.[93]

In short, for the skeptics, cyber attack, by its very nature, is generally used to refer offensive activities which do not directly cause deadly and bloody results among the networks and computer systems of actors of the cyberspace unlike in the cases of conventional warfare. In terms of cyber war, it should be noted that there is not yet a critical example like the examples of conventional acts of wars as the world has experienced by the World Wars. This makes the argument of skeptics stronger compared to pessimists. However, even on daily basis there are increasing numbers of cyber incidents that are more identical with cyber attacks which uphold cyber pessimists' arguments.

All in all, based on comparison between the Clausewitzian nature of conventional warfare and new characteristics of cyber war and empirical evidence, skeptics indicate that 'there is no example of cyber war' and 'cyber war will not take place.'[94] On the other hand, pessimists advise caution about the cyber danger by underlining the possible and observable characteristics and effects of cyber attacks and cyber weapons. Moreover, in order to point out significance of the issue, most of the scholars from pessimist side try to build analogy with the search for strategies for new capabilities and new threats in the first stages of development of nuclear weapons.[95] They suggest

---

[93] Ibid., pp.410-416.

[94] Rid, "Cyber War Will Not Take Place"; Rid, "Cyberwar and Peace"; Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth"; Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War."

[95] Clarke, "War From Cyberspace," p.31. ; Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," p.14.

that lack of strategies due to freshness of the capabilities and threats could increase vulnerabilities, so that cyber danger should not be ignored.[96]

Comparison proves to be helpful in analyzing and in classification however comparison should not be converted to reductionism. In this debate, it should repeatedly be underlined that cyberspace has different characteristics when it is compared to air, land and sea as a domain. In this line, review of the literature indicates that there is a sharper distinction between arguments of cyber skeptics and cyber pessimists than arguments of cyber optimists and cyber pessimists. As a result, the disagreements between skeptics and pessimists bring about a central debate by two main interlinked points. First point is current improbability of cyberwar as skeptics argue lead the actors for downgrading the risk of vulnerabilities in cyberspace without searching for new strategies rather concentrating on opportunity-based strategies. Second point is based on the arguments of pessimists by claiming that new threats and vulnerabilities from cyberspace call for new strategies which may be defined as risk-based strategies. In this regard, the debate relies on these points can be seen highly effective in strategy planning process of the US.

2.4 Capabilities in the Cyberspace: Cyber Power and Offense-Defense Balance

As cyberspace offers new types of attacks which are based on new capabilities of the domain, the significance of cyber attacks should be examined through analyzing their impact on power and offense-defense balance, and also on international anarchy and security dilemma in order to explore the issue from security perspective.

Cyber power and capabilities in cyberspace may help to explain the ongoing security strategies of the United States. Power which is measured either relatively or absolutely

---

[96] Clarke, "War From Cyberspace"; Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft."

is the main indicator of capabilities of a state according to realists.[97] Capabilities of state are the main determinant of their security in international politics.[98] While economic, military and political power is described as the main subtitles to measure power in politics according to traditional IR theories, informational resources on sources of power has been rapidly gaining more importance.[99] Rise of technology makes information and knowledge more valuable and vice-versa, so that, in this day and age, information and related technologies which are the basis of cyber power are taken into account as a new medium of power.

One of the prominent IR scholars, Joseph Nye who developed the popular term soft power is interested in cyber power in time of information revolution. Nye positions himself by neither ignoring the rise of importance of cyber power nor accepting the changes in geographical space.[100] Similar to conventional power definition of Nye, cyber power is defined as "the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain."[101] Nye's cyber power definition "rests upon a set of resources that relate to the creation, control

---

[97] Charles L. Glaser and Chairn Kaufmann, "What Is the Offense-Defense Balance and How Can We Measure It?," *International Security* 22, no. 4 (1998), p.2.

[98] Ibid., p.3.

[99] Myriam A. Dunn, "Securing the Digital Age: The Challenges of Complexity for Critical Infrastructure Protection and IR Theory," in *International Relations and Security in the Digital Age*, ed. Johan Eriksson and Giampiero Giacomello (Oxon: Routledge, 2007), pp.89-90.; Myriam Dunn Cavelty and Elgin M. Brunner, "Introduction: Information, Power and Security- An Outline of Debates and Implications," in *Power and Security in the Information Age : Investigating the Role of the State in Cyberspace*, ed. Myriam Dunn Cavelty, Victor Mauer, and Sai Felicia Krishna-Hensel (Hampshire: Ashgate, 2007), p.8.;David J. Rothkopf, "Cyberpolitik: The Changing Nature of Power in the Information Age.," *Journal of International Affairs* 51, no. 2 (1998): 325–59.

[100] Joseph S Nye Jr, "Cyber Power," 2010, p.3. http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.

[101] Ibid., pp. 3-5.

and communication of electronic and computer based information –infrastructure, networks, soft-ware, human skills."[102]

Starting from this point of view, it may be asked that whether states have still the ultimate power in cyberspace or their supremacy is shaken. Answer to this question is based on two consequential and interlinked effects of cyberspace and cyber power. At first, due to the changing nature of power, resources of power imply growing significance of information technologies and resources.[103] This means that power of informational resources increases the capability to control traditional resources of power – military forces and economic productivity-.[104]

Secondly, as the nature of power is changing in the direction towards cyber power, this implies critical results for the distribution of power[105] since the entry barrier is relatively low, and the cost of having cyber weapons is relatively cheap[106]. This also means that there is wide range of actors in cyberspace that could have the same capabilities with states on the one hand,[107] and could have relatively low vulnerabilities than states on the other hand.

---

[102] Ibid., p.3.

[103] Myriam Dunn Cavelty, "Is Anything Ever New?- Exploring the Specifities of Security and Governance in the Information Age," in *Power and Security in the Information Age : Investigating the Role of the State in Cyberspace*, ed. Myriam Dunn Cavelty, Victor Mauer, and Sai Felicia Krishna-Hensel (Hampshire: Ashgate, 2007), p.29.

[104] Ibid., p.29.

[105] Ibid., p.29.

[106] Nye, "Cyber Power," p.4.

[107] Dunn Cavelty, "Is Anything Ever New?- Exploring the Specifities of Security and Governance in the Information Age," p.29. ; Derek S. Reveron, "An Introduction to National Security and Cyberspace," in *Cyberspace and National Security: Threats Opportunities and Power in a Virtual World*, ed. Derek S. Reveron (Washington, DC: Georgetown University Press, 2012).

The changing nature of the power and the distribution of power in cyberspace bring the contradictive issues of asymmetric power and asymmetric vulnerabilities. This discussion derives from the assumption of relatively weak actors are getting more powerful while strong actors are getting more vulnerable since they are more dependent on operational cyberspace.[108] In other words, it is claimed that cyber domain produces more serious threats for high-tech dependent West rather than rouge states or insurgency movements.[109] From this point, together with the low cost and entry barriers, cyber domain seems like more beneficial for non-state actors and weaker states whose dependency on operational cyberspace is relatively low.

In terms of vulnerabilities, the rising level of individual access to the Internet is vital. As it is widely known many of the economic, social, and technical actions of a state have been oriented by the Internet or by other networks. For instance, control systems for airplanes, trains, natural gas pipelines and software, commercial web-based supply chains, and financial transactions and networked banking systems are all tied to the Internet.[110] Contrary to the technological dependence of the states, neither individuals nor non-state actors have to protect such critical infrastructures or critical sectors. "Their major vulnerability is to legal and illegal coercion by governments and organizations if they are apprehended…"[111] Moreover, Nye states that:

> While a few states like the United States, Russia, Britain, France, and China are reputed to have greater capacity than others, it makes little sense to speak of

---

[108] Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (2013), p.375.

[109] Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," p.64.

[110] Fred H. Cate, "China and Information Security Threats: Policy Responses in the United States," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (New York: Oxford University Press, 2015), p.300.

[111] Nye, "Cyber Power," p.13.

> dominance in cyber space as in sea power or air power. If anything, dependence on complex cyber systems for support of military and economic activities creates new vulnerabilities in large states that can be exploited by non-state actors.[112]

This can be described as one of the strategic challenges posed by cyber power.[113] But, Lindsay argues that these high-tech systems cannot be threatened by non-state actors since invention of the system depend upon the skills and professionalism on engineering and intelligence preparation.[114] Therefore, one cannot speak of asymmetric power in cyber domain.[115] Liff also joins this argument by adding that as the weaker actors are getting stronger, they will rely more on the strategy of deterrence rather than using its capability against strong one.[116] Based on these claims, for this group there is no asymmetric power which will increase the risk for war.

Although the assumptions of asymmetric power and asymmetric vulnerabilities are downplayed through rational inferences mainly by skeptical point of view, states -as still the major powers of international politics- could not ignore security dilemma in a more anarchical cyber domain due to higher level of uncertainty. In addition to the high level of uncertainty under the assumption of growing level of asymmetry, another

---

[112] Ibid., p.4.

[113] Paul Cornish, *The Vulnerabilities of Developed States to Economic Cyber Warfare* (London, 2011), https://www.chathamhouse.org/sites/files/chathamhouse/0611wp_cornish.pdf.

[114] Lindsay, "Stuxnet and the Limits of Cyber Warfare," p.385.

[115] Ibid., p.385.; Tim Maurer, "The Case for Cyberwarfare," *Foreign Policy*, October 19, 2011, http://foreignpolicy.com/2011/10/19/the-case-for-cyberwarfare/

[116] Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," pp.411-12.; Lindsay, "Stuxnet and the Limits of Cyber Warfare," p.376.; Clarke, "War From Cyberspace," p.32.; Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," pp.27-29.

aspect that increases the security dilemma in cyberspace is the controversial nature of the offense-defense balance.

According to offense-defense theorists, if defense is superior to offense and if there is arms control, war can be avoided.[117] However, different characteristics of cyberspace mainly physicality, temporality, attribution and accountability may prevent making straightforward inferences about the offense-defense balance. These two main arguments of the offense-defense theory do not seem directly applicable in cyberspace. Therefore, it is not easy to assume if defense is easier, states choose defensive strategies or if offense is the convenient way to be secure, states choose escalatory politics by offensive actions.

For many, cyberspace is claimed as an offense dominant domain where arms control almost impossible due to lower cost of weaponization and attribution problem.[118] The variables of this debate can be named as vulnerabilities, attribution problem, unpredictability of offense, and complexity of defense.[119] Variety of actors should also be added as an important variable in shaping of this balance since cyber threats do not only come from states, but also from extremist groups such as terrorist organizations or other illegal groups or individuals.

Technical reasons behind this may be seen as the rapid developments in offensive capabilities vs. slower improvements in defensive capabilities. In addition, the lack of possibility to repulse all attacks in cyberspace due to the uneven speed of cyber attacks

---

[117] Glaser and Kaufmann, "What Is the Offense-Defense Balance and How Can We Measure It?" p.1.

[118] Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," pp.32-33.

[119] Locatelli, *The Offense/ Defense Balance in Cyberspace*; Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft."

support this argument.[120] But, although offense is served as easier than defense technically and rationally, in an environment where authentication of an action even by forensics is harder, it seems it is hard to grasp who your opponent is and to decide whom to attack.

Defensive strategies are also important since the frequency of cyber attacks reveals the crucial need for protection and destruction in virtual domain. Among the defense advocates, in addition to debates over offensive versus defensive strategies in the cyber realm, there is another debate between passive cyber defense strategies and active cyber defense strategies. Passive cyber defense that implies general anti-virus programs and firewalls which protect personal computers from any malicious software aims to minimize the effects of cyber attack[121] "without the intention of taking the initiative"[122]. Although passive cyber defense should be a part of a successful cyber defense program[123], active cyber defense is superior to take the immediate actions against more serious and advanced cyber threats.[124] Contrary to passive cyber defense, active cyber defense implies offensive actions to defend the domain.[125] Cyber exploitation, counter attack, preemptive and preventive strikes are categorized as

---

[120] Lindsay, "Stuxnet and the Limits of Cyber Warfare," p.376.

[121] Wong, "Active Cyber Defense: Enhancing National Cyber Defense," p.13.

[122] "Passive Defense", *Department of Defense, Dictionary of Military and Associated Terms*, http://www.dtic.mil/doctrine/dod_dictionary/ (Accessed on 20.03.2016)

[123] Nye, "Cyber Power," p.17.

[124] Irving Lachow, *Active Cyber Defense A Framework for Policymakers* (Washington, DC, 2013), http://www.cnas.org/files/documents/publications/CNAS_ActiveCyberDefense_Lachow_0.pdf.

[125] Wong, "Active Cyber Defense: Enhancing National Cyber Defense," p.19.

offensive actions on behalf of active cyber defense.[126] These offensive measures may help deterrence work even though there is attribution problem.[127]

As the active cyber defense is suggested for a successful cyber defense program, the supremacy of offensive actions in cyber domain cannot be ignored in terms of the offense-defense balance. In this regard, it may be argued that the offensive cyber actions are important for both in offensive and defensive manner to gather intelligence and to secure intelligence. At final say, cybersecurity cannot only be sustained by defensive actions, it needs to be supplemented by offensive strategies which are mainly based on developing qualified cyber weapons and employing them when it is necessary.

The changing nature of power with high level of uncertainty and unpredictability of the results of offense dominant and defense dominant strategies increase the security dilemma for actors in cyber domain. Moreover, as cyberspace lacks legal commitments and powerful international regulations, the extent of anarchy rises as well. Attribution problem and asymmetry issues stay on the table as 'Pandora's box' and each actor tries to benefit from vagueness and uncertainty of cyberspace along with the line of their interests.

2.5 Conclusion

All in all, one can speak of many alterations based on the rise of the cyberspace. Roughly, at first, information revolution brings a new conflictual domain that is open to power struggles with a new medium of power. It also means that cyberspace is a new domain in security studies which includes new types of weapons such as viruses as hacking and cyber espionage tools to attack the networks, infrastructure and more

---

[126] Ibid., pp.19-27.

[127] Nye, "Cyber Power," p.17.

importantly information. Moreover, cyber domain contributes to recent debates on inquiries about states which are presented as the main actors of IR again by bringing non-state actors into game more openly. Therefore, one of the most important outcomes of technology revolution is undeniable inclusion of variety of actors simply from states to non-state actors. This diversification does not only imply a group of terrorists, but also it brings individual aggressors to the IR scene either with individual motivation or as pawns.

As this complex cyber environment affects almost every single aspect of socio-political relations, states are highly vulnerable to cyber threats. Reflections of this revolution should be interpreted in detail by looking at whether there are effects of the cyberspace as a new domain on the security strategies of the actors of this system.

In this regard, the dependence of the US on information and digital technologies as the birthplace of the Internet forces it to deal with cyber domain as a national security issue. Rather than promoting general analysis and theorizing about cybersecurity that can be viewed as relatively nascent area, this thesis concentrates on the US policy concerning cybersecurity. In order to explain this, it is crucial to analyze decision-making process during various administrations. In doing so, this thesis will try to answer the following questions: what is cybersecurity policy of the US? While dealing with this question, this thesis will also analyze how specific policies and strategies concerning cybersecurity have been developed? How is cybersecurity presented as a national security issue by policymakers? What are the repercussions of these policies on the country's foreign relations?

CHAPTER 3

CLINTON ERA: YEARS OF BURGEONING

3.1 Introduction

Although the rise of information technologies dates back to 1960s, ARPANET project, security-politics nexus of these technologies are not that much apparent before the Clinton Administration. This chapter aims to address how cybersecurity evolved as a national security issue during the Clinton period by underlining critical points of cybersecurity. In doing so, this chapter will allow us to compare and to contrast the following patterns of cybersecurity in Bush and Obama term.

This chapter begins with the general examination of the foreign policy context of the post-Cold War presidency and trends in the policy-making in order to position cyberspace among other policy issues. Then, it tries to find out the reasons of why and how cybersecurity became one of the primary policy issues of the Clinton period. After investigating positions of cyber bureaucracy in domestic politics, repercussions of this standing in international arena will be examined before running through the Bush term.

3.2 Foreign Policy Framework of the Clinton Administration

Understanding the post-Cold War politics and foreign policy may be a useful guide to position cybersecurity in Clinton era. In other words, foreign policy environment of the Clinton Administration is important to analyze the evaluation of cybersecurity issue in this broad policy framework.

With the end of the Cold War, international order was revised; priorities and interests of states needed to be reviewed. William Jefferson Clinton took office in 1993 at the end of the Cold War as the first elected post-Cold War president. For the US under the leadership of Clinton, it was a time of rescheduling political agenda accordingly to the new international order. The new world order was stated in Clinton's inaugural address:

> To renew America, we must meet challenges abroad as well as at home. There is no longer a clear division between what is foreign and what is domestic. The world economy, the world environment, the world AIDS crisis, the world arms race: they affect us all. Today, as an older order passes, the new world is more free but less stable. Communism's collapse has called forth old animosities and new dangers. Clearly, America must continue to lead the world we did so much to make.
>
> While America rebuilds at home, we will not shrink from the challenges nor fail to seize the opportunities of this new world. Together with our friends and allies, we will work to shape change, lest it engulf us. When our vital interests are challenged or the will and conscience of the international community is defied, we will act, with peaceful diplomacy whenever possible, with force when necessary.[128]

In his inaugural address, Clinton underlined the emerging threats in this new international order. The end of the Cold War brings new uncertainties as the well-known and single existential threat of the Soviet Union disappears.

From the same statement, one may find some clues about his foreign policy. First of all, there was emphasis on inclusionary policy understanding that melted domestic and

---

[128] William J. Clinton: "Inaugural Address," January 20, 1993. Online by Gerhard Peters and John T. Woolley, *The American Presidency Project*. http://www.presidency.ucsb.edu/ws/?pid=4636 (Accessed on 29.03.2016)

foreign issues in the same pot.[129] This also implies that successful foreign policy would be possible by achieving national and international economic security.[130] Secondly, there was an emphasis on peaceful diplomacy. Lastly, it signaled for multilateral actions. In this line, it could be understood from his inaugural address that Clinton's policy-making team was to concentrate more on global economic prosperity and search for a multilateral action under the UN in an international crisis by merging domestic and foreign.

It may be argued that the complex political environment of the post-Cold War period and Clinton's personal inexperience in foreign policy making shaped the policies and strategies of the Clinton Administration in his first term.[131] In detail, it was expected from the US to define its role on critical foreign policy issues such as the reintegration of the former Soviet states into international system, effectiveness of the UN, environmental degradation, humanitarian intervention and human rights problems, regulations on international trade, as well as, legacy of the Cold War on national developments, mainly on economy.[132]

In his first years of presidency, it was claimed that Clinton tried to keep balance among main agencies of foreign policy and kept distance from international crises rather than

---

[129] James McCormik, *American Foreign Policy and Process*, 6th ed. (Wadsworth Cengage Learning, 2014), p.160.

[130] Ibid., p.160.

[131] Ibid., p.162.

[132] Theodore C. Sorenson, "America's Firt Post-Cold War President," *Foreign Affairs* 71, no. 4 (1992): 13–30; Stephen M Walt, "Two Cheers for Clinton's Foreign Policy," *Foreign Affairs* 79, no. 2 (March 2000): 63–79; Rasmus Sinding Søndergaard, "Bill Clinton's 'Democratic Enlargement' and the Securitisation of Democracy Promotion," *Diplomacy & Statecraft* 26, no. 3 (September 2015): 534–51.

pursuing active and comprehensive foreign policy.[133] The first term of the Clinton Administration, particularly his policy-making team, was highly criticized because of ineffective and non-strategic policy applications.[134] Those criticisms mainly stemmed from the primary position of achieving economic prosperity among policy issues during his first term and secondary position of concentrating on political side of the international re-settlement.[135] But, it should be underlined that it was not very surprising since economic revival was always in top of his agenda since his presidential campaign. In one of his speeches, he clearly showed the importance of greater economic prosperity in order to pursue successful policies at home and abroad. "In this new era our first foreign priority and our domestic priority are one and the same: reviving our economy."[136] In that vein, apart from the achievements of free trade agreements and the creation of General Agreement on Tariffs and Trade (GATT)[137], the US had a low profile in foreign policy issues in Clinton's early period.[138]

Dynamics of foreign policy team of Clinton evolved through his second term with the call of ongoing international crises in Somalia, Haiti and Bosnia and with the change in

---

[133] Ibid., p.97.; Douglas Brinkley, "Democratic Enlargement: The Clinton Doctrine," *Foreign Policy*, no. 106 (1997): 111–27.

[134] McCormik, *American Foreign Policy and Process*, p.162.; Tim Weiner, "Clinton as a Military Leader - Tough On-the-Job Training," *New York Times*, October 28, 1996, http://www.nytimes.com/1996/10/28/us/clinton-as-a-military-leader-tough-on-the-job-training.html?pagewanted=all; John McCain, "Imagery or Purpose? The Choice in November," *Foreign Policy*, no. 103 (1996): 20–34.

[135] McCormik, *American Foreign Policy and Process*, p.163.

[136] Thomas L. Friedman, "Clinton and Foreign Policy/A Special Report.; Clinton's Foreign-Policy Agenda Reaches Across Broad Spectrum," *New York Times*, October 4,1992, http://www.nytimes.com/1992/10/04/us/1992-campaign-issues-foreign-policy-looking-abroad-clinton-foreign-policy.html?pagewanted=all ; McCormik, *American Foreign Policy and Process*, p.163.

[137] Ibid., p.164.

[138] Massari, "US Foreign Policy Decision-Making during the Clinton Administration," p.97.

his policy-making team.[139] In the opening session of Clinton's Address Before a Joint Session of the Congress on the State of the Union, he committed for taking immediate actions when necessary by declaring "we face no imminent threat, but we do have an enemy. The enemy of our time is inaction. So tonight I issue a call to action…"[140] Through stressing the importance of taking necessary measures, Clinton tried to overcome the main criticism on his first term which was based on passive foreign policy understanding. The changing nature of Clinton's foreign policy understanding becomes clearer in the National Security Strategy for a New Century. It projected for a shift towards traditional foreign policy principles by clearly defining threats to the US interests rather than pursuing new principles that focus on economic and democratic goals.[141]

Along with the line of this change and international crises, it can be argued that the second term of the Clinton Administration engaged more in policy issues from a security perspective. Enlargement of NATO, enhancing relationship with China, arms control and non-proliferation issue, and the crises in Bosnia and Kosovo were the main themes of the second term of the Clinton Administration together with improving global economic prosperity.[142] While there were such fundamental issues for Clinton to define, the policy-making process and the designation of strategies for the emerging threats should be in general taken into account in the context of post-Cold War.[143]

---

[139] Ibid., p.97.; McCormik, *American Foreign Policy and Process*, pp.162-167.

[140] William J. Clinton, "Address Before a Joint Session of the Congress on the State of the Union," *The American Presidency Project*, February 4, 1997, http://www.presidency.ucsb.edu/ws/?pid=53358.

[141] "A National Security Strategy for a New Century," *White House*, 1998;McCormik, *American Foreign Policy and Process*, p.167.

[142] Clinton, "Address Before a Joint Session of the Congress on the State of the Union."

[143] Massari, "US Foreign Policy Decision-Making during the Clinton Administration," p.94.

Cybersecurity became a critical issue in this complex policy environment with interlinked issues of national and international events.

While he faced many other developments, presidency of Clinton can be seen as the first years when vulnerabilities of this new kind of cyber threat on both physical domain and cyber domain were identified.

3.3 Burgeoning of Cybersecurity

With the end of the Cold War and the disappearance of the Soviet Union, the nature of threats has changed particularly for the US. As mentioned above, there were new threats and security issues to deal with. Cyber threats may be categorized with these new threats. In such a political environment, one may easily argue that disappearance of well-known danger of the Soviet Union and decreasing level of the nuclear threat paved the way for emergence of new threats.[144] However, one could also find more specific reasons about how cybersecurity was presented as a national security issue in the years of the Clinton Administration. These are vulnerability and risk assessment of threats to critical infrastructure and the economic interests of the US. As vulnerabilities and risks of cyber threats became obvious in line of the economic interests for competitiveness, cybersecurity integrated as a vital part of the security agenda as the cyber pessimists expect. This was accelerated by the remarkable cyber incidents of 1990s.

---

[144] Morton H. Halperin, Priscilla A. Clapp, and Arnold Kanter, *Bureaucratic Politics and Foreign Policy* (Washington, DC: The Brookings Institution, 2006), p.11.

3.3.1 Causes of Burgeoning

3.3.1.1 Vulnerability and Risk Assessment of Threats to Critical Infrastructure

Penetration of the term of cybersecurity into security discourse and political discourse took a while before it became more popularized. In the very beginning, there were various topics which are now evaluated under the umbrella term of cybersecurity such as critical infrastructure protection, data security, and network security. As the significance of these issues was realized through analysis of increasing vulnerabilities and risk assessment on information and critical infrastructure, the cruciality of the cybersecurity issue was underlined during the Clinton Administration.

As it is widely known and previously discussed, the US is accepted as technology superior state. However, as technology is getting advanced, threats are also getting advanced. It may be argued that increasing threat perceptions of cyberspace are generally based upon advantages and disadvantages of depending on these networked systems of the information technologies. This paradoxical issue exacerbated in 1990s. In other words, apart from advantages of technological advancement, in terms of cybersecurity, 1990s were the years of intrusions into protected government networks in the US. In 1990s, several incidents of interruptions and breakdowns on these critical infrastructures caused by either malicious intentions or technical problems demonstrated the vulnerability and risks caused by any hostile actions.[145] For example, during the Operation Desert Storm, the US military computers were hacked. It was the case that underlined the extent of vulnerabilities of new age.[146] In 1998, a group of

---

[145] Office of Science and Technology Policy National Security and International Affairs Division, *Cybernation: The American Infrastructure in the Information Age* (Washington, DC, 1998), http://fas.org/irp/threat/980107-cyber2.html.

[146] Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure Information Age* (New York: Routledge, 2008), p.70.

teenage hackers intruded into computer systems of the Air Force Computer Emergency Response Team in San Antonio, Texas.[147] Although the crisis was not caused by malicious intentions of an external power, they revealed the vulnerabilities of the US. These were important incidents for realization of a new existential threat from the perspective of securitization.

Any incidents of intrusions may indicate the vulnerability of the US and significance of the issue. Therefore, as a result of these intrusions, in 1998, *Cybernation: The American Infrastructure in the Information Age* was prepared for underlining the importance of infrastructures and their ties with the cyber domain. In this report of the Office of Science and Technology Policy, it was stated:

> The sectors serve a wide variety of customers throughout society. Major interruptions in the services of any sector could have serious and widespread health, safety, and national security implications. There are numerous interconnections and mutual dependencies among the infrastructure sectors and among the information networks that support them. The public telephone network, for example, relies in part on the power grid, the power grid on transportation, and all of the sectors on telecommunications and the financial infrastructure. Most sectors employ the public telephone network for at least some of their cybernetic channels. Most control networks also have some connection to public networks, many to Internet. Additionally, there are shared rights-of-way in many locations throughout the country. The infrastructure is inherently regional, national, and even global in scope. All sectors have components distributed over wide geographic areas.[148]

As services of transportation, finance, energy, and telecommunications relied on computer networks, suspicions about vulnerability and reliability of these systems

---

[147] "Cyberwar Timeline," InfoPlease, http://www.infoplease.com/world/events/cyberwar-timeline.html#1990 (Accessed on 10.05.2016)

[148] Office of Science and Technology Policy National Security and International Affairs Division, *Cybernation: The American Infrastructure in the Information Age*.

became more apparent.[149] Interconnectedness or interdependence of these services was illustrated as a critical feature. It means that risks were increasing for widespread critical infrastructures depending on networks for many sectors of services. Moreover, not only is the public infrastructure dependent on computers and other information systems, but also military security systems and government networks. To put it differently, while technological advancement provides common utility for public on the one hand, it is also possible to observe reverse effects jointly. The reverse effect which may be called as an emerging existential threat requires new security strategies for the US from the perspectives of cyber-pessimists.

3.3.1.2 Economic Interests

Throughout the Cold War, secrecy and protection was essential part of the principles of the technological competition between two blocs.[150] In order to control technological exchange, the Coordinating Committee for Multilateral Export Controls (CoCoM) was established in 1949 by the Western bloc against the Eastern bloc.[151] That is why they were not able to share and trade legally/officially the technological products during the Cold War compared to the post-Cold War period. It was stated in 1994 as:

> Thirty years ago, computer systems presented relatively simple security challenges. They were expensive, isolated in environmentally controlled facilities, and their use was an arcane art understood by few. Consequently, protecting them was relatively easy, a matter of controlling access to the computer room and clearing the small number of specialists who needed such

---

[149] Ibid.

[150] Elidor Mehilli, "Technology and the Cold War," in *Coordinating Committee for Multilateral Export Controls*, ed. Artemy M. Kalinovsky and Craig Daigle (New York: Routledge, 2014), p.292.

[151] Ibid., p.298.

> access. As these systems evolved, their connectivity was extended, first by remote terminals and eventually by local and wide-area networks.[152]

It can be argued that with the collapse of the Soviet Union and the disappearance of communist threat, there has been an increase in commercialization of technology products as in the case of the Internet. Therefore, economic interests in the post-Cold War period which was consolidated along with the policy objectives of the Clinton Administrations could be defined as a critical determinant among the causes of burgeoning of cybersecurity.

Technological advancement had important role for economic advancement and competitiveness as well, as it is claimed in the US Code dates back to 1992:

> Telecommunications and information are vital to the public welfare, national security, and competitiveness of the United States. Rapid technological advances being made in the telecommunications and information fields make it imperative that the United States maintain effective national and international policies and programs capable of taking advantage of continued advancements. Telecommunications and information policies and recommendations advancing the strategic interests and the international competitiveness of the United States are essential aspects of the Nation's involvement in international commerce.[153]

The code shows us that attributions to the national security were obvious as of 1992. It may be argued that the concerns over national security increased the as the free market activities increased. Furthermore, in addition to the increasing level of free market activities, as economic security and economic prosperity were the driving forces of the post-Cold War politics of the US, market interests should not be thought apart from the cybersecurity. It may be understood from one of the hearings of the 104th Congress:

---

[152] Joint Security Commission, "Redefining Security: A Report to the Secretary of Defense and the Director of Central Intelligence" (Washington, DC: US Government Printing Office, 1994).

[153] *United States Code* (Washington: Government Printing Office, 2008), p.294.

> Much of our national economy also depends on the NII. The vast majority of transactions conducted by banks and other financial institutions are done via electronic funds transfers. For example, one major bank transfers approximately $600 billion electronically per day to the Federal Reserve. Over $2 trillion is sent in international wire transfers every day. In addition, most securities transactions are conducted via computerized systems.[154]

This statement shows us the importance of the critical infrastructures on economic activities. Moreover, it can be said that infrastructures are also important to uphold "productivity, quality of life, and economic progression by driving growth, creating jobs, and improving productivity, quality of life and efficiency."[155] In this respect, it may be argued that as Clinton favored free trade, market demands about lifting up restrictions on several technology products was suitable with the policies of Clinton that were based on economic competitiveness. In this manner, demands and efforts of technology market to ease the control on technological exports can be mentioned as one of the internal driving forces that brought new security needs and thus revised regulations.[156]

Since lifting up barriers on trade of information technology products makes them accessible for everyone it reveals new vulnerabilities for the public and private services that are based upon information technology. A critical example of this can be observed in export control of encryption products and cryptography which are vital tools for

---

[154] "*Security in Cyberspace" Hearing Bef*ore *the Permanent Subcommittee on Investigations of the Committee on Governmental Affairs,* the U.S. Senate, 104th Cong., 2 (1996), https://archive.org/stream/securityincybers00unit#page/n1/mode/2up.

[155] "Role of Critical Infrastructure in National Prosperity," *Public Safety Canada*, October, 2015, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-rl-crtclnfrstrctr-ntnlprsprty/2016-rl-crtclnfrstrctr-ntnlprsprty-en.pdf.

[156] John Markoff, "Clinton Proposes Initiatives On the Scrambling of Data," *New York Times*, 1996, http://www.nytimes.com/1996/07/13/business/clinton-proposes-initiatives-on-the-scrambling-of-data.html.

security systems.[157] As software industry backed by the Congress wanted to compete in international market, the administration was left no choice to follow the policy to ease control on encryption products.[158] Nonetheless, the potential vulnerabilities of encryption products continued to be underlined with a memorandum in 1996:

> Encryption products, when used outside the United States, can jeopardize our foreign policy and national security interests. Moreover, such products, when used by international criminal organizations, can threaten the safety of U.S. citizens here and abroad, as well as the safety of the citizens of other countries. The exportation of encryption products accordingly must be controlled to further U.S. foreign policy objectives, and promote our national security, including the protection of the safety of U.S. citizens abroad. [159]

This situation demonstrates that the vulnerabilities of the US have increased as the technological advancement is backed by technological openness, which may bring negative effects on national security. The negative effects may stem from cyber espionage and other versions of cyber crime which are the main threats for private sector by causing economic loss. The cost of use of these malicious tools has an increasing scale as free-market standards get applied. Parallel to this, one may argue that one of the concerns of the government about cyberspace seems to be related to any possible negative effects on economic prosperity. Therefore, economic interests and market motives seem to have an impact on the ascending cybersecurity and the regulations on cyberspace.

---

[157] "Use Cryptography Correctly," *The Institute of Electrical and Electronics Engineers*, http://cybersecurity.ieee.org/blog/2015/11/13/use-cryptography-correctly/.(Accessed on: 10.05.2016)

[158] Markoff, "Clinton Proposes Initiatives On the Scrambling of Data."

[159] "Memorandum For The Vice President, The Secretary Of State, The Secretary Of The Treasury, The Secretary Of Defense,The Attorney General," *White House*, 1996, http://fas.org/irp/offdocs/eo_crypt_9611_memo.htm.

3.3.2 Cyber Incidents of 1990s and the 'First Cyberwar'

In addition to the reasons of the need of critical infrastructure protection and economic motives, critical cyber intrusions of 1990s can also be shown as key determinant of the story of burgeoning.

The events of the 1990s demonstrated the cyberwar issue was not a remote possibility for the US. The first intrusion of 1990s took place when the US military computers were hacked in the Gulf War during the Operation Desert Storm.[160] Then, in 1994, Rome Laboratory, the research facility of the Air Forces, was hacked.[161] Until the intrusions were revealed, the sensitive systems data were stolen by the hackers with an estimated cost of half a million dollar.[162] These incidents continued during the 1990s. In 1998, there were many detected intrusions in both public and private sector including various agencies such as the Department of Energy, the US military, and NASA.[163] Then, with the Moonlight Maze, more sophisticated attacks on the Pentagon, NASA and the Department of Energy, the security weakness and vulnerabilities became more obvious.[164] The intrusions on critical government networks by average hackers also brought the asymmetry issue as well as security weakness of government. Moreover, these cases brought the attribution problem to the table, as the attackers have

---

[160] United States General Accounting Office, "Computer Security: Hackers Penetrate the DoD Computer Systems" (1991); Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure Information Age*, p.70.

[161] United States General Accounting Office, "Information Security:Computer Attacks at Department of Defense Pose Increasing Risks" (1996).

[162] Ibid.

[163] "Pentagon 'at War' with Computer Hackers," *CNN*, 1999, http://edition.cnn.com/TECH/computing/9903/05/pentagon.hackers/index.html; Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure Information Age*, p.82.

[164] Ibid., p.82.

remained un-authenticated.[165] These incidents helped the realization of the controversial features of cyberspace such as the attribution problem, temporality and accountability, which increase the vulnerabilities and risk assessment of the US in the cyber domain.

While the US administration, mainly the DoD was dealing with such cyber incidents, Kosovo crisis which was called as 'first war on the Internet[166]' or the 'first cyberwar'[167] can be seen as major international case of the Clinton term. The role of the Internet in the Kosovo conflict was very extensive. It was used both for propaganda by non-governmental organizations[168] and as a tool to exchange data by government.[169] Moreover, Kosovo conflict had more malicious characteristics than previous incidents since the NATO servers and the US government websites were hacked. Although this case did not result with a catastrophic damage of the Internet it got attention of the public by its malicious characteristics and common usage with participation of a broad range of actors.[170]

---

[165] Ibid., p.82.

[166] Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet As A Tool For Influencing Foreign Policy," in *Networks and Netwars: The Future of Terror, Crime, and Militancy*, ed. John Arquilla and David Ronfeldt (Santa Monica: RAND, 2001), 239–88.

[167] Ellen Joan Pollock and Andrea Petersen, "Unsolicited E-Mail Hits Targets In America in First Cyberwar," *Wall Street Journal*, 1999, http://www.wsj.com/articles/SB923519887609541882.

[168] Denning, "Activism, Hacktivism, and Cyberterrorism: the Internet As A Tool For Influencing Foreign Policy."

[169] Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure Information Age*, pp.73-75.

[170] Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet As A Tool For Influencing Foreign Policy."

Cyber attacks –hacking, web defacements and DoS- that were launched against NATO web servers[171] and the US government websites during this crisis are worth mentioning because of their aggressive features although operational capability of NATO did not depend on web-servers. They were essential because neither NATO nor the Pentagon took the counter measures against these pro-Serbian international hackers.[172] It was claimed that the US did not want to commit a war crime by information operations as far as legal regulations were concerned.[173] At this point, it could be said that preferences of refrainment from a cyber response was tried to be explained by considering the legal and ethical aspect of information warfare.

It should be noted that there were also counteraccusations by claiming that the US also used offensive information operations in cyberspace during 1990s. Firstly, in the Gulf War of 1991, the US attacked Iraqi information based systems of radar and communication systems with the aim of intercepting their information sharing and gathering mechanism.[174] Another example of the offensive actions of the US may be observed during the Kosovo crisis. It was argued that there were cyber attacks on Serbia during NATO bombing although it was not officially declared and accepted by the US due to legal limitations.[175] Therefore, the claim based on the US commitment to

---

[171] "Serb Supporters Sock It to NATO, U.S. Web Sites," *CNN*, 1999, http://edition.cnn.com/TECH/computing/9904/06/serbnato.idg/index.html; "Belgrade's Cyber-Assault," *CBS New*, 1999, http://www.cbsnews.com/news/belgrades-cyber-assault/.

[172] "Pentagon Kept the Lid on Cyberwar in Kosovo," *The Guardian*, 1999, http://www.theguardian.com/world/1999/nov/09/balkans.

[173] Ibid.; Bradley Graham, "Military Grappling With Rules For Cyber Warfare," *The Washington Post*, 1999, http://www.washingtonpost.com/wp-srv/WPcap/1999-11/08/011r-110899-idx.html.

[174] Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure Information Age*, p.69.

[175] Ibid., p.69.; Julian Borger, "Pentagon Kept the Lid on Cyberwar in Kosovo," *The Guardian*, November 9, 1999, http://www.theguardian.com/world/1999/nov/09/balkans.

the legal restrictions was not very convincing for most since they argued that the US also used offensive actions in cyberspace during Kosovo crisis. The use of offensive actions by the US was a noteworthy case because it revealed the fact of strategic advantages of cyberspace. It means that as the characteristics of cyberspace allow actors to utilize from cyber attacks without a judgement, cyberspace offers a grey zone especially for states to pursue their secret agenda.

To conclude, the story of burgeoning of cyberspace and information security as a national security issue started through the end of the presidency of Clinton as the foreign policy team concentrated more on critical foreign policy and security issues together with the realization of the vulnerabilities and economic interests of the US. The realization of the vulnerabilities and risk assessment of the US may be interpreted as their pessimist standing in the field of cybersecurity since they accepted the potential dangers and damage from cyberspace, and they needed to build-up new strategies. In the vein of burgeoning of cyberspace and cybersecurity, efforts to come up with strategies for cybersecurity intensified in the second period of the Clinton Administration as the securitization move became clearer.

3.4 Building-up Cybersecurity Strategy in Domestic Politics

When states tried to adapt to the international order as of 1991, priority of the national governments was to modify security needs in this environment. In the very beginning, as mentioned above, the agenda of the US mainly focused on developing economic strategies. In this manner, developing strategies for cyberspace was not a priority during the first term of the Clinton Administration.

One of the early examples of the secondary position of cybersecurity during the first years of the Clinton Administration can be found in the report of Les Aspin, the Secretary of Defense. In the *Report on the Bottom-Up Review* of 1993 which focused on the new defense strategy of the US in the post-Cold War, threats from weapons of mass destruction and aim of non-proliferation were kept constant as a critical matter of

security, while regional dangers of illegal activities and overseas danger of democratic transition period in the former socialist bloc were addressed together with dangers embedded in the international economic system, and environment.[176] In light of these threats, ways of modifying defense structure was sought. However, among the report, there was no mention of cybersecurity or even security need deriving from technological advances. Rather, the point was on the superiority of the US in terms of weapons due to technological development.[177] Therefore, it could be argued that cybersecurity was not yet on the agenda of the Presidency or top-level bureaucratic agents as of 1993. However, the Department of Defense was not totally negligent in cybersecurity; rather it was aware of the dangers from rising technological dependence.

In accordance with the factors that triggered cybersecurity, federal agencies as a whole tried to figure out new nature of dangers throughout the 1990s. President and the Department of Defense played critical roles in shaping the cybersecurity strategies in domestic politics, while the legislative efforts were more limited in complementing securitization move of the other federal agencies.

3.4.1 Role of the Department of Defense

As the DoD is mainly responsible with military security of the US, it takes part in both process of implementation and formulation of security policy. The position of the DoD over cybersecurity can be traced through the statements and official documents of the Secretary of Defense who is the main representative of the DoD in addition to the official documents of the DoD. In policy formulation process, common belief about standing of the DoD based on the idea that the military personnel are more open to

---

[176] Les Aspin, *Report on the Bottom-Up Review*, 1993.

[177] Ibid., p.32.

belligerent strategies than civilian policy makers.[178] However, the post-Cold War cases of American use of force demonstrated just the opposite.[179] In terms of national cybersecurity strategies, as attacks and use of force in cyberspace are clearly distinguished from conventional military use of force, it is worth providing details on the debate of civilian and military officers.

Effective functioning of the DoD is highly dependent upon computers and communications networks which make private sector an important actor.[180] In this line, in the beginning, cybersecurity was just more about protecting information and other advanced technologies for the DoD. Therefore, the DoD can be seen as the primary agency that called for developing all-inclusive strategies which were primarily based on collaborative strategies of public and private sectors against rising cyber threats. However, since military bureaucracy was aware of the emerging danger on information systems security, the attempts of the DoD were vital to call for new strategies. In the report of *Redefining Security* which implied recommendations for 'developing a new approach to security', dated 1994, it was claimed that:

> With the end of the Cold War and facing new challenges to US economic competitiveness, policymakers are focusing on the threat from foreign government and nongovernment entities to US advanced technologies, defense-related industries, proprietary data, intellectual property rights, and trade secrets. The increased value of US technical information necessitates balancing

---

[178] Glenn P. Hastedt, *American Foreign Policy* (Upper Saddle River, N.J. : Pearson/Prentice Hall, 2011), p.215.

[179] Christopher Gelpi and Peter D. Feaver, "Speak Softly and Carry a Big Stick? Veterans in the Political Elite and the American Use of Force," *American Political Science Review* 96, no. 4 (2002), p.779.

[180] Joint Security Commission, "Redefining Security: A Report to the Secretary of Defense and the Director of Central Intelligence."

> national policy objectives and the importance of sharing information with the need to protect our leading edge technologies.[181]

In this report, first steps of a securitization move by the DoD as a critical securitizing actor can be traced. Threats from both states and non-state actors to the technological advancement of the US were emphasized as a new factor of protecting national objectives of the US. This may be seen as the identification of existential threats to the US national security. To deal with these emerging threats and to protect these vital technologies, developing counterintelligence strategies were the primary recommendation.[182] A recommendation for developing new strategies may be interpreted as a step towards developing extraordinary measures. Moreover, in the same report, the new phase opened by cyberspace was also asserted:

> Networks are already recognized as a battlefield of the future. Information weapons will attack and defend at electronic speeds using strategies and tactics yet to be perfected. This technology is capable of deciding the outcomes of geopolitical crises without the firing of a single weapon. Our security policies and processes must protect our ability to conduct such infowars while denying our enemies that same advantage.[183]

There were two critical points about this report. Firstly, it defined the new domain as a new battlefield contrary to the arguments of the cyber skeptics who do not accept cyberspace a new battleground. This is significant since it also attempted to define new strategies and measures for new battlefield. Secondly, it emphasized the importance of keeping relative power of the US at top level to sustain cybersecurity. It may be interpreted as a signal for an increase in offensive capabilities of the US which may

---

[181] Ibid.

[182] Ibid.

[183] Ibid.

help to overcome the problem of asymmetric power issue. Due to potential profound effects of depending on information technologies, this report also underlined a call for more comprehensive security strategies for immediate action in addition to the counterintelligence strategies.[184]

In 1994, Defense Science Board Summer Study Task Force also worked on a report on *Information Architecture for the Battlefield* which evaluated the requirements of information warfare in the emerging global security environment. The paradoxical nature of the cyberspace was stated as:

> The Department of Defense has been a leader, in adapting information technologies. The DoD spends hundreds of millions of dollars to leverage this commercial technology. These coincident activities have provided the DoD with very powerful capabilities while simultaneously making U.S. forces dependent on the same technologies. U.S. combat forces have begun to use information per se as a powerful new weapon. Paradoxically, these same new strengths create significant vulnerabilities. The tens of thousands of computers connected to other computers has increased the damage that can be inflicted from the vantage point of a single computer or computer-controlled network.[185]

It could be claimed that demonstrating the vulnerabilities of the both public and private systems seem like a vital part of the securitization move in terms of cybersecurity since it may help uphold the attention and awareness of the audience. In addition to demonstrating vulnerabilities of the DoD due to its dependence on information technologies, in that report, importance of enhancing capabilities on information warfare in both defensive and offensive ways was underlined.[186] In the same report, it

---

[184] Ibid.

[185] Defense Science Board, *Report of the Defense Science Board Summer Study Task Force on Information Architecture for the Battlefield* (Washington, DC, 1994).

[186] Ibid.

was argued that in order to have improved offensive capabilities in this information battlefield, enhanced systems of protection of the US military assets was needed.[187] In line with the defense advocates in cyberspace, priority was given to enhancing defense systems for success in offense. The order between offense and defense of the DoD may be interpreted as an aim to decrease the level of vulnerabilities of the US against the existential threats from cyberspace by defending the domain.

The voice of military community became louder in time as the information attacks and network intrusions get more frequent. As a result of increasing analysis on information technologies and so on cyberspace, main characteristics of the cyberspace became more obvious for the DoD in the consecutive report of the Defense Science Board in 1996 which was named as *Information Warfare*:

> Information warfare offers a veil of anonymity to potential attackers. Attackers can hide in the mesh of inter-netted systems and often use previously conquered systems to launch their attacks. The lack of geographical, spatial, and political boundaries offers further anonymity and legal and regulatory arbitrage; this lack also invalidates previously established "nation-state" sanctuaries. Information warfare is also relatively cheap to wage, offering a high return on investment for resource-poor adversaries. The technology required to mount attacks is relatively simple and ubiquitous. During information warfare, demand for information will dramatically increase while the capacity of the information infrastructure will most certainly decrease. The law, particularly international law, is currently ambiguous regarding criminality in and acts of war on information infrastructures. This ambiguity, coupled with a lack of clearly designated responsibilities for electronic defense hinders the development of remedies and limits response options.[188]

---

[187] Ibid.

[188] Defense Science Board, *Report of the Defense Science Board on Information Warfare* (Washington, DC, 1996).

In the report of 1996, attribution problem, low level of entry barriers, physicality, temporality, permeation and accountability issues of cyberspace were emphasized. In terms of securitization of cybersecurity, the significance of this report can be seen in its clear analysis of features of cyberspace in order to take necessary steps both at national and international levels, notwithstanding, the last part of this text proved that there was no international cybersecurity measures. Following the report of *Information Architecture for the Battlefield of* the Defense Science Board, the report of *Information Warfare* recommended organizing and upgrading defensive capabilities for information warfare as the primary strategy through underlining the "need for extraordinary action to deal with the present and emerging challenges of defending against possible information warfare attacks on facilities, information, information systems, and networks of the United States."[189] The stress on 'information warfare' is essential for a speech act because the nature of the word 'warfare' itself may be very useful for a securitization move. The use of the phrase of extraordinary actions is highly remarkable to securitize the issue, although the recommended strategies for extraordinary measures in cyberspace are differentiated from the measures of traditional domains.

Through the end of the Clinton era, critical infrastructure protection was paid more attention by the DoD as well. In the roadmap of *Critical Infrastructure Protection Executive Plan*, 2000 which was prepared for the Pentagon, cyberspace was given special attention by underlining importance of the critical infrastructure protection at this new domain.[190] In this document, protection of critical infrastructure at both

---

[189] Ibid.

[190] "Critical Infrastructure Protection Execution Plan," *The Department of Defense*, March 13, 2000, http://oai.dtic.mil/oai/oai?&verb=getRecord&metadataPrefix=html&identifier=ADA391662.

physical and cyber domain was closely tied to military success due to dependence of the DoD on this infrastructure.

All these show that it was the military wing, the Pentagon, who emphasized striking capability of the US in military technology and thus vulnerabilities from cyberspace. The DoD could be seen as a very important securitizing actor since it put into word the dangers of cyber threats by pointing the US national security as a referent object. It also showed its comprehension about the characteristics of cyberspace which may allow to take proper measures. The measure that recommended by the DoD was based on a working information-sharing mechanism among the actors of the public and private sectors. Even though this measure is open to criticisms, the securitizing efforts of the DoD during the burgeoning era were significant.

3.4.2 Role of the Presidency

Prior to second term of the Clinton Administration, cybersecurity was not a major security issue. It became a critical issue as the Administration became more interested in security issues. This started when President Clinton published the *Presidential Decision Directive-29* (PDD-29) in order to enhance coordination on security policies in the new threat environment of the post-Cold War.[191] In parallel to this, the securitizing efforts of the DoD were supported by the presidential initiatives and policies. By the *Executive Order of 1996*, the President's Commission on Critical Infrastructure Protection was established by bringing cyber threats into the security agenda within the framework of critical infrastructure protection.[192] In one of the commission reports which was named *Protecting America's Infrastructures,* dated

---

[191] William J. Clinton, "Presidential Decision Directive 29: Security Policy Coordination" (Washington, DC: Government Printing Office, 1994).

[192] William J. Clinton, *Executive Order 13010 Critical Infrastructure Protection* (Washington, DC, 1996).

1997, vulnerabilities and cyber threats that could harm economic prosperity of the US more than physical threats for main infrastructures which were transportation, oil and gas production and storage, emergency services, water supply, government services, banking and finance, electrical power and information and communications were emphasized.[193] Furthermore, in the same report of the President's Commission on Critical Infrastructure Protection, the effects of cyberspace were introduced as follows:

> […] the cyber revolution brings us into a new age as surely as the industrial revolution did two centuries ago. Now, as then, our continued security requires a reordering of national priorities and new understanding about our respective roles in support of the national goals.[194]

This text showed that the US accepted the challenges of cyberspace in its security agenda. Moreover, the report referred the borderless characteristic of the new domain beyond sovereign boundaries and wide range of cyber attacks and actors. Both the awareness on the challenges and characteristics of cyberspace may be interpreted as the pessimist standing of the Clinton Administration along with the discussion in the literature. In addition to this, the President also underlined the importance of public-private partnership in this document. Increasing information sharing efforts and building a public-private partnership seemed like prominent part of American cyberspace strategy at domestic level since operational capability of the US critical infrastructure was mainly in the hands of the private sector.[195]

---

[193] *Critical Foundations: Protecting America's Infrastructures* (Washington, DC: U.S. Government Printing Office, 1997), https://fas.org/sgp/library/pccip.pdf.

[194] Ibid.

[195] Clinton, *Executive Order 13010 Critical Infrastructure Protection*.

In light of this report, *Presidential Decision Directive/NSC 63* (PDD-63) was published in May of 1998. Briefly, this document intended to put a guideline to minimize or to eliminate risks and vulnerabilities coming mainly from cyberspace.[196] It was again and again emphasized that protection of critical infrastructure was vital for functioning of both public and private services. Therefore, public-private partnership that enhances information sharing capacity was presented as the primary way to achieve the national goal of cybersecurity mainly by defensive strategies.[197] In PDD-63, the public-private partnership which was associated with critical infrastructure protection was presented as a critical national cybersecurity strategy.

A National Coordinator for Security Infrastructure Protection and Counter-Terrorism, Richard Clarke, was appointed to accomplish the aim of PDD-63. In his press briefing, it was again very apparent that cybersecurity which was promoted as a national security issue mainly referred to the protection of critical infrastructure.[198] Under this system, in control of Clarke, security of critical infrastructure was considered as a part of strategy of combatting terrorism.[199] Here, policymakers emphasized the importance of cybersecurity through linking it with combating terrorism. This was important to get support of the national audience as a critical part of the securitization theory.

---

[196] William J. Clinton, *Presidential Decision Directive 63: Critical Infrastructure Protection*, *The White House* (Washington, DC, 1998), http://fas.org/irp/offdocs/pdd/pdd-63.htm.

[197] Ibid.

[198] William J. Clinton: "Press Briefing by Richard Clarke, National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism; and Jeffrey Hunker, Director of the Critical Infrastructure Assurance Office," May 22, 1998. Online by Gerhard Peters and John T. Woolley, The American Presidency Project. http://www.presidency.ucsb.edu/ws/?pid=48290.

[199] Ibid.; Judith Miller and William J. Broad, "Exercise Finds U.S. Unable To Handle Germ War Threat," *New York Times*, 1998, http://www.nytimes.com/1998/04/26/world/exercise-finds-us-unable-to-handle-germ-war-threat.html?pagewanted=1.

More clear standing of Clinton on cyberspace strategy came on the scene in his commencement speech to the Naval Academy at Annapolis, in 1998. Similar to the DoD reports, the president stated cyberspace as a new battlefield together with non-traditional threats and attacks that could come from wide range of actors including terrorist organizations.[200] As it was stated:

> We also face threats to critical national infrastructures, which increasingly could take the form of a cyber-attack in addition to physical attack or sabotage, and could originate from terrorist or criminal groups as well as hostile states.[201]

This statement of Clinton showed that the awareness of the cyber danger from terrorists. It may be seen as a great contribution to the speech act by the DoD by the top-level federal agency, the Presidency. Then, he declared an extensive strategy of detection, deterrence and defense for fighting against cyber attacks aggressively.[202] However, although it should be noted that characteristics of cyberspace would prevent this conventional strategies to work, the attempts to develop emergency measures are vital regarding the securitization of the virtual domain. Furthermore, in terms of definition of cyberspace, it was an important step to represent it as the battlefield because the word itself requires for a state policy and strategy and implies categorization of this new domain together with traditional domains of war. Therefore, the strategy declared can be seen as a result of this categorization.

Through the end of Clinton's presidency, in 2000, a *National Plan for Information System Protection* was prepared with the purpose of adapting the US security agenda to

---

[200] "President Bill Clinton Speaks To The Naval Academy At Annapolis," *CNN*, 1998, http://edition.cnn.com/ALLPOLITICS/1998/05/22/clinton.academy/transcript.html.

[201] "A National Security Strategy for a New Century," *White House*, 1998.

[202] Ibid.

the requirements of the information age. This plan can be seen as the final work of a series of comprehensive efforts during the presidency of Clinton because it suggested the US as the most vulnerable target. It may be understood from the below extract:

> More than any other nation, America is dependent upon its cyberspace. Attacks upon our cyberspace could crash electrical power grids, telephone networks, transportation systems, and financial institutions. All of those sectors depend upon control networks involving computer systems. In the next war, the target could be America's infrastructure and the new weapon could be a computer-generated attack on our critical networks and systems. We know other governments are developing that capability.[203]

After ten years of efforts, it was understood that the cyberspace posed new threats to national security of the US while growing capabilities also urged new security planning for the US. Denoting the US vulnerabilities in cyberspace together with the increasing potential dangers from other actors was like a final designation of the existential threat in this new domain as a part of securitization move. With respect to dependence on cyberspace, in this document, three steps – prepare and prevent, detect and respond, build strong foundations- were determined as the main strategies to fight against cyber threats at national level.[204] The three steps involved all the strategies that had been recommended in previous reports and documents of the Pentagon. However, it was important since it suggested a clear roadmap for strategies.

The role of the President in the burgeoning era seems very important since Clinton joined in the securitization move by emphasizing existential threats and extraordinary measures. His efforts were important in order to convince the public because of his

---

[203] William J. Clinton, "Defending America's Cyberspace: National Plan for Information Systems Protection An Invitation to a Dialogue" (Washington: Government Printing Office, 2000), https://fas.org/irp/offdocs/pdd/CIP-plan.pdf.

[204] Ibid.

emphasis on vulnerabilities of the critical infrastructure of the US. However, these attempts which may be defined as a securitization move did not bring in radical cybersecurity strategies at national level. In this sense, domestic strategies of cybersecurity can be summarized as having defense dominant nature which was based on urgent requirement of public-private partnership in order to enhance information-sharing mechanisms.

3.4.3 Role of the Legislative Efforts

Congressional power is regulated under Article I of the Constitution. Congress is the main legislative authority, although there has been cyclical dominance of these branches on policymaking process of critical issues due to shared responsibilities of presidency and congress. Moreover, Congress, itself, is also a part of the system of checks and balances by having two chambers –the House of Representatives and the Senate-. They both have voting power; moreover, positive vote of both chambers is required for finalization of legislative act. In the House of Representatives and the Senate, after a bill is introduced by one of the members, mainly committees are responsible for analyzing and reporting the process of the bill.

As it could be expected, legislative efforts to enhance cybersecurity were very limited in time of Clinton. However, as this study names the Clinton era as burgeoning of cybersecurity, legislative efforts may be expected to started in the Clinton period even though they did not go one step further from introduction of the cybersecurity issue at the Congress. Nevertheless, it should not be ignored that the Congress contributed to the securitization move of cybersecurity by using the terms of cyber threat and security for cyberspace. For instance, the necessity to revise national security was very clear in one of the articles of the 104th Congress which was titled as the *National Security and Information Age,* dated 1996:

> […] we must be willing to reconsider our previously defined notions of national security. The threat from cyberspace, because it can emanate from a borderless world that transcends national boundaries, eludes many of our traditional national security assets. We cannot permit this problem to get lost in the seams of our intelligence, enforcement and defense communities. We will undoubtedly require the types of international alliances that has served us well in our defense of our physical perimeters.[205]

This statement called attention to the distinguished features of cyberspace that required reconfiguration of strategies. It can also be seen as a call for new emergency measures. Consecutively, the 105th Congress also worked to address the threats from cyberspace in another article which was named as the *National Security and Information Technology*, dated 1998:

> We need to come to this task with a clear sense of purpose and full understanding of the urgency involved. America has gained much from information technology, and stands to gain much more as these systems mature. Our future depends on the success of this technology. But that success and our security depend on finding the policies and practices that will identify and correct vulnerabilities before they are exploited.[206]

The statement which highlighted the strategic importance of cyberspace for the future of the US boiled down the reason of the US interests in cyberspace. In addition to these calls for actions, in 1999, a decision was arrived to increase the fiscal spending on the

---

[205] U.S. Senate, "National Security and Information Age" (Washington, DC: Government Publishing Office, 1996), https://www.congress.gov/congressional-record/1996/9/28/senate-section/article/s11758-1?q=%7B%22search%22%3A%5B%22information+security%22%5D%7D&resultIndex=23.

[206] U.S. Senate, "National Security and Information Technology" (Washington, DC: Government Publishing Office, 1998), https://www.congress.gov/congressional-record/1998/10/12/senate-section/article/s12359-1?q=%7B%22search%22%3A%5B%22information+security%22%5D%7D&resultIndex=11.

cybersecurity by 40%.[207] It was an important step to increase national capabilities to enhance national cybersecurity strategies.

The role of the Congress as another securitizing actor was relatively low compared to the DoD and the Presidency. However, the congressional attempts by speeches and hearings may be vital for convincing the audience about significance of the cybersecurity which was a relatively new and strange subject. Empirically, it may be argued that the limited efforts of the Congress tried to support the works of other agencies to bring new measures to take necessary actions against cyber threats.

3.5 Building-up International Cybersecurity Strategy

International efforts for developing a more comprehensive cybersecurity strategy also began through the end of the 1990s. Similar to national evolution of the cybersecurity issue, it may be argued that this was related with the rising awareness of the cyber threats and increasing use of cyber attacks in international crises.

It has been already mentioned that neither the US nor NATO responded to cyber attacks during the Kosovo crisis, despite the fact that they had capability for hacking critical infrastructures of Serbia. It was widely explained by emphasizing the US commitment to legal principles or as any offensive response might be treated as war crime.[208] In such an environment, it may be expected that international community needs regulations at cyber domain.

The main attempt for international regulations came from Russian side. Russia proposed a resolution "developments in the field of information and

---

[207] Matt Hamblen, "Clinton Commits $1.46B to Fight Cyberterrorism" *CNN*, January 26, 1999, http://edition.cnn.com/TECH/computing/9901/26/clinton.idg/index.html; William J. Clinton, *Statement of Administration Policy: H.R. 4576 - Department of Defense Appropriations Bill, FY 2001*, *White House* (Washington, 2000), http://www.presidency.ucsb.edu/ws/index.php?pid=74826&st=cyber&st1=.

[208] "Pentagon Kept the Lid on Cyberwar in Kosovo."

telecommunications in the context of international security" to the First Committee of the United Nations General Assembly.[209] This is accepted as the starting point of the debate on arms control in cyber domain between Russian Federation and the United States.[210] The US rejected the Russian proposal.[211] It was not new for the US not to be a part of international regimes. In the case of the Kyoto protocol as well, US had shied away from signing when it was not totally compatible with its national interests. The refrainment of the Clinton Administration from an international agreement on cybersecurity could be explained through the characteristics of cyberspace which prevent detection of the aggressive power, and thus hinder any law enforcement. Therefore, it may be argued that due to the superiority of the US in both cyber offense and defense, the White House did not want to limit its power and capability in cyberspace through any institutionalization of cyberspace.

It is unavoidable that cyber operations critically required legal regulations that propose international law enforcement especially to define the results of varied types of cyber attacks and to control the use of cyber weapons as in the case of weapons of mass destructions. However, this brings a question of rationality of such a regulation for a technology superior state, the US who is able to utilize from the strategic advantages of cyberspace, despite the asymmetry issue. With respect to this fact, there was no consensus for an international cybersecurity strategy during the Clinton Administration. Therefore, one may argue that the relatively successful securitization move of the securitizing actors of domestic politics could not be observed at international arena.

---

[209] Tim Maurer, *Cyber Norm Emergence at the United Nations - An Analysis of the Activities at the UN Regarding Cyber-Security* (Cambridge, 2011), http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf.; The United Nations Office for Disarmament Affairs, https://www.un.org/disarmament/topics/informationsecurity/.

[210] "U.S. Military Grapples With Cyber Warfare Rules" *Reuters*, November 8, 1999.

[211] Ibid.

During this era, there was not a major successful attempt to take extraordinary measures for international cybersecurity strategy.

3.6 Conclusion

In general, policy environment of the first term of Clinton was vague following the end of the Cold War and emergence of more complex international political order. Cyberspace and cybersecurity found a place within the context of the adaptation process to new world order. Therefore, it can be said that in the first term of Clinton period, security of cyberspace was also downplayed by the Presidency because policies of the Administration had more passive characteristics. In the second term of the Clinton Administration, the critical nature of cyber threats was more apparent and the awareness increased. The increasing awareness was caused by the vulnerabilities and risk assessment and the economic interests based on free-market trends at home which were mainly consolidated by the primary cyber attacks of 1990s.

One may argue that this awareness led to a securitization move by the securitizing actors which were primarily the DoD and the Presidency. The DoD was more active in this process by the effective use of the speech act. At first, the DoD used the speech act to introduce the vulnerabilities of the US in cyberspace. This may be seen as the first step for securitization since it defined the referent object. Then, cyber threats were defined as emerging existential threats to the national security of the US. The uses of the critical words and phrases such as warfare, national security, battleground, and capabilities while mentioning cyberspace were highly critical to securitize the issue through speech act. The speech act was followed by the promotion of new strategies as extraordinary actions. Although relatively ordinary characteristic of these strategies which was based on enhancing information-sharing mechanism among public and private sectors of the US may undermine the evolution of cybersecurity from perspective of securitization, one may claim the existence of a securitization move at national level.

In this line, at national level, among the bureaucratic agencies, it may be argued that the DoD shaped the perceptions on cyberspace and cybersecurity during Clinton era. The position of the DoD stemmed from its explicit and distinct vulnerabilities due to cyber incidents. The position of the DoD was supported by the Presidential actions only in the second-half of the 1990s. Clinton, in person, tried to address the new threats emanating from cyberspace and the need to protect national security by enhancing protection of critical infrastructures through developing a common mechanism that included public and private sectors which was the base of risk-based strategies of the US. These may be interpreted as a relatively successful securitization move that increased public awareness through federal efforts.

At international level, one could not see many parallels with the national efforts. Although there was a call to develop an international cybersecurity strategy mainly by Russian side, there was no concrete support from the US. Because of this, one cannot claim of the existence of an international securitization move on the subject of cybersecurity during the Clinton Administration. However, Clinton era can also be defined as the burgeoning of strategic and tactical importance of cyberspace which became more obvious with the use of offensive cyber weapons during the Kosovo crisis. This era may also be accepted as the realization of opportunity-based strategies that is based on strategic use of cyberspace.

All in all, for Clinton era, it could be argued that there were multilateral efforts of securitizing actors at home in order to have a successful securitization move. Contrary to the national attempts, the US did not seem to be willing to cooperate on issues of institutionalism and international law which may put an enforcement mechanism by preventing offensive use of cyberspace as it would limit its own opportunities to strike back in the international cyberspace.

CHAPTER 4

BUSH ERA: CYBERSECURTIY IN THE SHADOW OF TERRORISM

4.1 Introduction

The discussion regarding the rapid evolution of cyberspace and cybersecurity in the US entered relatively a new phase by the Bush Administration, particularly with the impact of rising terrorism discourse. This chapter aims to analyze evolution of cybersecurity through the discourse of terrorism of the Bush Administration in the light of war on terrorism.

In order to understand the evolution of cybersecurity strategies and its linkage with national security, it is essential to discuss effects of the general security policy of the Bush Administration which was primarily composed of global war on terrorism. In this analysis, it is also important to analyze the positions and the roles of main bureaucratic agencies in defining cyber threats and cybersecurity. In doing so, first an overview of the foreign policy framework of the Bush Administration will be offered in order to shed light on the main policy issues. Then, the roles of principle agencies in particular the Department of Homeland Security, the Department of Defense and the President will be analyzed. In addition to them, the effects of non-governmental organizations and agencies will be discussed concerning the national dimension of the cybersecurity. In order to shed light on international repercussions, the last section will focus on questioning the development of the cybersecurity at international arena considering the Russian use of cyberspace. Thus this chapter will analyze the effects of primary security issues on the emergence of new threat perceptions in the US during presidency of Bush.

4.2 Foreign Policy Framework of the Bush Administration

During the election campaign, George W. Bush clearly pointed out his position on foreign policy issues in his speech at Ronald Reagan Presidential Library, titled *'A Distinctly American Internationalism'*:

> American foreign policy must be more than the management of crisis. It must have a great and guiding goal: to turn this time of American influence into generations of democratic peace. This is accomplished by concentrating on enduring national interests. And these are my priorities. An American president should work with our strong democratic allies in Europe and Asia to extend the peace. He should promote a fully democratic Western Hemisphere, bound together by free trade. He should defend America's interests in the Persian Gulf and advance peace in the Middle East, based upon a secure Israel. He must check the contagious spread of weapons of mass destruction, and the means to deliver them. He must lead toward a world that trades in freedom. And he must pursue all these goals with focus, patience and strength. I will address these responsibilities as this campaign continues. To each, I bring the same approach: A distinctly American internationalism. Idealism, without illusions. Confidence, without conceit. Realism, in the service of American ideals.[212]

In this statement, Bush signaled a foreign policy which would be based on liberal values of democracy and free trade with the support of realist applications. The national and international developments after his election strengthened his position on pursing a realist approach by merging it with idealism.[213] It was the September 11, 2001 attack that shaped the whole picture of the international politics and security studies in the first decade of 21th century. War on terrorism and growing terrorist threats, fight against 'axis of evil', non-proliferation of weapons of mass destruction and invasion of Afghanistan and Iraq were the main developments that affected the Bush period. It

---

[212] McCormik, *American Foreign Policy and Process*, p.178.; George W. Bush, "A Distinctly American Internationalism," November 19, 1999, http://fas.org/news/usa/1999/11/991119-bush-foreignpolicy.htm.

[213] McCormik, *American Foreign Policy and Process*, p.182.

could be said that while these developments and policy-making of the Bush term were important factors in defining the US policy framework, they were also central in analyzing the main policy issues of the 2000s.

The terrorist attacks on the World Trade Center and the Pentagon which are at hearth of the US have opened the phase of fighting against terrorism for the US. This had tremendous impact on political agendas of all bureaucratic agencies and public in general. The major impact of 9/11 has been to lead the US to pursue more assertive policies at national and international levels.[214] At national level, there was great congressional support for actions of the Bush Administration when it was about combatting and defeating terrorism. Congressional authorization of the president to use of force against terrorist attacks by the 'Authorization for Use of Military Force', the US PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism), and the Department of Homeland Security Act of 2002, which were adopted by an overwhelming majority in the Congress can be seen as clear examples of this support. With this support, the Bush Administration expanded its foreign policy agenda. It included humanitarian interventions, peacekeeping operations, fighting against 'axis of evil' –Iran, Iraq and North Korea- and resolving internal conflicts especially in the Middle East in addition to the main combat against terrorism.[215]

At international level, the Bush Administration mainly followed the path of unilateral actions whenever the multilateral actions were in deadlock.[216] In this light, it is generally accepted that unilateral and preemptive actions were central parts of the Bush

---

[214] Ibid., pp.180-181.

[215] Ibid., pp.180-181.

[216] Ibid., p.187.

Doctrine in achieving national and international security.[217] As shown below, the unilateral characteristic was asserted in the *National Security Strategy, 2002*, which drew the international strategy of the US for the challenges from new threats:

> While the United States will constantly strive to enlist the support of the international community, we will not hesitate to act alone, if necessary, to exercise our right of self-defense by acting preemptively against such terrorists, to prevent them from doing harm against our people and our country.[218]

After his reelection, Bush signaled that the promotion of democracy will be the main goal of his foreign policy in the second term.[219] However, the second term of the Bush Administration confronted growing criticism at home and abroad due to the unilateral actions of Bush especially after the Iraqi War.[220] It may be argued that the decreasing level of public and international support with growing skepticism on the policies of the Bush Administration prevented Bush from focusing on other critical policy issues like cybersecurity.

All these imply that the main mission of the Bush Administration was global war on terrorism. In this sense, efforts about cybersecurity would find its place depending upon its linkage to terrorism particularly in the first years of Bush. In the second term of the Bush Administration, there was decreasing level of national and international support for the policies of Bush which would also undermine the concerns regarding cybersecurity.

---

[217] Robert Jervis, "Understanding the Bush Doctrine," *Political Science Quarterly* 118, no. 3 (2003): 365–88.

[218] George W. Bush, *The National Security Strategy of the United States of America* (Washington, DC, 2002), http://www.state.gov/documents/organization/63562.pdf.

[219] McCormik, *American Foreign Policy and Process*, p.196.

[220] Ibid., p.196.

4.3 Developing Cybersecurity Strategy and Proliferation of Cyberterrorism Discourse in Domestic Politics

Prior to 9/11 attacks, it can be said that there was an increasing rhetorical awareness of cyberterrorism. For instance, in his election campaign, Bush also paid attention to cyberterrorism by declaring that "American forces are overused and underfunded precisely when they are confronted by a host of new threats and challenges — the spread of weapons of mass destruction, the rise of cyberterrorism, the proliferation of missile technology."[221] It is very remarkable that Bush mentioned cyberterrorism along with weapons of mass destruction and missiles, since they are treated as the main tools of traditional warfare and traditional threat perceptions. This underlined the significance of the cybersecurity along with the terrorism since the US cyberspace is highly vulnerable to cyber threats not only from state actors but also from non-state actors, due to increasing terrorist attacks and variety of actors in cyberspace. After September 11, 2001, terrorist attacks, there were growing concerns for national security of the US in the line of terrorism. Therefore, it may be expected that cybersecurity would be dealt within the context of the national security of the US by Bush as much as it was linked to terrorism as a continuation of Clinton era's legacy with respect to cybersecurity and cyberterrorism.

It was the concept of cyberterrorism that grabbed the public attention more in the first years of Bush Administration since terrorism was the primary issue of Bush after 9/11. Following the catastrophic terrorist attacks of 9/11, discourse on cyberterrorism and cyber threats were again reshaped as the attacks posed serious challenges to the US national security perceptions and interests. Cyberterrorism was defined as "unlawful attacks and threats of attacks against computers, networks and the information stored

---

[221] Chuck Vinch, *Questions Still Unanswered on Bush's Plans for Military* (Washington, 2000), http://fas.org/news/usa/2000/usa-001109.htm.

therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives."[222] The motivation behind the attacks is the central part that distinguishes cyberterrorism from traditional forms of cyber attacks such as hacktivism which does not imply pursuit of political goals.[223]

On the other hand, the protection of the critical infrastructure from basic cyber attacks was still important, even though with a lower emphasis compared to cyberterrorism discourse. Despite that, some incidents fostered significance of critical infrastructure for national security. For instance, in 2003, one of the fastest computer worms which is called Sapphire was discovered. Due to its speed and extend that affected all the internet connections around the globe in a very limited time, 43 % of the US machines were infected and the infection resulted in slowing down of Web services, disruption in bank services and airlines.[224] Again in 2003, the Blaster computer worm was spread. Its intrusion on computer systems of a closed nuclear power plant in Ohio clearly displayed the importance of cyber attacks.[225] These are the early cases of the Bush Administration that warned American public about their vulnerabilities even to more basic cyber attacks.

---

[222] Dorothy E. Denning, "Cyberterrorism" Testimony before the Special Oversight Panel on Terrorism, US House of Representatives, May 23, 2000, http://www.iwar.org.uk/cyberterror/resources/house/00-05-23denning.htm.

[223] Ibid.

[224] Brian Krebs, "Bush Approves Cybersecurity Strategy," *Security Focus*, 2003, http://www.securityfocus.com/news/2204; David Moore et al., "Sapphire/Slammer Worm Shatters Previous Speed Records For Spreading Through The Internet," *ScienceDaily*, 2003, https://www.sciencedaily.com/releases/2003/02/030205073007.htm.

[225] Clay Wilson, *Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress*, 2003, p.3. https://fas.org/irp/crs/RL32114.pdf.

With the pressing issues such as terrorist attacks and urgency of critical infrastructure protection there were several internal attempts in order to enhance cybersecurity as it will be examined below.

4.3.1 Role of the Department of Homeland Security

The Department of Homeland Security (DHS) was established on 25 November 2002, by the Homeland Security Act of 2002 as a result of the terrorist attacks of September 11, 2001. Since then, the DHS, which has incorporated cybersecurity into its main topics, is one of the popular executive agencies on security issues. In the field of cybersecurity, the DHS can be seen as the coordinator among the bureaucratic agencies and sectors of the US.[226] It could also be stated that concern of the DHS about cybersecurity derives from difficulty of securing cyberspace which is vital for critical infrastructure. In addition to the protection of critical infrastructure, combating cyber crime, securing federal networks and information sharing are main themes that the agency works for.[227] In line with this, the National Cybersecurity Division (NCSD) under the Department's Information Analysis and Infrastructure Protection Directorate was established in 2003 with the aim of developing a comprehensive cybersecurity strategy to protect critical infrastructure.[228] It was the first institutional attempt of the DHS to promote national cybersecurity strategy of the US.

As an early attempt, a roadmap was planned to secure cyberspace under the leadership of Richard Clarke, the National Coordinator for Security, who is called the first 'cybersecurity czar' and the head of the President's Critical Infrastructure Advisory

---

[226] Bush, *The National Strategy to Secure Cyberspace*.

[227] "Cybersecurity," *Department of Homeland Security*, https://www.dhs.gov/topic/cybersecurity

[228] "National Cybersecurity Division Resilient Accord Read Ahead," *Department of Homeland Security*, https://www.fbiic.gov/public/2010/sep/NCSD_Information_for_Resilient_Accord_20100310_v00.pdf. (Accessed on 07.4. 2016)

Board. The final draft of the *National Strategy to Secure Cyberspace* which was released by the DHS in 2003 tried to outline strategic objectives and actions that were to be taken with the purpose of securing cyberspace.

There are two main points to be mentioned about this document. Firstly, this document can be seen as one of the primary documents that clearly offer a roadmap for a strategy to secure cyberspace in Bush era by suggesting an initiative as a response to cyber attacks. Secondly, it was also a roadmap which was built on the ground of collaborative actions of public-private sectors by accepting the strategic challenges from the ascending cyberspace.[229] In part of the Letter from President of the *National Strategy to Secure Cyberspace*, 2003, Bush clearly stated that "the cornerstone of America's cyberspace security strategy is and will remain a public-private partnership."[230] The NCSD has been responsible for implementing this overtly emphasized cooperation which included enhancing capabilities of each sector on analysis, management and response to reduce vulnerabilities of cyber incidents which were vital for the US economy and national security.[231] Establishment of a special division and the responsibilities attached may be seen as decisiveness of the US for developing a working mechanism between public and private sectors. This decisiveness may also indicate the pessimist standing of the new administration in the subject of cybersecurity.

This strategic document also emphasized the instantaneity and attribution problem, which are very crucial in analyzing cyberspace as cyber-pessimists clearly underline as

---

[229] Bush, *The National Strategy to Secure Cyberspace*.

[230] Ibid.

[231] Ibid. P.x

distinguished characteristics of cyberspace to deal with the threats from cyberspace.[232] However, this comprehensive document was criticized by many analysts and security experts. They claimed that these recommendations and motives of this strategy would never be actualized unless there was a strong and specific implementation structure that prompted private sector to take necessary actions.[233] Besides the lack of an implementation mechanism, incentives of the White House on cybersecurity were not very convincing because it was not given a primary role in time of fighting against terrorism.[234] In terms of securitization, the lack of an implementation mechanism also undermined the speech act efforts since taking extraordinary measures is vital for finalizing the securitization.

In February 2004, the DHS published its general guiding principles in the document of *'Securing Our Homeland'* which was based on combatting terrorism. According to the strategic plan of the DHS, three objectives to secure homeland were defined. These were directly related with the terrorism by preventing terrorist attacks, decreasing the level of vulnerabilities and damage to such attacks.[235] As it could be expected in the information age, vulnerabilities in the information age do not only derive from physical world but also from virtual world. In this vein, the DHS underlined the importance of

---

[232] Ibid.

[233] Dennis Fisher, "Cyber Plans Future Bleak," *E-Week*, 2003, http://www.eweek.com/c/a/Security/Cyber-Plans-Future-Bleak.

[234] Michael Fitzgerald, "Homeland Cybersecurity Efforts Doubted," *Security Focus*, 2003, http://www.securityfocus.com/news/3043; Krebs, "Bush Approves Cybersecurity Strategy"; "FBI Warns of Fake Govt Sites, ISIS Defacements." (Accessed on 28-08-2015)

[235] Department of Homeland Security, "Securing Our Homeland:U.S. Department of Homeland Security Strategic Plan" (Washington, DC: Department of Homeland Security, 2004).

reducing vulnerabilities of infrastructure at both physical domain and cyberspace.[236] This was important to understand the awareness of the DHS on such a critical topic.

In the consecutive years, the agency worked for fulfilling its missions as projected in the *National Cybersecurity Strategy* and the *Securing Homeland*. For instance, in 2006, the DHS administered and coordinated a 'cyber storm' which may be defined as a simulation in exercising response and recovery mechanism in time of a cyber attack.[237] This may be interpreted as a crucial step to materialize the information-sharing mechanism between public and private sector. Moreover, such an exercise was also vital to predict and classify the vulnerabilities and required responses. Although these attempts of the DHS to take some emergency measures for enhancing national cybersecurity were highly remarkable, they could not prevent cyber attacks on the DHS networks which were reached 884 cyber incidents during 2005-2006.[238] The inability to prevent such attacks may also increase the public awareness for the vulnerabilities of the US.

The Comprehensive National Cybersecurity Initiative (CNCI) of the Bush Administration, which was based on the idea of strengthening national cybersecurity through defensive and counterintelligence activities of all related sectors and federal agencies, was the final attempt that regulated roles and responsibilities of the DHS.[239]

---

[236] Ibid.

[237] Department of Homeland Security, "Cyber Storm Exercise Report" (Washington, DC: Department of Homeland Security National Cybersecurity Division, 2006).

[238] Robert Westervelt, "DHS Suffered More than 800 Cyber Attacks in Two Years" *Computer Weekly*, June 25, 2007, http://www.computerweekly.com/news/2240081110/DHS-suffered-more-than-800-cyber-attacks-in-two-years.

[239] "The Comprehensive National Cybersecurity Initiative," *The White House*, https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative (Accessed on 18.05.2016)

The CNCI which was an initiative that took place in between presidential terms of Bush and Obama was actually planned by Bush in *National Security Presidential Directive-54* and *Homeland Security Presidential Directive-23* in January 2008. Therefore, although preliminary actions of the DHS on securing cyberspace dated back to first term of Bush Administration, it could be said that its mission has become more clear through the end of the decade by the realization of the CNCI. With respect to role of the DHS in securitizing the cyberspace, it may be argued that the DHS was not very active in defining and emphasizing the referent object and the existential threat. It concentrated more on developing some emergency measures like enhancing partnership mechanism as necessitated by its coordinating role. For this reason, one may argue that the DHS, as one of the primary securitizing actors, could not effectively use its securitizing power in the age of war on terrorism.

4.3.2 Role of the Department of Defense

During the Clinton period, it was the DoD which was mainly responsible for cybersecurity strategy. This began to change with the establishment of the DHS as a critical bureaucratic agency in terms of national security. Nevertheless the position of the DoD was still significant in strategic planning of cybersecurity since it was the main agency that conducted offensive and defensive operations in cyberspace. Moreover, in international arena, the primary role still belonged to the DoD.[240]

It could be argued that there was no change in the threat perception of the DoD as far as cyberspace was highly concerned, because vulnerability of the US in the cyber domain remained the same or even increased as the US military dependence on critical infrastructure increased. Additionally, perception of high level of vulnerabilities was consolidated as a result of the rising cyberterrorism discourse.

---

[240] Bush, *The National Strategy to Secure Cyberspace*.

Even though there was no empirical example of an act of cyberterrorism, the evidence which implied that the access to advance technologies by terrorist organizations called for actions. This made the issue more vital for the DoD since the role in taking actions against terrorist organizations primarily belonged to it. In 2003, in the *Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress* which aimed to address role of critical agencies, in particular the role of the DoD, in the field of cyberterrorism, a Specialist in Technology and National Security Foreign Affairs, Defense, and Trade Division reported that:

> Members of Al Qaeda and other terrorist groups have a record of using computer networks in planning terrorist acts. Evidence suggests that terrorists used the Internet to plan their operations for September 11, 2001. Mouhammed Atta, the leader of the attacks, made his air ticket reservations online, and Al Qaeda cells reportedly were using the Internet-based telephone services to communicate with other cells overseas. Khalid Shaikh Mohammed, mastermind of the attacks against the World Trade Center, reportedly used the Internet chat software to communicate with at least two airline hijackers. International terrorist groups, including Al Qaeda, are also known to use advances in technology such as optoelectronics (such as military night-vision devices), special communications equipment, GPS systems, and other electronic equipment, according to the DHS officials. The DHS Homeland Security Bulletins advise that many terrorists may now have access to very expensive high technology equipment.[241]

It was critical to address increasing capabilities of terrorist organizations in order to evaluate the capabilities of the DoD in responding these threats. In addition to the increasing capabilities of terrorist organizations, it was expected that terrorists' access to advanced technologies would increase the risk posed by terrorist-sponsoring states which were defined as Cuba, Iran, Iraq, Libya, North Korea, Syria, and Sudan as of

[241] Wilson, *Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress*.

2002.[242] It may be claimed that this extends the threat perception on cyberterrorism from terrorist organizations to state enemies by naming them. These two points might have been effective in strengthening measures taken by the DoD. In this respect, it also included a preparation for offensive use of cyber weapons.[243]

This broadened understanding was consolidated in subsequent strategic documents of the DoD. The *National Military Strategy of the US* in 2004 defined cyberspace as a new battleground in accordance with the extension of threat perception.[244] In the same document, it was accepted that impact of the cyber attacks may be 'disruptive' rather than being 'destructive' and 'lethal'.[245] Despite this fact –non-lethal impact- which downgraded the significance of cyberspace from the skeptical side, the importance of cyberspace was not ignored; rather it was included as a new sphere for the DoD to fight in the same line with the arguments of cyber-pessimists. This became clear in the *National Military Strategy of the United States of America: A Strategy for Today; A Vision for Tomorrow* which was prepared by the DoD in 2004 with the aim of identifying the role of armed forces to be successful in securing the US interests while fighting against terrorism. It may be understood from the following extract:

> Adversaries threaten the United States throughout a complex battlespace, extending from critical regions overseas to the homeland and spanning the global commons of international airspace, waters, space and cyberspace. [...] The Armed Forces must have the ability to operate across the air, land, sea, space and cyberspace domains of the battlespace. Armed Forces must employ

---

[242] Ibid.

[243] Ibid.

[244] Joint Chief of Staff, *The National Military Strategy of the United States of America: A Strategy for Today; A Vision for Tomorrow* (Washington, DC, 2004), p.1. http://archive.defense.gov/news/Mar2005/d20050318nms.pdf.

[245] Ibid., p.1.

> military capabilities to ensure access to these domains to protect the Nation, forces in the field and US global interests. The non-linear nature of the current security environment requires multi-layered active and passive measures to counter numerous diverse conventional and asymmetric threats. These include conventional weapons, ballistic and cruise missiles and WMD/E. They also include threats in cyberspace aimed at networks and data critical to US information-enabled systems. Such threats require a comprehensive concept of deterrence encompassing traditional adversaries, terrorist networks and rogue states able to employ any range of capabilities.[246]

In addition to the emphasis on a combined version of active and passive measures which may be defensive, deterrence was expected to be effective against varied range of actors with broadened capabilities. However, it was critical for this document since it underlined that the traditional deterrence capabilities may not work for adversaries with asymmetric capabilities.[247] In the same report, it was also claimed that:

> Some of these adversaries are politically unconstrained and, particularly in the case of non-state actors, may be less susceptible to traditional means of deterrence. Adversaries increasingly seek asymmetric capabilities and will use them in innovative ways. They will avoid US strengths like precision strike and seek to counter US power projection capabilities by creating anti-access environments.[248]

These texts were important since they showed consideration for new strategies apart from deterrence. It may be argued that the official documents and the reports on extension of threats, actors and battleground were used to show the urgency to develop new strategies for security of cyberspace by attempting a securitization move. In other words, it was critical for a securitization move to mention security weaknesses in

---

[246] Ibid., p.18.

[247] Ibid., p.5.

[248] Ibid., p.5.

cyberspace by labeling it as a new battleground in which varied range of actors may utilize.

The subsequent document of the *National Military Strategy for Cyber Operation*, 2006, aimed at emphasizing the superiority of the US in cyberspace by developing a comprehensive strategy for cyber domain. It was clearly claimed that a coordinated and a mix of offensive and defensive strategies needed to be developed because "the DoD cyberspace operations are strongest when offensive and defensive capabilities are mutually supporting."[249] With respect to this, "Network Operations, Information Operations, Kinetic Actions, and Law Enforcement and Counterintelligence" were described as primary actions to achieve this aim.[250] It was highly significant to underline the probability of using kinetic actions which means conventional military action in order to ensure superiority of the US in cyberspace while other policy statements and official documents almost offered the same strategies of developing capabilities in cyberspace by enhancing intelligence and information-sharing mechanisms. To put it differently, it was suggested that the defensive nature of the network and information operations which belong to cyberspace might be complemented either by defensive or offensive kinetic actions.[251] Moreover, highlighting the importance of an enforcement mechanism and counterintelligence investigations were also significant to materialize the main military strategy of deterrence in cyber domain. Therefore, one may argue that as the *National Military Strategy for Cyber Operation* tried to implement number of missions and strategies that

---

[249] Joint Chief of Staff, *The National Military Strategy for Cyber Operations*, p.10.

[250] Ibid., p.15.

[251] Ibid., p.15.

were mentioned before, it was the primary document that upheld promises for cybersecurity.

Another critical aspect of the official documents of the DoD could be found in the two sequential documents. At first, in the Quadrennial Defense Review Report of 2006, China as an emerging power came to the scene with an emphasis on developing military capabilities of China in both traditional and cyber domains. It was reported that:

> The pace and scope of China's military build-up already puts regional military balances at risk. China is likely to continue making large investments in high-end, asymmetric military capabilities, emphasizing electronic and cyber-warfare; counter-space operations. […] It -the US- will also seek to ensure that no foreign power can dictate the terms of regional or global security.[252]

Then in 2008, the *National Defense Strategy*, which addressed the strategic objectives of the US in an environment of global struggle against extremism, expressed the same point by reporting "China is developing technologies to disrupt our traditional advantages. Examples include development of anti-satellite capabilities and cyber warfare."[253] These may be seen as significant claims in terms of expanding the spectrum of threats by including both state and non-state actors. It may be argued that the inclusion of state and non-state actors by naming them and stressing their capabilities may be useful in convincing the audience for the required missions of ensuring national and global security in the cyberspace.

---

[252] Secretary of Defense, *Quadrennial Defense Review Report* (Washington, DC, 2006), pp.29-30. http://archive.defense.gov/pubs/pdfs/QDR20060203.pdf.

[253]"National Defense Strategy," The Department of Defense, p.22. http://www.defense.gov/Portals/1/Documents/pubs/2008NationalDefenseStrategy.pdf. (Accessed 10.04.2016)

In this line of expansion, it was again suggested that strategy of deterrence needed to be redesigned in that strategic document:

> Finally, the number of potential adversaries, the breadth of their capabilities, and the need to design approaches to deterrence for each, create new challenges. We must tailor deterrence to fit particular actors, situations, and forms of warfare. The same developments that add to the complexity of the challenge also offer us a greater variety of capabilities and methods to deter or dissuade adversaries. This diversity of tools, military and non-military, allows us to create more plausible reactions to attacks in the eyes of opponents and a more credible deterrence to them. In addition, changes in capabilities, especially new technologies, permit us to create increasingly credible defenses to convince would-be attackers that their efforts are ultimately futile. [...] We must build both our ability to withstand attack – a fundamental and defensive aspect of deterrence – and improve our resiliency beyond an attack. An important change in planning for the myriad of future potential threats must be post-attack recovery and operational capacity. […] For the future, the global scope of problems, and the growing complexity of deterrence in new domains of conflict, will require an integrated interagency and international approach if we are to make use of all the tools available to us.[254]

This text shows that it became more apparent that the traditional deterrence might not work in cyberspace. However, there was still no clear strategy of redesigning deterrence or methods to fight cyber threats. Therefore, the efforts for a successful securitization were downplayed since the DoD could not redesign strategies to secure cyberspace.

Although its primary position on national cybersecurity strategy was undermined with the establishment of the DHS, the DoD still played an important role both in pointing to the vulnerabilities and threats and in shaping strategic moves during the Bush Administration. It was very successful in targeting the adversaries and potential vulnerabilities in terms of securitization. It revealed the dangers about increasing

---

[254] Ibid., p.12.

capabilities of state and non-state actors in cyberspace by clearly addressing China as an emerging power at all levels and naming terrorist organizations that may cause damage. Moreover, the DoD accepted cyberspace as a newly emerging battleground. In this line, it brought the possibility of using cyberspace for offensive purposes. The emphasis on offensive measures is also vital for a securitization move since the model expects a concrete step as an extraordinary measure. All these provide that the expressions and documents of the military wing of the Bush Administration were still important for the evolution of the national strategy for cybersecurity.

4.3.3 Role of the President

It can be said that Bush was an active president in security issues in general. Therefore, although his main interests were focused on terrorism, cyberspace also grabbed his attention, as this domain clearly affected national security. As vulnerability of networked systems posed serious threats for public and government with DoS of 1990s, and computer worms which slowed down operation of systems, cybersecurity was also embedded in national security policies in Bush Administration.

However, Bush's policy and standing toward cybersecurity was a little bit ambiguous. For example, while he emphasized the rise of cyberterrorism during his election campaign which may be interpreted as an attempt for securitization of cyberspace, there was not any cyber- prefix in for instance one of the most critical documents of the Bush term, the National *Security Strategy of the United States of America*, 2002 which included the immediate strategic reactions of the US to the terrorist attacks.[255] There was only a limited emphasis on information operations and critical infrastructure protection as follows:

---

[255] Bush, *The National Security Strategy of the United States of America*, 2002.

> This broad portfolio of military capabilities must also include the ability to defend the homeland, conduct information operations, ensure U.S. access to distant theaters, and protect critical U.S. infrastructure and assets in outer space.[256]

Following the National Security Strategy of 2002, the *National Security Strategy of the United States of America*, 2006 did not also bring the cybersecurity issue to the table. One and only mention of the existence and acceptance of cybersecurity can be found while mentioning enhancing capabilities of the DoD in accordance with the new security challenges. It was stated that the DoD renewed its capabilities to accommodate 'disruptive challenges such as (such as biotechnology, cyber and space operations, or directed-energy weapons'.[257] These can be seen as an indication of negligence with regard to cybersecurity in the presence of other critical security issues, like terrorism.

Contrary to these critical and strategic documents of security strategy, Bush tried to organize cybersecurity strategy through National Security Presidential Directives (NSPDs) and Homeland Security Presidential Directives (HSPDs). In addition to these national security strategies, Bush issued *Critical Infrastructure Identification, Prioritization, and Protection, HSPD-7*. It can be defined as an organizing document since it specified roles of the DHS and other federal agencies in developing a national cybersecurity strategy. HSPD-7 may be interpreted as a pursuit for developing more organized and enhanced strategies to protect critical infrastructures from terrorists since it stated that:

> Critical infrastructure and key resources provide the essential services that underpin American society. The Nation possesses numerous key resources,

---

[256] Ibid.

[257] George W. Bush, *The National Security Strategy of the United States of America* (Washington, DC, 2006), http://www.state.gov/documents/organization/64884.pdf.

> whose exploitation or destruction by terrorists could cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction, or could profoundly affect our national prestige and morale. In addition, there is critical infrastructure so vital that its incapacitation, exploitation, or destruction, through terrorist attack, could have a debilitating effect on security and economic well-being. […] While it is not possible to protect or eliminate the vulnerability of all critical infrastructure and key resources throughout the country, strategic improvements in security can make it more difficult for attacks to succeed and can lessen the impact of attacks that may occur. In addition to strategic security enhancements, tactical security improvements can be rapidly implemented to deter, mitigate, or neutralize potential attacks.[258]

Although the influence of war on terrorism cannot be clearly seen in the blueprint for a national cybersecurity strategy, it was apparent in presidential directive's search for enhanced strategies against both states and non-state actors. This expression may be seen as one of the fundamental emphasis of Bush on security weakness of the US in cyberspace. It was an important example of the speech act that included both the referent object and existential threat in cyberspace. However, in terms of measures, this directive again mainly foresaw an agency-based and coordinated protection plan at national level similar to previous recommendations.[259]

Through the end of his presidency two presidential directives and a roadmap for a cybersecurity initiative were issued by Bush. In two concurrent presidential directives - NSPD-54, 2008 and HSPD-23, 2008- roles and responsibilities of bureaucratic agencies were again defined to enhance the national cybersecurity strategy. It may be argued that these directives did not bring major proposals for cybersecurity strategy apart from incentives on launching the Comprehensive National Cybersecurity

---

[258] George W. Bush, *Homeland Security Presidential Directive (HSPD-7): Critical Infrastructure Identification, Prioritization, and Protection, 2003* (Washington, DC, 2003), http://fas.org/irp/offdocs/nspd/hspd-7.html.

[259] Ibid.

Initiative (CNCI). Nevertheless, they were important in terms of the emphasis on the importance of strategic use of cyberspace. In the directives, it was stated that "the United States must maintain restricted access to and use of cyberspace for a broad range of national purposes"[260] because:

> The electronic information infrastructure of the United States is subject to constant intrusion by adversaries that may include foreign intelligence and military services, organized criminal groups, and terrorists trying to steal sensitive information or damage, degrade, or destroy data, information systems, or the critical infrastructures that depend upon them. Cyber criminals are intent on malicious activity, including the manipulation of stock prices, online extortion, and fraud. These activities cost American citizens and businesses tens of billions of dollars each year. Hackers and insiders have penetrated or shut down utilities in countries on at least three continents. Some terrorist groups have established sophisticated on-line presences and maybe developing cyber attacks against the United States.[261]

This text clearly displayed the security concerns of the US in cyberspace. It presented the aims of intrusions and damage that were caused by cyber criminals. These expressions were highly remarkable for securitization of cyberspace since the referent objects, existential threats and damage were epitomized by Bush. Moreover, they also demonstrated the impact of the discourse of terrorism on cybersecurity.

In this political environment, in general, it could be said that terrorist organizations were treated as main aggressors that threaten the US national security. Once, in HSPD-7, it was expressed that "terrorists seek to destroy, incapacitate, or exploit critical infrastructure and key resources across the United States to threaten national security,

---

[260] George W. Bush, "National Security Presidential Directive (NSPD-54) and Homeland Security Presidential Directive (HSPD-23): Cybersecurity Policy," 2008, https://fas.org/irp/offdocs/nspd/nspd-54.pdf.

[261] Ibid.

cause mass casualties, weaken our economy, and damage public morale and confidence."[262] It continued in other directives. Although the perceptions on opponents were getting expanded through the end of the Bush term, discourses and increasing emphasis on 'terrorist exploitation of vulnerabilities,' 'terrorist threats' and 'terrorist attacks on critical infrastructure' were the main features of the Bush Administration that differentiated him from the Clinton period.

The frequent use of 'terrorism' may be understood as a part of a speech act since the audience mainly concentrated on the discourse on terrorism, so that it would be easier for Bush to take some measures for other critical security issues. Therefore, although the emergency measures and strategies were not very satisfying for a successful securitization, Bush, in parallel to the arguments of cyber-pessimists, continued the securitization move of cyberspace by using speech act to refer to the referent objects and existential threats.

4.3.4 Role of the Legislative Efforts

Similar to the legislative efforts of the Clinton Administration, laws and regulations that may support a comprehensive national cybersecurity strategy were limited in Bush era. Therefore, the Congress was not very active as a securitizing actor during the Bush period.

One critical legislative development regarding the cybersecurity may be seen as E-Government Act of 2002 which regulated the use of the internet and electronic government services with the aim of promoting security and advantages of these services.[263] This law which was signed by Bush in 2002 included a subchapter for

---

[262] Bush, *Homeland Security Presidential Directive (HSPD-7): Critical Infrastructure Identification, Prioritization, and Protection*.

[263] Public Law 107–347: E-Government Act of 2002, 107th Congress, December 17, 2002. https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf

information security which was named Federal Information Security Management Act of 2002 (FISMA, 2002). It concentrated on the unauthorized use of information systems that could harm the US services. In order to overcome this problem, it defined some requirements for federal agencies. For instance, FISMA, 2002 "requires each agency's senior officials to provide security for the information and systems that support their operations and assets and to develop plans and procedures to ensure the continuity of such information and systems."[264] Such requirement would establish a ground for enhancing information-sharing mechanism starting among federal agencies.

Other than E-Government Act of 2002, there were no major legislations. But, there were some other efforts which may be considered as speech act. For instance, in one of the House Resolutions of the early Bush Administration, cyberterrorism was defined as "an emerging threat to the national security of the United States and the nation's electronic infrastructure."[265] It was an important step since it stated an emerging existential threat to the US national security. The speech act which defined existential threat was tried to be supported by more concrete actions. Cyberterrorism Prevention Act of 2001 and Cyberterrorism Preparedness Act of 2001 were offered consecutively. But, they could not find full support in the Senate, and could not become law.

Although the Congress was not totally negligent about growing threats from cyberspace, it could not put effective regulations that may help securitization move of cyberspace to implement more radical national strategies. Therefore, it may be argued

---

[264] Ibid.

[265] Expressing the sense of Congress regarding Internet security and "cyberterrorism", House of Representatives, 107th Congress, https://www.congress.gov/bill/107th-congress/house-concurrent-resolution/22?q=%7B%22search%22%3A%5B%22cyberterror%22%5D%7D&resultIndex=3

that the role of the Congress as a securitizing actor did not imply a linear growth rather there was a stagnation compared to the Clinton Administration

4.3.5 Role of the Non-Governmental Organizations and Agencies

It may be claimed that the effects of the media and research centers on national security issues have increased as the access to media tools has become easier with the spread of the Internet. Role of the non-governmental organizations and agencies was much obvious in the Bush Administration. Although they were not considered as securitizing actors, their role were crucial to support the main securitizing actors. There were growing number of reports, analysis and news based on vulnerabilities of cyberspace and cybersecurity.

In the early years of Bush Administration, risks and vulnerabilities of cyberspace were expressed as follows in the Washington Post:

> Cybersecurity is a problem that if not handled properly can dramatically affect millions of our citizens and undermine core institutions of our society just as effectively as a weapon of mass destruction. Fortunately, the terrorists have not yet demonstrated the capacity to carry out large-scale terror, but that doesn't mean they haven't achieved the necessary level of expertise to do it. And beyond state-sponsored terrorism and organized terror groups, there are countless small-scale cyber attackers and hackers lurking about -- mostly here in America -- trying to manufacture similar chaos, as we are currently being reminded by the latest "worm" attack. […] This situation is alarming when one considers that America has many thousands of dams, airports, chemical plants, federal reservoirs and of course power plants (of which 104 are nuclear), most of whose integral systems are operated and controlled by sophisticated computer systems or other automated controllers. These systems are now experiencing cyber attacks. In the second half of 2002 alone, 60 percent of

> power and energy companies experienced at least one severe cyber attack. Fortunately, none incurred catastrophic loss.[266]

It was critical to demonstrate the potential effects of cyber attacks by concrete data of examples and numbers. By doing this, through widespread communication tools of media, the US would be more effective and successful in convincing the audience to take any offensive measures in cyberspace, when necessary. Moreover, in addition to the cyber attacks from traditional actors, there was growing sensitivity to cyberterrorism although many of the examples of cyber incidents could not be defined as cyberterrorism, which means destructive or disruptive computer based attacks by terrorist organizations.[267] For instance, Dorothy Denning who is an important scholar on information security claims that cyberterrorism should not be ignored and not to be caught unprepared:

> The next generation of terrorists will grow up in a digital world, with ever more powerful and easy-to-use hacking tools at their disposal. They might see greater potential for cyber terrorism than do the terrorists of today, and their level of knowledge and skill relating to hacking will be greater. Cyber terrorism could also become more attractive as the real and virtual worlds become more closely coupled, with automobiles, appliances, and other devices attached to the Internet. Unless these systems are carefully secured, conducting an operation that physically harms someone may be as easy as penetrating a Web site is today. At least for now, hijacked vehicles, truck bombs, and biological weapons seem to pose a greater threat than cyber terrorism. However, just as the events

---

[266] Rick White and Stratton Sclavos, "Targeting Our Computers," *The Washington Post*, August 15, 2003, https://www.washingtonpost.com/archive/opinions/2003/08/15/targeting-our-computers/a8836d55-7dd7-401b-b170-d486e468241c/.

[267] Dorothy E. Denning, *Is Cyber Terror Next?* (New York, 2001), http://poli.haifa.ac.il/~terror/homer/27.9.02/cyber terrorism.htm.

> of September 11 caught us by surprise, so could a major cyber assault. We cannot afford to shrug off the threat.[268]

This looks like a call for taking measures against increasing level of dangers from cyberspace. An analogy with such a catastrophic event - the 9/11- may be interpreted as a complete effort to define measures against cyberterrorism. Moreover, it may also be argued that the fear of cyberterrorism derives from the fear from unknown. Capabilities, vulnerabilities and damage of cyber attacks represent challenges for security perception since they differ from traditional capabilities, vulnerabilities and attacks. It is because cyberterrorism issue proceeds on the probability of the cyber attacks. It can be clearly seen in the following extract:

> Unsettling signs of al Qaeda's aims and skills in cyberspace have led some government experts to conclude that terrorists are at the threshold of using the Internet as a direct instrument of bloodshed. The new threat bears little resemblance to familiar financial disruptions by hackers responsible for viruses and worms. It comes instead at the meeting points of computers and the physical structures they control. U.S. analysts believe that by disabling or taking command of the floodgates in a dam, for example, or of substations handling 300,000 volts of electric power, an intruder could use virtual tools to destroy real-world lives and property. They surmise, with limited evidence, that al Qaeda aims to employ those techniques in synchrony with "kinetic weapons" such as explosives.[269]

Additionally, statements of the Homeland Security Chair, John Gordon may grab the attention of the public since they touch upon cyberterrorism and traditional terrorism from the same security perspective by stating:

---

[268] Ibid.

[269] Barton Gellman, "Cyber-Attacks by Al Qaeda Feared," *Washington Post*, 2002, http://www.washingtonpost.com/wp-dyn/content/article/2006/06/12/AR2006061200711.html.

> Whether someone detonates a bomb that causes bodily harm to innocent people or hacks into a Web-based IT system in a way that could, for instance, take a power grid offline and result in a blackout, the result is ostensibly the same; both are acts of terrorism. […] "As long as there are major cybersecurity vulnerabilities, someone will exploit those," Gordon said. "The damage will be the same whether the attacker was a bored teenager, an organized criminal or a [hostile] nation or state. We need to focus on the vulnerabilities--and not get to hung up on who the attacker will be."[270]

During the Bush era one of the distinctive aspects was the increasing role of the media and political research centers in terms of cybersecurity compared to the Clinton era. Media also called next president for taking more serious action against rising cyber threats since there was an urgency to have more strict policies against losing relative power in cyberspace. This was done by analogies of September 11 and dealing with cybersecurity in the same basket as a matter as important as terrorism which was the main national security concern of the US, especially after the terrorist attacks.

4.4 An International Attempt?

Presidency of Bush did not come up with a great strategy for international cybersecurity despite the need for it which became more apparent with the strategic use of cyberspace to complement actions in traditional domains. Prior to 9/11, in June 2001, Secretary of Defense Donald Rumsfeld informed allies of the US to be ready for new threats in post-Cold War. Among these new threats, cyber attacks were categorized together with terrorism, weapons of mass destruction and high-tech weapons as future security challenges for trans-Atlantic alliance.[271] This can be seen as

---

[270] Elizabeth Montalbano, "Homeland Security Chair Likens 'Cyber Terrorists' to Al Qaeda," *CRN News*, 2004, http://www.crn.com/news/security/18825553/homeland-security-chair-likens-cyber-terrorists-to-al-qaeda.htm.

[271] Gerry J. Gilmore, "Rumsfeld To NATO: Prepare Now For Emerging Threats," *American Forces Press Service*, June 7, 2001, archive.defense.gov/news/newsarticle.aspx?id=45921.

intimation for international cooperation to secure cyberspace. The intimation became apparent with the *National Strategy to Secure Cyberspace*, 2003. It was stated that:

> America's cyberspace links the United States to the rest of the world. A network of networks spans the planet, allowing malicious actors on one continent to act on systems thousands of miles away. Cyber attacks cross borders at light speed, and discerning the source of malicious activity is difficult. America must be capable of safeguarding and defending its critical systems and networks. Enabling our ability to do so requires a system of international cooperation to facilitate information sharing, reduce vulnerabilities, and deter malicious actors.[272]

This underlined that the US national security strategy of cyberspace needed to be complemented by the international cooperation on cyberspace. It implied almost the same strategic moves of national arena for international domain. Concerning this, detecting and preventing through developing a system of 'international watch-and-warning networks' which was based on enhancing information sharing capabilities at international level were defined as central for a successful international cybersecurity strategy.[273] However, there were no consecutive concrete initiatives to materialize these strategic moves. Moreover, the discourses about international cybersecurity were not that much incisive and rigid compared to discourse at domestic politics.

Nevertheless, legal side of the cyberspace was not ignored thanks to efforts for promoting global integration into Council of Europe Convention on Cybercrime.[274] In 2004, this objective was realized with the ratification of the Convention on Cybercrime

---

[272] Bush, *The National Strategy to Secure Cyberspace*.

[273] Ibid.

[274] Ibid.

by the Council of Europe.[275] However, it should be noted that this convention was ratified by only 26 countries while there were 20 countries which signed but not ratified the Convention as of 2009.[276] Inadequateness of international strategies as in the case this relatively unsuccessful initiative may be seen as a clear example of difficulty of developing an international cybersecurity strategy.

Besides, during the Bush Administration, an international regulation that increased information sharing and response mechanism in cyberspace was not accomplished. The difficulty of developing a comprehensive international cybersecurity strategy may stem from the strategic importance of the cyberspace. Although characteristics of cyberspace make states more vulnerable to cyber attacks from non-state actors, they are also able to use cyberspace during international conflicts against states as well. It means that cyberspace offers states a hidden battleground to pursue their national interests.

There were two major cases that revealed strategic uses of cyberspace during Bush era. Subsequently, Russia used cyberspace offensively in Estonian and Georgian cases. Prior to intervention in Georgia, Russia already used cyber attacks against Estonia in 2007. In both cases, same methods such as DDoS attacks and web defacements were used against Estonia and Georgia.[277] In Estonian case, cyber attacks disrupted the use of electronic services.[278] In Georgian case, they had more strategic results since they

---

[275] Nazli Choucri, Stuart Madnick, and Jeremy Ferwerda, "Institutions for Cybersecurity: International Responses and Global Imperatives," *Information Technology for Development*, (2013), p.16.

[276] Ibid., p.16.

[277] Eneken Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified* (Tallinn, 2008), p.7. http://www.ismlab.usf.edu/isec/files/Georgia-Cyber-Attack-NATO-Aug-2008.pdf.

[278] Ibid., p.15.

damaged communication systems of a government which was in 'state of war'.[279] The two countries have relatively low level of dependence on network based critical infrastructures and operational cyberspace compared to the US and other high-tech states[280] so that it may be claimed that the damage is relatively low for them. On the other hand, it may also be argued that Russian strategic use of cyberspace shows the importance of cyberspace in complementing an action in physical domain even against an actor whose dependence on critical infrastructure is relatively low.

The strategic use of cyberspace by Russia also underlines the attribution problem one more time as the source of the cyber attacks in Estonia and Georgia remains unauthenticated exactly. By this means, cyberspace offers a strategic and tactical ground in complementing traditional operations by its legally unbinding character. Russian use of cyberspace for strategic purposes such as disrupting the communication by attacking government and civilian infrastructure during invasion of Georgia can be given as a good example of the refrainment from a restrictive international implementation on cyberspace.

The cases of Estonia and Georgia pushed only the NATO to pursue more active policies in cyberspace. In 2008, Bucharest Summit, it was decided to establish a Cyber Defense Policy by asserting "the need for NATO and nations to protect key information systems; to share best practices; and to provide a capability to assist Allied nations, upon request, to counter a cyber attack."[281] Although the efforts of the NATO were important for the partners in the alliance, it did not represent a general norm of

---

[279] Ibid., p.15.; John Markoff, "Before the Gunfire, Cyberattacks," *The New York Times*, August 12, 2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0.

[280] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, p.17.

[281] Jason Healey and Klara Totova Jordan, *NATO's Cyber Capabilities: Yesterday,Today, and Tomorrow*, 2014, https://www.ciaonet.org/attachments/26619/uploads.

behavior for cyberspace. Therefore, in such a strategic environment, it is not very surprising not to have general international standards to ensure cybersecurity at international level.

4.5 Conclusion

During Presidency of Bush, cybersecurity was still on the security agenda of the US even though there were more important issues like Afghanistan and Iraq operations. This study argues that through the end of the 43th presidency in post-9/11 period, critical infrastructure protection, and more inclusionary, defense of cyberspace were given emphasis by linking it with terrorism. As it can be observed, these national efforts that were supported by presidential directives almost urged the same internal strategy which was based on public–private partnership to enhance information sharing mechanism as in Clinton Administration. By means of all these reports and documents, national cybersecurity strategy of Bush term which was based on risk-based strategies can be summarized with two main points. First, securing cyberspace is all inclusive process. It means that not only federal agencies are responsible to ensure cybersecurity so that cooperative actions of public and private sectors are vital for this strategy. Secondly, as it is was suggested in the National Strategy to Secure Cyberspace, 2003, a response team which signals for offensive strategies is required either to prevent cyber attacks or to reduce vulnerabilities, if prevention is not possible. At international level, for me, cyberspace may be used for strategic purposes, so that although an international legal regulation seem to be required to prevent increasing level of cyber attacks, it is not very possible and rational to restrict strategic actions in cyberspace.

When it is compared to Presidency of Clinton, it may be argued that the speech act of securitizing actors were more limited but still striking. In terms of the roles of bureaucratic agencies, it can be said that responsibility of them expanded in the Bush era by inclusion of the DHS although the speech act by the DHS was very limited. Therefore, the inclusion did not bring a successful securitization of cybersecurity at

national level. Yet, it was still critically important to define cyberspace as a new 'battleground' and 'part of terrorism' by using speech act. It may be still defined as a securitization attempt. On the other hand, one could not speak of the international securitization of cyberspace. Although Russia, as one of the major opponents, utilized cyberspace, there was no clear international move to prevent further offensive actions. In addition to the emergence of the importance of the strategic use of cyberspace, two interlinked and internal reasons may prevent the US to call for an international action: the decreasing level of the Bush's credibility and increasing level of unilateral emphasis of the Bush Administration. Along with the reasons that may prevent proposals for international regulations and the strategic use of cyberspace, opportunity-based strategies continued to be influential at international level.

CHAPTER 5

OBAMA ERA: INCREASING EFFORTS

5.1 Introduction

This chapter will examine how the Obama Administration handles cybersecurity at national and international politics.

In parallel with the previous chapters on Clinton and Bush, this chapter will also start with a brief introduction with the aim of introducing foreign policy issues of the Obama Administration. Then, in the same line, it will try to show the growing internal concerns over cyberspace by relying on policy statements of the main bureaucratic agencies such as the Presidency, the Department of Homeland Security, the Department of Defense and the Congress regarding the legislative efforts. In order to examine the evolution of international cybersecurity strategy, primary cases of the Obama era, such as the use of sophisticated Stuxnet worm on Iranian nuclear facility, the outbreak of the cyber attacks on Sony Pictures Entertainment, and ongoing effects of Chinese cyber attacks will be examined. These are highly critical cases to evaluate and interpret bilateral and multilateral efforts of the US regarding the international cybersecurity strategy.

As a conclusion, in the light of above mentioned internal and international developments, it will be argued that the Obama Administration has brought in a 'change' on the development of the national cybersecurity strategy compared to the Clinton and Bush era. Obama, in person, has shown his intention by making more comprehensive efforts to demonstrate possible effects of emerging cyber threats on national security. Regarding the presidential attempts, other critical federal agencies

have mostly worked in coordination with the Presidency. On the other hand, lack of a clear international cybersecurity strategy, which stems from diverse threat perceptions among states about cyberspace and the possibility of strategic offensive use of cyberspace to complement an action in physical domain will be examined to show the 'continuity' of his predecessors' efforts.

5.2 Foreign Policy Framework of the Obama Administration

Barack H. Obama came to power in a political environment where there was a sharp decrease in public and international support for the policies of the president. In such a context, major promises of Obama during his election campaign focused on 'hope and change.'[282] The election of Obama as the 44th President of the US was very important not only for the US but also for the globe as a whole because he came with promises of 'hope and change.' Obama emphasized the global engagement with the US allies to promote democracy and freedom, and he was expected to pursue a multilateral approach in his foreign policy contrary to unilateral rhetoric of the Bush Administration. These two notions that were mostly stated during the election campaign of Obama can be seen as a reflection of his motive for changing the direction of national and international policies of the US.[283] It has mainly implied 'resetting' the relations with major countries like Russia and ending running battles in Afghanistan and Iraq.[284]

---

[282] "Obama Speech: 'Yes, We Can Change,'" *CNN*, January 27, 2008, http://edition.cnn.com/2008/POLITICS/01/26/obama.transcript/index.html?eref=rss_latest; "Transcript: 'This Is Your Victory,' Says Obama," *CNN*, 2008, http://edition.cnn.com/2008/POLITICS/11/04/obama.transcript/; "Barack Obama's New Hampshire Primary Speech," *New York Times*, January 8, 2008, http://www.nytimes.com/2008/01/08/us/politics/08text-obama.html?_r=0. (Accessed on 14.04.2016)

[283] McCormik, *American Foreign Policy and Process*, p.212.

[284] Ibid., p.212.

In accordance with 'hope and change' and 'reset and restart', Obama announced his foreign policy priorities as follows: non-proliferation by 'stopping the use of nuclear weapons,' 'combating extremism within the rule of law,' 'sustainable global economy, which appear in the Millennium Development Goals and 'selective promotion of democracy'.[285] Regarding priorities of his foreign policy agenda, Obama has dealt with the security issues such as wars in Afghanistan and Iraq, fighting against extremist groups, and Iranian nuclear ambitions, which were inherited from the Bush period in his first years. He has also been interested in developing bilateral relations especially with China and Russia. In addition to these critical policy issues, the Arab Spring occurred in one of the most conflictual regions of the world- the Middle East-. However, Obama has not been able to put forth radical changes in none-of these critical issues. For many analysts, foreign policy approach of the US during Obama's presidency has been relatively successful in keeping up with the rhetoric of 'change', Obama had promised; rather he was stuck between 'continuity and change.'[286] In the light of foreign policy issues and approach of Obama, this study argues that the cybersecurity strategies of the Obama Administration have displayed a certain degree of change, particularly at national domain when compared to policies of the previous administrations while demonstrating continuity, particularly at international level.

---

[285] Barack H. Obama, "Remarks by the President to the United Nations General Assembly" (New York: Office of the Press Secretary, 2009), https://www.whitehouse.gov/the-press-office/remarks-president-united-nations-general-assembly.

[286] Holland Jack, "Why Is Change so Hard? Understanding Continuity in Barack Obama's Foreign Policy," in *Obama's Foreign Policy: Ending the War on Terror*, ed. Michelle Bentley and Holland Jack (New York: Routledge, 2014); Róbert Ondrejcsák, *American Foreign and Security Policy under Barack Obama: Change and Continuity* (Bratislava, 2009), http://cenaa.org/analysis/american-foreign-and-security-policy-under-barack-obama-change-and-continuity/.

5.3 Increasing Efforts on Enhancing National Cybersecurity Strategy

Obama took the office in 2009 when there was growing sensitivity on cybersecurity in the light of the CSIS Report on cyberspace for 44th Presidency. It was a critical report since it underlined the growing risk of incremental capabilities of other states regarding the cyberspace by stating "our most dangerous opponents are the militaries and intelligence services of other nations. They are sophisticated, well resourced, and persistent.[287]" As explicitly stated in this report, increasing capabilities of 'dangerous opponents' could pose serious threats the US economic competitiveness. Additionally, higher level of exploitation of vulnerabilities in cyberspace could be the base of conflicts among states.[288] As indicated in this report, to protect the country against such conflicts and to keep the US competitiveness at top, it was seen necessary for the 44th Presidency to organize national and international cybersecurity strategies. Moreover, this report openly linked cybersecurity to the US national security, and also claimed that:

> Cybersecurity can no longer be relegated to information technology offices and chief information officers. Nor is it primarily a problem for homeland security and counterterrorism. And it is completely inadequate to defer national security to private sector and the market. This is a strategic issue on par with weapons of mass destruction and global jihad, where the federal government bears primary responsibility.[289]

Once, Bush, in his election campaign, equated cyberterrorism with weapons of mass destruction. Therefore, it was the second time that the issue of cybersecurity was

---

[287] Commission on Cybersecurity for the 44th Presidency, *Securing Cyberspace for the 44th Presidency*, p.13.

[288] Ibid., p.13.

[289] Ibid., p.15.

handled in the same category with weapons of mass destruction. In addition to this, it anticipated more clear strategies since cybersecurity is a critical national security issue that should be handled separately. Furthermore, as it can be deduced from the CSIS Report, the significance of cybersecurity and the call for top-level actions especially from the Presidency, were much more highlighted during Obama's presidency. Considering the implications of this report, this study argues that Obama was expected to be more active in defining more radical cybersecurity strategies at home.

5.3.1 Role of the Presidency

It was inevitable for Obama, whose computer systems at campaign headquarters during his election campaign were exposed to cyber attacks to take necessary actions to secure cyberspace. In presidential campaign of 2008, Obama actively used social networking tools which can be described as a part of cyberspace. However, as increasing level of dependence on critical infrastructures extends the vulnerabilities, very similarly, in this case, the election campaign of Obama was quite vulnerable to cyber attacks. Computers in the Obama's campaign headquarters were hacked with the purpose of stealing data about future policies and personal information of the users.[290] In November 2008, Federal Bureau of Investigation (FBI) reported that hackers who intruded into computer systems were from China but their origins and motives remained unknown.[291] It was also stated that the cyber intrusions were materialized despite the campaign team of Obama had been warned before the attacks.[292] This event proves that disregard for the potentiality of cyber attacks, lack of serious attention may lead to security breaches.

---

[290] "Obama, McCain Campaigns' Computers Hacked for Policy Data," *CNN*, November 6, 2008, http://edition.cnn.com/2008/TECH/11/06/campaign.computers.hacked/.

[291] Lee Glendinning, "Obama, McCain Computers 'Hacked' During Election Campaign," *The Guardian*, November 7, 2008, http://www.theguardian.com/global/2008/nov/07/obama-white-house-usa.

[292] Ibid.

Therefore, it caused concerns about cyberspace for the Obama Administration. He voiced these concerns in a speech as follows: "It was a powerful reminder: in this information age, one of your greatest strengths — in our case, our ability to communicate to a wide range of supporters through the Internet — could also be one of your greatest vulnerabilities.[293]" It was an important start for the Obama Administration since Obama was exposed to paradoxical nature of cyberspace.

In May 2009, President Obama issued a report that was called *'Cybersecurity Policy Review.'* This report directly asserted importance of cyberspace by underlining its leading role in every segment of actions in the globally-interconnected world.[294] It was like a roadmap of the cybersecurity policies that would be followed by the Obama Administration. In such a critical domain, a striking national and international start was advised through running more comprehensive campaign at home and strengthening national and international partnerships under the leadership of the White House.[295] The reason behind efforts for developing more comprehensive campaign stemmed from the requirement of increasing the public awareness.[296] It was important for securitization to catch the public awareness to take necessary measures.

Following the Cybersecurity Policy Review, rising significance of cybersecurity can be understood more clearly from the inclusion of cybersecurity into the National Security Strategy while the documents of his predecessor, Bush, had downplayed the issue by

---

[293] David A. Sanger and John Markoff, "Obama Outlines Coordinated Cyber-Security Plan," *The New York Times*, May 29, 2009, http://www.nytimes.com/2009/05/30/us/politics/30cyber.html?_r=0.

[294] Barack H. Obama, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, DC, 2009), https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[295] Ibid., p.v.

[296] Ibid., p.vi.

excluding it from the security strategy. In the *National Security Strategy of 2010*, which manifested the strategic security agenda of the US with a promise of 'renewing American leadership' at home and abroad[297], Obama started to analyze cyberspace by accepting it as a new domain, through differentiating it from traditional battlegrounds due to its asymmetric power and threat issues. He showed it by saying "in addition to facing enemies on traditional battlefields, the United States must now be prepared for asymmetric threats, such as those that target our reliance on space and cyberspace[298]" and "this means credibly underwriting U.S. defense commitments with tailored approaches to deterrence and ensuring the US military continues to have the necessary capabilities across all domains—land, air, sea, space, and cyber.[299]" Here, it was obvious that Obama referred to cyber threats as existential threats as anticipated by securitization theory by addressing their asymmetric characteristics.

As cybersecurity was treated as a national security issue, it was defined as a new pillar in strengthening security. It was asserted in the same document as:

> Cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation. The very technologies that empower us to lead and create also empower those who would disrupt and destroy. They enable our military superiority, but our unclassified government networks are constantly probed by intruders. Our daily lives and public safety depend on power and electric grids, but potential adversaries could use cyber vulnerabilities to disrupt them on a massive scale. The Internet and e-commerce are keys to our economic competitiveness, but cyber criminals have cost companies and consumers hundreds of millions of dollars and valuable intellectual property. The threats we face range from individual criminal

---

[297] Barack H. Obama, *National Security Strategy* (Washington, DC, 2010), pp.1-2. http://nssarchive.us/NSSR/2010.pdf.

[298] Ibid., p.17.

[299] Ibid., p.22.

> hackers to organized criminal groups, from terrorist networks to advanced nation states. Defending against these threats to our security, prosperity, and personal privacy requires networks that are secure, trustworthy, and resilient. Our digital infrastructure, therefore, is a strategic national asset, and protecting it—while safeguarding privacy and civil liberties—is a national security priority. We will deter, prevent, detect, defend against, and quickly recover from cyber intrusions and attacks by: investing in people and technology and strengthening partnerships.[300]

From this text, one may understand that it was the US national security that was threatened by the existential threats from cyberspace. Moreover, this document may be the first proof to understand how Obama would deal with cybersecurity and what he would do during his presidency. Firstly, he apparently showed his interest in dealing with cybersecurity as national security issue since this domain as a 'national asset' poses new and asymmetric threats due to vulnerabilities of the US.[301] Secondly, he was aware of the dangers coming from various actors in cyberspace that required improving offensive, defensive and recovery capabilities. In this regard, he called for a strategy that relied on enhancing partnership both in national and international domains.[302] In such a crucial document, it was understood that Obama attached more importance to cybersecurity more than his predecessors. Nevertheless, the roadmap for cybersecurity strategy was not that much different than his predecessors. Yet, he put more efforts in order to realize these strategies as it will be mentioned throughout this chapter.

In this line, at national level, Obama continued to implement regulations on cyberspace and cybersecurity that were inherited from the Bush Administration. He immediately focused on the CNCI. By the CNCI, two major points were determined: 'establishing a

---

[300] Ibid., pp.27-28.

[301] Ibid., pp.27-28.

[302] Ibid., pp.27-28.

defense mechanism against cyber threats by considering the vulnerabilities, and increasing information-sharing mechanism and counterintelligence capabilities' and 'promoting research and development in cyberspace to deter cyber intrusions'.[303] The continuation of the emphasis on defense may be interpreted as the continuation of risk-based strategies at national level. In order to achieve these national goals of the CNCI, responsibilities were allocated to almost every critical federal agency, particularly to the DHS. It was also important for increasing the numbers of the securitizing actors at federal level under an institutional structure.

President Obama's increasing efforts for sensitivity and awareness on cybersecurity was emphasized one more time when he declared October 2009 as the National Cybersecurity Awareness Month (NCSAM). It was an important proclamation which was lead by the President although the NCSAM has been administered by the DHS since 2004. Obama stated that "all Americans must recognize our shared responsibility and play an active role in securing the cyber networks we use every day.[304]" By this proclamation, he might have intended to get a nation-wide support for actions in cyberspace, which may be interpreted as a strong incentive to convince the audience as securitization theory suggests.

As of 2011, some important legislative efforts were carried out under the leadership of Obama the *Cybersecurity Legislative Proposal* was released. The distinguishing characteristics of this proposal were based upon its stress on the modification of the Computer Fraud and Abuse Act (CFAA) of 1986, which specified penalties for

---

[303] "The Comprehensive National Cybersecurity Initiative," *The White House*, https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative (Accessed on 17.04.2016)

[304] Barack H. Obama, *Presidential Proclamation: National Cybersecurity Awareness Month* (Washington, DC, 2010), https://www.whitehouse.gov/the-press-office/2010/10/01/presidential-proclamation-national-cybersecurity-awareness-month.

unauthorized actions to federal computer systems.[305] There have been changes and updates to some regulations with the aim of strengthening enforcement structure against cyber threats at least at home. Apart from the common views of enhancing cybersecurity by partnership and capabilities, relatively those changes with regard to strengthening enforcement structure were itemized in four main points as follows:

> 1) supplement the CFAA with a mandatory minimum penalty for damaging certain critical infrastructure computers;
>
> 2) increase the penalties for most violations of the CFAA;
>
> 3) modify the conspiracy and forfeiture provisions of the CFAA;
>
> 4) and make felony violation of the CFAA a racketeering predicate offense.[306]

These four points can simply be summed as portraying the attempts of the Obama Administration on extending the penalty mechanisms especially for cyber criminals, the purpose of which was to decrease or to prevent misuse of cyberspace. It can be seen as a concrete step to arrest cyber criminals and to fight them at legal level by forcing legislative actions. Therefore, this concrete step may also be stated as an attempt to take extraordinary measures in cyberspace as it was suggested in the securitization theory.

In October 2012, Obama issued Presidential Policy Directive-20 (PPD-20) on *the US Cyber Operations Policy* which superseded the *National Military Strategy for Cyber*

---

[305] Charles Doyle, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws* (Washington, DC, 2014), p.1. https://www.fas.org/sgp/crs/misc/97-1025.pdf.

[306] Gina Stevens, Legislative Attorney, and Jonathan Miller, *The Obama Administration's Cybersecurity Proposal: Criminal Provisions* (Washington, DC, 2011), p.2. https://www.fas.org/sgp/crs/misc/R41941.pdf.

Operation of 2006. This directive was very critical since it may be accepted as a blueprint in choosing and application of offensive and defensive measures and strategies in cyberspace, as introduced in the below extracts:

> The United States Government shall reserve the right to act in accordance with the United States' inherent right of self defense as recognized in international law, including through the conduct of DCEO* (Defensive Cyber Effects Operations). […] The United States Government shall identify potential targets of national importance where OCEO** (Offensive Cyber Effects Operations) can offer a favorable balance of effectiveness and risk as compared with other instruments of national power, establish and maintain OCEO capabilities integrated as appropriate with other U.S. offensive capabilities, and execute those capabilities in a manner consistent with the provisions of this directive.[307]
>
> The United States Government shall reserve use of DCEO to protect U.S. national interests in circumstances when network defense or law enforcement measures are insufficient or cannot be put in place in time to mitigate a threat, and when other previously approved measures would not be more appropriate, or if a Deputies or Principals Committee review determines that proposed DCEO provides an advantageous degree of effectiveness, timeliness, or efficiency compared to other methods commensurate with the risks; The United States Government shall conduct DCEO with the least intrusive methods feasible to mitigate a threat; The United States Government shall seek partnerships with industry, other levels of government as appropriate, and other nations and organizations to promote cooperative defensive capabilities,

---

* Defensive Cyber Effects Operations (DCEO): Operations and related programs or activities - other than network defense or cyber collection - conducted by or on behalf of the United States Government, in or through cyberspace, that are intended to enable or produce cyber effects outside United States government networks for the purpose of defending or protecting against imminent threats or ongoing attacks or malicious cyber activity against U.S. national interests from inside or outside cyberspace.

** Offensive Cyber Effects Operations (OCEO): Operations and related programs or activities - other than network defense, cyber collection, or DCEO - conducted by or on behalf of the United States Government, in or through cyberspace, that are intended to enable or produce cyber effects outside United States Government networks.

[307] Barack H. Obama, *Presidential Policy Directive (PPD-20): U.S. Cyber Operations Policy* (Washington, DC, 2012), pp.6-9. http://fas.org/irp/offdocs/ppd/ppd-20.pdf.

> including, as appropriate, through the use of DCEO as governed by the provisions in this directive; and Partnerships with industry and other levels of government for the protection of critical infrastructure shall be coordinated with the Department of Homeland Security (DHS), working with relevant sector-specific agencies and, as appropriate, the Department of Commerce (DOC).[308]

In this directive, it was asserted that the US would put either offensive capabilities or defensive capabilities in action, in accordance with the national and international laws in order to ensure its national interests. Moreover, 'emergency cyber actions' were also defined as an option for cyber operations. It was stated:

> A cyber operation undertaken at the direction of the head of a department or agency with appropriate authorities who has determined that such action is necessary, pursuant to the requirements of this directive, to mitigate an imminent threat or ongoing attack against U.S. national interests from inside or outside cyberspace and under circumstances that at the time do not permit obtaining prior Presidential approval to the extent that such approval would otherwise be required. [309]

In the implementation process of these actions, main role was given to the Secretary of Defense, which was the Pentagon. By the definition of 'emergency cyber actions,' it was also stated that the actions may be taken even without presidential authorization. The directive was interpreted by its assertive characteristics which implied more offensive prescriptions in cyberspace.[310] In the light of these, it may be asserted that the US tried to establish its own rules of engagement in cyberspace. To put it differently,

---

[308] Ibid., p.8.

[309] Ibid., p.4.

[310] Ellen Nakashima, "Obama Signs Secret Directive to Help Thwart Cyberattacks," *The Washington Post*, November 14, 2012, https://www.washingtonpost.com/world/national-security/obama-signs-secret-cybersecurity-directive-allowing-more-aggressive-military-role/2012/11/14/7bf51512-2cde-11e2-9ac2-1c61452669c3_story.html.

the US defined both national and international measures by this document. Therefore, it was another important step of the Obama Administration which may be understood as following the path of securitization move.

In 2012, four months later, another PPD, concentrating on the critical infrastructures, was issued. PPD-21: Critical Infrastructure Security and Resilience was the first time for the Obama Administration to emphasize the protection of critical infrastructure from both cyber and physical threats which were separate from cybersecurity. In the implementation process of these actions, the main authority lied with the Secretary of Homeland Security, the DHS. In the PPD-21, significance of coordinated protection of critical infrastructures for national prosperity was underlined as follows:

> Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure – including assets, networks, and systems – that are vital to public confidence and the Nation's safety, prosperity, and well-being.[311]

It was crucial to highlight the national prosperity to make public more aware about the cybersecurity. However, it may be argued and also understood that the directive did not offer a new strategy other than putting an emphasis on the coordinated and comprehensive efforts of the national and international partners.[312]

In 2013, Obama issued *the Executive Order 13636: Improving Critical Infrastructure Cybersecurity* which concentrated on developing a national cybersecurity strategy by using the Constitutional authority given to the President. By this order, it was again stated that "the cyber threat to critical infrastructure continues to grow and represents

---

[311] Barack H. Obama, *Presidential Policy Directive (PPD-21): Critical Infrastructure Security and Resilience* (Washington, DC, 2012), http://fas.org/irp/offdocs/ppd/ppd-21.pdf.

[312] Ibid.

one of the most serious national security challenges we must confront."[313] In order to sustain collaborative actions between public and private sectors and to improve capabilities of the private sector for protecting critical infrastructures from cyber attacks, development of a Cybersecurity Framework by the National Institute of Standards and Technology (NIST) was decided. Therefore, this document may be seen as a part of an inseparable whole as it stressed the main arguments on information-sharing and policy coordination among top agencies and sectors. Moreover, the executive order also worked for improved institutionalism for a developed national cybersecurity strategy. Contrary to the PPD-20 which tried to mobilize and organize aggressive actions to secure cyberspace at both national and international levels, this order has been repeating the same methods that have been offered over a decade. On the other hand, it could be said that this order was more than welcomed by public, who had strictly opposed to the bills that would violate private information because the Executive Order did not implied privacy concerns as much as the bills.[314] Ultimately, the use of presidential executive authority was welcomed in an environment where legislative efforts of the Congress for cybersecurity acts were in deadlock due to privacy concerns[315] which will be detailed throughout the chapter.

With the beginning of Obama's second term and through the end of his presidency, cybersecurity and offensive cyber actions have become more significant due to the Chinese and North Korean attacks on the US, and the use of cyber weapons by the

---

[313] Barack H. Obama, *Executive Order 13636: Improving Critical Infrastructure Cybersecurity* (Washington, DC, 2013), https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[314] Zack Whittaker, "Obama's Cybersecurity Executive Order: What You Need to Know," *ZDNet*, 2013, http://www.zdnet.com/article/obamas-cybersecurity-executive-order-what-you-need-to-know/.

[315] Gerry Smith, "Obama Drafts Cybersecurity Executive Order," *The Huffington Post*, September 12, 2012, http://www.huffingtonpost.com/2012/09/11/cybersecurity-executive-order-obama_n_1874250.html.

US towards Iranian nuclear facilities. As these cases raised the awareness about frequency of cyber actions, Obama issued a new Executive Order in 2015 to punish hackers. In *the Executive Order of Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities* of 2015, which empowered the Secretary of the Treasury to implement the sanctions against cyber threats, Obama stated that:

> Cyber threats pose one of the most serious economic and national security challenges to the United States, and my Administration is pursuing a comprehensive strategy to confront them. […] This Executive Order authorizes the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, to impose sanctions on individuals or entities that engage in malicious cyber-enabled activities that create a significant threat to the national security, foreign policy, or economic health or financial stability of the United States.[316]

This text complements the previous ones as speech act. However, there were still problems in the realization of extraordinary measures. For instance, authorizing sanctions program which can be defined as an emergency measure, may work effectively in preventing or deterring the increasing number of attacks in traditional domains. However, in cyberspace, as it is almost impossible to identify to the real origin of the cyber attacks, there will always be grey zones in implementation of this Executive Order. Nevertheless, this can be seen as an important attempt in terms of taking promising legal measures against a national emergency situation.

In February, 2016, the Obama Administration planned a *Cybersecurity National Action Plan* (CNAP) which aimed to 'secure our digital society and keep America

---

[316] Barack H. Obama, *Statement by the President on Executive Order "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities"* (Washington, DC, 2015), https://www.whitehouse.gov/the-press-office/2015/04/01/statement-president-executive-order-blocking-property-certain-persons-en.

competitive in the global digital economy'.[317] Along with the requirements of this plan, the President issued two new Executive Orders concerning cybersecurity. First one, which was officially named as *the Commission on Enhancing National Cybersecurity,* focused on establishing a commission. The Department of Commerce was decided to be in charge of this commission in order to improve risk management strategies especially of business sector.[318] Second one was about showing his consideration for privacy concerns that were derived from legislative actions on cybersecurity. In this line, Obama established a *Federal Privacy Council* to keep personal data safer.[319] With the establishment of these two new entities, it may be asserted that through the end of his presidency, Obama has still been working on enhancing cybersecurity strategies at national level.

Presidency of Obama can be seen as the peak of the urgency for improved cybersecurity. The issue was always on top of his security agenda during his presidency as it can be seen very clearly through the examination of the official documents of the PPD-21, Critical Infrastructure Security and Resilience and the Executive Order 13636, Improving Critical Infrastructure Cybersecurity. Both the Executive Order and the Policy Directive regarded cybersecurity as a national security issue. It was critically important in terms of speech act. Emphasis on the prioritization of cybersecurity can also be seen as an indication of how Obama has paid attention and responded to the calls for increasing federal responsibility with a new rhetoric that emphasized perceived threat and security. The definition of offensive, defensive and emergency

---

[317] "Fact Sheet: Cybersecurity National Action Plan," *The White House*, https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

[318] Barack H. Obama, *Executive Order: Commission on Enhancing National Cybersecurity*, *The White House* (Washington, DC, 2016), https://www.whitehouse.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity.

[319] *Fact Sheet: Cybersecurity National Action Plan*.

cyber operations were also critical for the US to specify the measures regarding cyberspace. Those more clear definitions which may be interpreted as the US's own rules of engagement in cyberspace may be seen as the successful securitization moves of Obama. Furthermore, his active positions in speech act and legislative actions as a securitizing actor have also been very critical for a securitization attempt.

5.3.2 Role of the Department of Homeland Security

It can be said that long-lasting efforts of the DHS have become more apparent with the Obama Administration that has pursued more active policies to secure cyberspace. Therefore, federal efforts of the DHS can be treated as to establish a roof for common policies among federal agencies in the field of cybersecurity. These efforts have been mainly defense-based from the beginning since federal system which is highly dependent on information technologies need protection. There have been some institutional attempts to materialize these defense-based strategies. For example, under the *National Cybersecurity Protection System* (NCPS), which was planned as a system to increase capabilities of 'intrusion detection, analytics, intrusion prevention, and information sharing,'[320] and the CNCI, EINSTEIN has been developed as an early warning system for cyber threats toward federal networks.[321] In addition to EINSTEIN, *Continuous Diagnostics and Mitigation* (CDM) program of the Department of Homeland Security's Federal Network Resilience Division, which was an initiative to protect government networks through 'providing adequate, risk-based, and cost-effective cybersecurity and more efficiently allocate cybersecurity

---

[320] "National Cybersecurity Protection System (NCPS)," *Department of Homeland Security*, 2015, https://www.dhs.gov/national-cybersecurity-protection-system-ncps

[321] "Securing Federal Networks," *Department of Homeland Security*, 2015, http://www.dhs.gov/topic/securing-federal-networks.

resources'[322] has also been supported and funded by the Congress which passed full-year spending bill.[323] These as part of risk-based strategies have been critical outcomes of ongoing securitization efforts for enhancing national cybersecurity strategy.

In name of protecting critical infrastructures, the DHS have worked for strengthening coordination between public-private sectors as it has always been the case. The DHS's *National Cybersecurity and Communications Integration Center* (NCCIC) and *NCCIC's Industrial Control Systems Cyber Emergency Response Team* (ICS-CERT), which have been the parts of information-sharing mechanism, have performed to develop collaborative relationship on cybersecurity during the Obama term.[324] *Critical Infrastructure Cyber Community Voluntary Program* (C^3VP) was launched in February, 2014 with the mission of enhancing capabilities and effectiveness in risk management. This program was comprised with number of actors from both government entities and private sectors.[325] Moreover, with the purpose of enhancing public-private partnership, the DHS established Critical Infrastructure Partnership Advisory Council which has offered a ground for communication and cooperation between government and representatives from private sector[326] in 2014. Within the legal framework of these institutions, the DHS has tried to work closely with public

---

[322] "Continuous Diagnostics and Mitigation (CDM)," *Department of Homeland Security*, 2015, https://www.dhs.gov/cdm

[323] Nicole Blake Johnson, "2014 Spending Bill Funds Continuous Monitoring Program," *Federal Times*, 2014, http://archive.federaltimes.com/article/20140114/CYBER/301140013/2014-spending-bill-funds-continuous-monitoring-program.

[324] "Protecting Critical Infrastructure," *Department of Homeland Security*, 2015, http://www.dhs.gov/topic/protecting-critical-infrastructure.

[325] "Critical Infrastructure Cyber Community Voluntary Program," *United States Computer Emergency Readiness Team (US-CERT)*, https://www.us-cert.gov/ccubedvp. (Accessed on 09.07.2015)

[326] "Critical Infrastructure Partnership Advisory Council," *Department of Homeland Security*, 2015, https://www.dhs.gov/critical-infrastructure-partnership-advisory-council

and private sectors. However, these institutional attempts of the DHS that were also strongly supported by the Presidency, generally lingered over privacy concerns from the public, which feared the sharing of private information.[327] It may be inferred that the DHS have worked intensively to realize one of the critical risk-based measure – public-private information-sharing mechanism- to secure cyberspace which have been suggested since the Clinton Administration. Efforts for fulfilling the mission also demonstrate the critical role of the DHS as a securitizing actor.

In *the Quadrennial Homeland Security Review Report (QHSR): A Strategic Framework for a Secure Homeland*, 2010, 'Safeguarding and Securing Cyberspace' was ranked as the fourth mission of the DHS in addition to issues non-related to cybersecurity. This mission was legitimized by showing the urgency of securing cyberspace since there are varieties of opponents that try to exploit vulnerabilities of the US. It was stated as:

> Yet as we migrate ever more of our economic and societal transactions to cyberspace, these benefits come with increasing risk. Not only is cyberspace inherently insecure as built, but as a Nation we face a variety of adversaries who are working day and night to use our dependence on cyberspace against us. Sophisticated cyber criminals and nation-states, among others, are among the actors in cyberspace who now pose great cost and risk both to our economy and national security. They exploit vulnerabilities in cyberspace to steal money and information, and to destroy, disrupt, or threaten the delivery of critical services.[328]

By attracting attention to adversaries, vulnerabilities and threats in cyberspace, the DHS tried to justify that it had worked hard at raising the public awareness and nation-

---

[327] Ellen Nakashima, "White House Declassifies Outline of Cybersecurity Program," *The Washington Post*, March 3, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/03/02/AR2010030202113.html.

[328] Janet Napolitano, "The Quadrennial Homeland Security Review Report (QHSR): A Strategic Framework for a Secure Homeland" (Washington, DC: Department of Homeland Security, 2010), https://www.dhs.gov/xlibrary/assets/qhsr_report.pdf.

wide support on national cybersecurity strategy which was defined as a part of its goal on promoting cybersecurity knowledge. Moreover, the emphasis on the variety of adversaries, similar to Bush's address on both terrorist organizations and terror-sponsoring nations, was also important to take measures against them when necessary. This may be seen as a significant contribution of the DHS as a securitizing actor through the speech act.

Furthermore, by this report, the DHS put forth more assertive attempts against cyber criminals by stating:

> Through law enforcement efforts, we must identify and locate domestic and international cyber criminals involved in significant cyber intrusions, identity theft, financial crime, and national security-related crimes committed utilizing the Internet. We must ensure that criminal organizations engaged in high-consequence or wide-scale cyber crime are aggressively investigated and disrupted, and their leaders arrested, indicted, and prosecuted. Through counterintelligence efforts, we must identify and thwart hostile intelligence collection activities and other cyber threats directed against the Nation.[329]

Enhancing legal aspects to improve cybersecurity was important to complement the speech act by putting more strict measures. This can also be seen as a base of Obama's PPD-20, which was a kind of definition of the US rules of engagement in cyberspace, and sanctions program that prescribe more aggressive action for any hostile nation or organization in a legal framework.

Following the mission of 'Safeguarding and Securing Cyberspace' as it was stated in QHSR 2010, the DHS published its blueprint for a secure cyberspace in 2011. There were two main components of the *Blueprint for A Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise* to implement the

[329] Ibid., p.56.

estimated strategies. Firstly, ensuring critical infrastructure protection which was described as the backbone of the US economy was emphasized.[330] Secondly, the intention of working for a nation-wide cybersecurity approach by integrating all related sectors, companies and even individuals were asserted.[331] It was apparent that in ten years from its establishment, the responsibilities of the DHS did not change with this document, but rather they were emphasized again. This may reveal that ongoing efforts for national cybersecurity strategy should not be thought apart from risk-based strategies as this blueprint re-emphasized by stating "risk-based decision making is defined as the determination of a course of action predicated primarily on the assessment of risk and the expected impact of that course of action on that risk."[332]

Significant progress of the strategies of the DHS by the leadership of the White House can be seen in its growing emphasis on law enforcement structure. It was asserted in QHSR 2014 as follows:

> Complementary cybersecurity and law enforcement capabilities are critical to safeguarding and securing cyberspace. Law enforcement performs an essential role in achieving our Nation's cybersecurity objectives by investigating a wide range of cybercrimes, from theft and fraud to child exploitation, and apprehending and prosecuting those responsible. […] DHS will work with other federal agencies to conduct high-impact criminal investigations to disrupt and defeat cyber criminals, prioritize the recruitment and training of technical

---

[330] Janet Napolitano, "Blueprint for A Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise" (Washington, DC: Department of Homeland Security, 2011), pp. 7-8. https://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf.

[331] Ibid., pp. 7-8.

[332] Ibid., p. D-5.

> experts, develop standardized methods, and broadly share cyber response best practices and tools.[333]

It can be seen as an important step to take necessary measures against cyber attacks. However, as it is already underlined, although it is relatively hard to identify criminals in cyberspace and the deterrence capability of law enforcement is relatively low, it was an important development in terms of implementing new measures in combating cyber attacks. In order to arrest the cyber criminals, the US federal agencies have worked hard. The decisiveness was obvious in the process of arresting a Russian cyber criminal, Evgeniy Bogachev, who was accused of computer hacking and wire fraud that resulted with more than $100 million loss with a remarkable reward bounty.[334] The actualization of such striking criminal cases and the appearance of them in the news together with the governmental efforts may be very important to increase the public awareness on cybersecurity breaches.

All the efforts and institutional attempts of the DHS demonstrate it as an important securitizing actor of Obama era. It has been successful in actualizing long-lasting efforts for public-private cooperation through launching major initiatives. It was important to materialize the extraordinary measures as securitization theory expects. Moreover, it, as an important agency for security, has supported the presidential calls to develop more effective legal measures through speech acts which may be seen in the QHSR. Therefore, it may be argued that the DHS have accomplished its responsibilities

---

[333] Jeh Charles Johnson, "Quadrennial Homeland Security Review" (Washington, DC: Department of Homeland Security, 2014), pp.44-45. https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf.

[334] "US Offers Highest-Ever Cybercrime Reward for Arrest Of Russian Hacker" Reuters, February 24, 2015, http://www.theguardian.com/us-news/2015/feb/24/us-highest-ever-cybercrime-reward-evgeniy-bogachev.

and coordinating role in implementing national cybersecurity strategy during the Obama Administration.

5.3.3 Role of the Department of Defense

The DoD has been one of the critical agencies since the beginning of the cybersecurity debate in Clinton period. In this respect, the establishment of the US Cyber Command (USCYBERCOM or CYBERCOM) in 2010 can be taken into account as the most important signal of how seriously the DoD has tried to deal with the challenges from cyberspace in both offensive and defensive manner. CYBERCOM was planned to enhance both offensive and defensive capabilities.[335] Defensive focus is related with assuring access to cyberspace, and offensive focus relies on improving capabilities for 'full spectrum military cyberspace operations'.[336] Its role and effectiveness were tried to be increased after the publication of PPD-20[337] which directly outlined the enhancement and the use of offensive capabilities in cyberspace. This attempt of institutionalism which brought military power to the scene was important in terms of securitization since it could be treated as an extraordinary measure.

By the year of 2011, the DoD was much more concerned about cyberspace since its functional ability at military, intelligence, control and business hinged on networks and computing devices.[338] Actually the policy statement of 2011 called *Strategy for*

---

[335] "U.S. Cyber Command Fact Sheet," *US Department of Defense*, 2010, http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet UPDATED replaces May 21 Fact Sheet.pdf.

[336] Ibid.

[337] Glenn Greenwald and Ewen MacAskill, "Obama Orders US to Draw Up Overseas Target List for Cyber-Attacks," *The Guardian*, June 7, 2013, http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas.

[338] "The Department of Defense Strategy for Operating in Cyberspace" (Washington, DC: Department of Defense, 2011), p.1. http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

Operating in Cyberspace, which was the first cyber strategy document of the DoD can be seen as a summary of ten years debates over cyberspace as it portrayed cyberspace as an operational domain, highlighting strategy of defense to protect networks, and advising public-private partnership at home and allying at abroad. Moreover, this document was important also for mentioning the asymmetries as:

> Low barriers to entry for malicious cyber activity, including the widespread availability of hacking tools, mean that an individual or small group of determined cyber actors can potentially cause significant damage to both the DoD and US national and economic security. Small-scale technologies can have an impact disproportionate to their size; potential adversaries do not have to build expensive weapons systems to pose a significant threat to US national security.[339]

It may be argued that the changing nature of power and the redistribution of power in cyberspace alongside the possibilities of asymmetric power and asymmetric vulnerabilities issues brought it into foreground the cybersecurity as a national security issue. According to the DoD *Strategy for Operating in Cyberspace of 2011*, cyber threats toward the DoD may raise in three ways as "theft or exploitation of data; disruption or denial of access or service that affects the availability of networks, information, or network-enabled resources; and destructive action including corruption, manipulation, or direct activity that threatens to destroy or degrade networks or connected systems."[340] It is understood that as activities of the DoD rely on a functioning cyberspace, these kind of threats may directly decrease its operational capability. To overcome such vulnerabilities, the DoD Strategy offered strategic initiatives for the DoD. Among them, international cooperation was underlined as a

---

[339] Ibid., p.1.

[340] Ibid., p.3.

requirement with respect to collective actions. Moreover, collective self-defense and collective deterrence arguments came to the scene with this report. It may be argued that developing a 'collective' understanding for cybersecurity with the allies of the US could be more fruitful tool for deterrence against hostile actions in cyberspace. Despite such efforts, this long-awaited strategic document of the DoD did not satisfy cybersecurity experts, and it was highly criticized since it lacked a new and critical strategy to response to cyber attacks when it is compared to previous policy statements of the DoD.[341] Nevertheless, it was important for a securitizing actor to continue its speech act through issuing official strategic documents.

After the first strategic document, the progress can be measured by the comparison with the following policy statement of the DoD, the *Department of Defense Cyber Strategy 2015*. Primarily, three missions of the DoD for the next five years were decided as follows. First, it must defend its own network; second, it must have capabilities to defend the US national interests; and lastly, it should be ready to pursue offensive actions in cyberspace to complement attacks in traditional domains.[342] In this line five strategic goals were determined. Among them, defending networks of the DoD and the US national interests, and collaboration with the US allies remained constant, while 'building and maintaining ready forces and capabilities to conduct cyberspace operations' were included as an emphasis on increasing offensive capabilities. In the light of these missions and strategic goals, it is possible to talk of a progress with regard to offensive strategies despite the ongoing emphasis on defensive measures.

---

[341] Sean Lawson, "DOD's 'First' Cyber Strategy Is Neither First, Nor a Strategy" *Forbes*, August 1, 2011, http://www.forbes.com/sites/seanlawson/2011/08/01/dods-first-cyber-strategy-is-neither-first-nor-a-strategy/#6d18112a33a8.

[342] Ash Carter, "The Department of Defense Cyber Strategy" (Washington, DC: Department of Defense, 2015), http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

There was also growing awareness on the requirement of building offensive capabilities. Establishment of the new *Cyber Mission Force* (CMF) which consisted of several teams to conduct offensive and defensive actions in cyberspace can be seen as an obvious example of this progress. Similar to the establishment of USCYBERCOM, the CMF can also be seen as an indicator of decisiveness of the US to promote national cybersecurity strategy. Moreover, it may be also interpreted actualization of the offensive and defensive missions of the DoD which were defined in the PPD-20, namely *the US Cyber Operations Policy*.

Contrary to the much criticized 2011 strategic roadmap of the DoD, the new cybersecurity strategy statement of 2015 was more welcomed. This time, it was approved by the public and the Congress since there was a great expectation to strengthen offensive capabilities of the US.[343] This support may be understood from the Congressional approval of the DoD budget request to increase spending on cyber capabilities. [344] Therefore, it may be argued that the DoD as a critical securitizing federal agency have made a progress through this strategic document which was also supported by other securitizing actor, the Congress.

By all these means, the DoD was expected to accomplish its missions for effective cybersecurity. The authorization of the DoD to conduct cyber operations even without presidential authorization for taking emergency actions and its emphasis on military activities have been the primary parts of the role of the DoD in securitizing cyberspace because these may be seen as important steps for extraordinary measures. The speech

---

[343] Elvina Nawaguna, "U.S. Needs Offensive Strategy to Deter Cyber Attacks: NSA Chief" *Reuters*, March 19, 2015, http://www.reuters.com/article/us-usa-defense-cybersecurity-idUSKBN0MF2G920150319.

[344] Cory Bennett, "Bipartisan Bill Would Speed DOD's Cyber Warfare Efforts" *The Hill*, May 2, 2016, http://thehill.com/policy/cybersecurity/268412-bipartisan-bill-would-speed-dods-cyber-warfare-purchases.

act efforts of the DoD which were examined under the previous administrations were supported by the strategic steps to materialize extraordinary measures during Obama era. For this reason, the role of the DoD has been highly critical in securitizing cyberspace to take necessary, and particularly risk-based, measures.

5.3.4 Role of the Legislative Efforts

During the Obama Administration, leading role of the presidency has been commonly followed by the Congress in strengthening legislative structure for cybersecurity. Therefore, Congressional actions should be examined in order to present legislative side of the securitization process.

Legislative actions may be important in order to enforce strategies that are proposed in the several policy statements of bureaucratic agencies. However, on subject of cybersecurity, in contrast to efforts of the bureaucratic agencies, there were no major legislative efforts that were enacted by the Congress before the late Obama period. Especially, there was disappointment about legislative efforts of the 111th and the 112th Congresses, while there were great expectations from the 113th Congress in 2013.[345]

Congressional involvement of the 111th Congress in the field of cybersecurity legislation was very limited. It could be understood from the higher level of involvement of the Executive Branch to push legislative branch which was driven especially by cybersecurity legislative proposals of Obama. There were about 80 drafts of cybersecurity legislations of the 111th Congress, but none of them has been able to pass and become law.[346] It was important that many strategic proposals stayed on paper

---

[345] Eric A. Fischer, *Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions*, 2013, https://www.fas.org/sgp/crs/natsec/R42114.pdf.

[346] Sandra I. Erwin, "Cybersecurity Legislation: Solution or Distraction?," *National Defense*, August, 2012, https://www.hollingsworthllp.com/uploads/23/doc/media.819.pdf.

despite the fact that federal agencies and executive branch prioritize of cybersecurity, legislative branch failed to turn these proposals into bills.

Although legislative activities of the 112th Congress did not meet the necessities, it held critical hearings to understand evolution of cybersecurity as a national security problem through legislative policymaking process. During the Obama Administration, Committees on Armed Services, Energy and Commerce, Financial Services, Foreign Affairs, Homeland Security, Judiciary, Oversight and Government Reform, Permanent Select Intelligence and Science, Space, and Technology have been the main Committees which are interested in cybersecurity of the US. According to report of the Congressional Research Service (CRS), the Committee on Homeland Security of the 112th Congress holds eleven hearings about cybersecurity of the US.[347] For instance, in the House Hearing titled *America is Under Cyber Attack: Why Urgent Action is Needed*, James A. Lewis who is a senior fellow and program director at the Center for Strategic and International Studies (CSIS), repeatedly pointed to cyber espionage and cyber crime as critical threats to the US national security. He emphasized that states should be treated as major opponents since they are more capable of intelligence activities thanks to their highly developed agencies.[348] These major opponents were named as Russia, China and two hostile states – North Korea and Iran since they endeavor to increase capabilities in cyberspace.[349] More noteworthy aspect of his statement was his emphasis on increasing capabilities of opponents which openly led to

---

[347] Rita Tehan, *Cybersecurity: Legislation, Hearings, and Executive Branch Documents*, 2015, p.33.

[348] "*America is Under Cyber Attack: Why Urgent Action is Needed" Hearing Before Committee on Homeland Security and Subcommittee on Oversight, Investigations, and Management, House of Representatives*, 112th Cong., 3 (2012) (statement of James A. Lewis) https://homeland.house.gov/hearing/subcommittee-hearing-america-under-cyber-attack-why-urgent-action-needed/

[349] Ibid.

security dilemmas. His statement underlined that new threats and increasing capabilities of other international actors could be seen as a summary of why cybersecurity has evolved as a national security issue for the US. On the other hand, addressing critical opponents was important in terms of speech act since the emphasis on existential threats from such leading international powers might help to produce more active security policies through effective securitization move.

In the light of the presidential proposals and statements, through the end of April 2013, the House of Representatives of the 113th Congress met for cybersecurity reform. Some analysts introduced this as 'cyber week' since several bills were introduced about cybersecurity. In this period, the Cyber Intelligence Sharing and Protection Act (H.R. 624, CISPA); Federal Information Security Amendments Act of 2013 (H.R. 1163, FISMA 2013); Cybersecurity Enhancement Act of 2013 (H.R. 756); and the Advancing America's Networking and Information Technology Research and Development Act of 2013 (H.R. 967) were passed and referred to the Senate.[350] These were significant to develop extraordinary measures for cybersecurity at national level.

CISPA may be seen as the most controversial proposed law about cybersecurity since it touched upon personal information sharing. In other words, it has been part of debate since the 112th Congress mainly because private companies like Google and Facebook or government were forced to provide third parties private information of users for the sake cybersecurity.[351] While the bill was supported by a wide range of companies from private sector, it was unacceptable for public and some civil-society organizations such as the Electronic Frontier Foundation, the Center for Democracy and Technology and American Civil Liberties Union due to privacy concerns were based on danger of abuse

---

[350] Ibid., p.7.

[351] Jason Reed, "US House of Representatives Passes CISPA Cybersecurity Bill" *Reuters*, April 20, 2013, http://www.rt.com/usa/congress-house-bill-cispa-031/ (Accessed on 31.07.2015)

of CISPA.[352] In such an environment, president Obama did not turn a deaf ear to opposition, and he signaled that the bill would not be approved as long as it undermined privacy of Americans.[353] The deadlock about CISPA demonstrated the importance of the support of the general audience in taking extraordinary measures at national level.

FISMA 2014 which was sponsored by Republican Representative Darrell E. Issa brought amendments to FISMA 2002 after it became Public Law with the approval of the Senate. This law underlined the authority of the Director of the Office of Management and Budget (OMB) with oversight and the Secretary of the DHS with implementation.[354] More importantly, there was 'rule of seven days' which required all federal agencies to share information on any security incidents.[355] This may be interpreted as an amendment to strengthen information sharing mechanism in order to ensure more collaborative federal action.

Similar to FISMA, the Cybersecurity Enhancement Act of 2013 and the Advancing America's Networking and Information Technology Research and Development Act of 2013 can be described as more technical legislative efforts that anticipated

---

[352] Andrew Couts, "CISPA Supporters List: 800+ Companies That Could Help Uncle Sam Snag Your Data" *Digital Trends*, 2012, http://www.digitaltrends.com/web/cispa-supporters-list-800-companies-that-could-help-uncle-sam-snag-your-data/.

[353] Adi Robertson, "Who Supports and Opposes CISPA, and Why?" *The Verge*, 2012, http://www.theverge.com/2012/5/2/2993495/cispa-hr-3523-business-support-opposition; Jason Koebler, "Obama Threatens to Veto CISPA, Citing Privacy Concerns" *US News*, 2013, http://www.usnews.com/news/articles/2013/04/16/obama-threatens-to-veto-cispa-citing-privacy-concerns.

[354] Public Law No: 113-283, https://www.congress.gov/bill/113th-congress/senate-bill/2521/.

[355] Public Law No: 113-283, https://www.congress.gov/bill/113th-congress/senate-bill/2521/.

advancement of research and development activities of federal agencies through collaboration, coordination and funding.[356]

The cyber week in the 113th Congress ended up with approval of FISMA and the Cybersecurity Enhancement Act on the one hand, and decline of CISPA and the Advancing America's Networking and Information Technology Research and Development Act by Senate. The approvals and declines of proposed laws brought the dilemma between national and individual security concerns. In other words, although there were ongoing efforts to enhance national cybersecurity strategy of the US through legislative actions, privacy concerns of individuals were the main determining factor for successful legislative efforts during the 113th Congress.

The Senate has been the authority that has hindered cybersecurity legislation. The proposed laws that passed the House of Representatives were caught in dilemma of national security vs privacy concerns in the Senate.[357] In 2015, Lewis in his Congressional Testimony made recommendations on the subject of how the US should secure cyberspace and what kind of strategies it should apply. Difficulty of deterrence, particularly unilateral version, in cyberspace was highlighted, although it could be seen as the primary strategy of the US since the Cold War. From this point of view, rather than deterring threats emanating from cyberspace unilaterally, enhancing cooperation by international agreements was proposed as a more rational strategy for the US and its

---

[356] House Committee on Science, Space, and Technology and Senate Committee on Commerce, Science, and Transportation, *Cybersecurity Enhancement Act of 2013*, 113th Cong., February 15, 2013; House Committee on Science, Space, and Technology and Senate Committee on Commerce, Science, and Transportation, *Advancing America's Networking and Information Technology Research and Development Act of 2013*, 113th Cong., March 5, 2013.

[357] Patricia Zengerle, "Senate Takes Up Cybersecurity Bill This Week," *Reuters*, August 4, 2015, http://www.reuters.com/article/us-usa-cybersecurity-congress-idUSKCN0Q91XT20150804.

allies that were also prone to cyber threats.[358] However, as cyberspace harbors variety of actors that are also able to conceal their identity, the origins of threats may diversify too. This may also prevent the development of international extraordinary measures.

As time passed with lack of enacted legislation, President Obama put more decisive efforts on cybersecurity legislation. It became more apparent with the promulgation of the Executive Order 13136. Especially in 2015, Obama got involved more in motivating cybersecurity legislation. He called the Congress to finalize the draft legislations which were generally stuck due to Senate's privacy concerns.[359]

Legislative policymaking process of the 114th Congress concentrated again on the similar bill to the House-led CISPA 2013 which was named as Cybersecurity Information Sharing Act of 2015. CISA was not unfamiliar to public since it was first introduced during the 113th Congress. The latest version of CISA 2015 has allowed private sector to share personal data of their consumers with federal agencies, as it was stated:

> Requires the Director of National Intelligence (DNI), the Department of Homeland Security (DHS), the Department of Defense (DOD), and the Department of Justice (DOJ) to develop and promulgate procedures to promote: (1) the timely sharing of classified and declassified cyber threat indicators in possession of the federal government with private entities, non-federal

---

[358] *U.S. International Strategy For Cybersecurity Testimony before the Senate Foreign Relations Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy, Senate,* 114th Cong., 5 (2015) (testimony of James A. Lewis) http://www.foreign.senate.gov/imo/media/doc/051415_REVISED_Lewis_Testimony.pdf

[359] Chris Strohm and Angela Greiling Keane, "President Urges Congress to Pass Bipartisan Cybersecurity Legislation," *Insurance Journal*, January 15, 2015, http://www.insurancejournal.com/news/national/2015/01/14/354020.htm;"Obama to Call for Congress to Pass New Cybersecurity Legislation," *Public Broadcasting Service*, January 13, 2015, http://www.pbs.org/newshour/rundown/obama-push-new-cybersecurity-legislation/;Tom Risen, "Obama Confronts Congress Deadlock on Cybersecurity," *The Us News*, January 13, 2015, http://www.usnews.com/news/articles/2015/01/13/obama-confronts-congress-deadlock-on-cybersecurity.

> government agencies, or state, tribal, or local governments; (2) the sharing of unclassified indicators with the public; and (3) the sharing of cybersecurity threats with entities to prevent or mitigate adverse effects.[360]

The part of the proposed law has been the center of the concerns of the US citizens. Almost the same objections have been voiced by the same organizations, as CISA and CISPA seem like they were cut from the same cloth based on the same data-sharing principles. This time Senator Ron Wyden, who, voted against CISA explained his opposition by arguing for privacy rights of citizens and limited impact of information-sharing legislation on cybersecurity.[361] Despite the opposition, this time, CISA passed the Senate and was signed into law by Obama by late 2015.[362] This was the primary achievement of the Obama Administration on cybersecurity legislation. Furthermore, by overcoming privacy concerns, it implied a ray of hope for further legislative efforts to take measures in legal arena.

Legislative branch of the US administration has dealt mainly with facilitating information-sharing mechanisms between public and private sectors, which was seen as the first step for more comprehensive cybersecurity legislation. It has been mainly advocated that information-sharing mechanism between public and private sectors would allow the US to defend cyberspace and to respond to similar cyber incidents. The point of enhancing an information-sharing mechanism was accepted by all federal

---

[360] Senate Committee on Intelligence, *Cybersecurity Information Sharing Act of 2015*, 114th Cong., March 17, 2015.

[361] "Wyden: Cybersecurity Bill Lacks Privacy Protections, Doesn't Secure Networks", March 12, 2015 http://www.wyden.senate.gov/news/press-releases/wyden-cybersecurity-bill-lacks-privacy-protections-doesnt-secure-networks.

[362] Everett Rosenfeld, "The Controversial 'Surveillance' Act Obama Just Signed," *CNBC*, December 22, 2015, http://www.cnbc.com/2015/12/22/the-controversial-surveillance-act-obama-just-signed.html.

agencies without criticism. However, the effects of the results of this overtly supported strategy have not been realized yet.

All in all, one may argue that the Congress has been the main branch which takes into account of the concerns of the public. This feature has restricted its ability in taking extraordinary measures for cyberspace. But, as mentioned in the Presidency section, insistence of Obama on cybersecurity legislations, which were in deadlock, through executive orders and personal statements may be interpreted as an important intervention on legislative branch. It demonstrates the determination of the top level federal agency, the Presidency, on taking necessary measures to secure cyberspace. Moreover, this also illustrates the difficulty of securitization of emerging and vague threats when the securitization move is not complemented and supported by the majority of the general audience as in the case of the Congressional drawbacks which have been caused by privacy concerns of the US citizens. To put it differently, it becomes harder to take extraordinary measures when the interest of the public, which is privacy concerns, is clashing with the national interests of the US. Therefore, the securitizing efforts of the Congress have been successful as much as it has overcome the privacy concerns.

5.4 Towards an International Cybersecurity Strategy?

During the Presidency of Obama, strategic use of cyber attacks and increased cyber capabilities of state and non-state actors have raised the awareness about the dangers from international sphere. Chinese attacks on the US networks, Stuxnet worm on Iran nuclear facilities which is also called Operation Olympic Games and Sony Pictures Case with North Korea were the main events of the Obama period that shaped the awareness and the threat perception at national and particularly in international levels. Cyber attacks of Chinese origin have been like an inseparable part of the US cybersecurity since it began in Clinton period and has continued since then increasingly on daily basis. On the other hand, offensive use of a cyber weapon –Stuxnet worm- and

Sony Pictures hacking have more unique characteristics that influence cybersecurity strategy.

In 2010, Stuxnet worm which was a jointly created cyber weapon by the US and Israel was discovered and officially confirmed by Obama in 2012.[363] Stuxnet was a cyber weapon that was used during peacetime when diplomatic efforts did not stop Iranian nuclear ambitions with the aim of postponement of Iranian nuclear enrichment program by damaging its infrastructure at Natanz facility.[364] This sophisticated worm seems like it fulfilled its aim as it damaged 1,000 centrifuges at Natanz.[365] Operation Olympic Games or infection by Stuxnet worm started in the last period of the Bush Administration, however its intrusion did not stop until it was discovered in the second year of President Obama.[366] It demonstrates how long a cyber weapon could effectively be used to exploit vulnerabilities in cyberspace. Moreover, its easy use during the peacetime without getting hindered by legal protection has revealed the importance of strategic use of cyberspace one more time. Stuxnet indicates that a cyber weapon can give damage in physical sphere; though cyber weapons are arguably less dangerous than traditional weapons they are highly effective in causing intended results either in physical sphere or cyber domain. Additionally, by use of Stuxnet, the US has

---

[363] John Leyden, "US Officials Confirm Stuxnet Was a Joint US-Israeli Op," *The Register*, June 1, 2012, http://www.theregister.co.uk/2012/06/01/stuxnet_joint_us_israeli_op/.

[364] Lindsay, "Stuxnet and the Limits of Cyber Warfare."

[365] David Albright, Paul Brannan, and Christina Walrond, *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment* (Institute for Science and International Security: Washington, DC, 2010), http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/.;William Yong and Robert F. Worth, "Bombings Hit Atomic Experts in Iran Streets," *New York Times*, November 29, 2010, http://www.nytimes.com/2010/11/30/world/middleeast/30tehran.html.

[366] Albright, Brannan, and Walrond, *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment*; Yong and Worth, "Bombings Hit Atomic Experts in Iran Streets."

showed its offensive capabilities in cyberspace. It can be seen as another critical point of this case.

Contrary to Operation Olympic Games, Sony Pictures demonstrates the US vulnerabilities in cyberspace one more time. Sony Pictures Entertainment which is an important corporation of the US in the film industry was hacked by a group of hackers in 2014.[367] It was just after the release of 'The Interview' which was about assassination of North Korean leader Kim Jong Un.[368] This made the US officials to think that the attacks were originated from North Korea although it was almost impossible to attribute it officially.[369] With the advantage of the attribution problem, North Koreans denied any responsibility of the attacks.[370] Three important features about this case were striking. Firstly, this hacking on a US corporation was the most costly one which was about $15 millions.[371] Secondly, it demonstrated that any power in cyberspace might be a potential critical opponent causing damage.[372] Lastly, although none of the nation-states was officially blamed by the US administration, Obama declared that the US will respond the attacks 'proportionally' and sanctions on

---

[367] Andrea Peterson, "The Sony Pictures Hack, Explained," *Washington Post*, December 18, 2014, https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/.

[368] Ibid.

[369] Ibid.

[370] Ibid.

[371] Ryan Faughnder, "Sony Says Studio Hack Cost It $15 Million in Fiscal Third Quarter," *Los Angeles Times*, April 2, 2015, http://www.latimes.com/entertainment/envelope/cotown/la-et-ct-sony-hack-cost-20150204-story.html.

[372] Steve Kroft, "The Attack on Sony," *CBS New*, April 12, 2015, http://www.cbsnews.com/news/north-korean-cyberattack-on-sony-60-minutes/.

North Korea will be expanded.[373] The sanctions were decided to be imposed on three of North Korean business and government agencies and ten government officials.[374]

North Korea as a state of 'axis of evil' has already been exposed to sanctions due to its nuclear program, but its malicious use of cyberspace required expansion of these measures. By February 2016, the Congress, in accordance with the preferences of Obama, has passed the bill that prescribed tightening sanctions on North Korea.[375] Imposing new measures against a threatening state is significant as it means putting the policies and strategies into practice rather than being a passive player in the cyberspace.

All these cases depict collaboration and regulation in international arena as vital for the US to sustain its superiority in this new domain. It was important for the US to lead its allies on the issue international cybersecurity. This would be possible through demonstrating the global effects of cyber threats which meant not only the US had vulnerabilities for cyberspace but also its allies might be exposed to these types of attacks brought by their technological advancements. In this line, similar to his predecessors, the first attempt of the Obama Administration was to make the US allies familiar with the cybersecurity in order to urge collective security. In addition to the

---

[373] Tim Walker and Lizzie Dearden, "President Obama Authorises New Sanctions Against North Korea After Sony Hack," *The Independent*, January 2, 2015, http://www.independent.co.uk/news/world/americas/sony-pictures-hack-president-obama-authorises-new-sanctions-against-north-korea-9954983.html; David A. Sanger, Michael S. Schmidt, and Nicole Perlroth, "Obama Vows a Response to Cyberattack on Sony," *New York Times*, December 20, 2014, http://www.nytimes.com/2014/12/20/world/fbi-accuses-north-korean-government-in-cyberattack-on-sony-pictures.html.

[374] Issie Lapowsky, "What We Know About the New U.S. Sanctions against North Korea in Response to Sony Hack," *Wired*, January 2, 2015, http://www.wired.com/2015/01/us-sanctions-north-korea-for-sony-hack/.

[375] Patricia Zengerle, "Congress Passes Tougher North Korea Sanctions, Sends Bill to Obama," *Reuters*, February 12, 2016, http://www.reuters.com/article/us-northkorea-usa-sanctions-idUSKCN0VL1WD; Kevin Liptak, "Obama Imposes New Sanctions on North Korea," *CNN*, February 18, 2016, http://edition.cnn.com/2016/02/18/politics/obama-north-korea-sanctions/.

many policy statements which underlined the international vulnerabilities vis-à-vis cyber attacks, the need for taking action was stated in 2011 in *the International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* which aimed to address the global challenges from cyberspace:

> When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners. We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests. In so doing, we will exhaust all options before military force whenever we can; will carefully weigh the costs and risks of action against the costs of inaction; and will act in a way that reflects our values and strengthens our legitimacy, seeking broad international support whenever possible.[376]

Relying on self-defense and collective security were the main methods which were emphasized in this document. By doing so, any offensive actions of the US might be legitimized by using self-defense and collective security arguments. These could be seen as the base of the opportunity-based strategies in cyberspace since characteristics of cyberspace offered grey zones without any legal commitments. Grey zones have been utilized by the strategic use of cyberspace.

Moreover, to show rising threats posed by cyberspace and to convince international audience, threats from potential adversaries were indicated by the Secretary of Defense as follows:

---

[376] Barack H. Obama, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC, 2011), p.14. https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

> Potential adversaries have invested significantly in cyber as it provides them with a viable, plausibly deniable capability to target the U.S. homeland and damage U.S. interests. Russia and China have developed advanced cyber capabilities and strategies. Russian actors are stealthy in their cyber tradecraft and their intentions are sometimes difficult to discern. China steals intellectual property (IP) from global businesses to benefit Chinese companies and undercut U.S. competitiveness. While Iran and North Korea have less developed cyber capabilities, they have displayed an overt level of hostile intent towards the United States and U.S. interests in cyberspace.[377]

Increased cyber capabilities of critical actors in cyberspace were the primary reason for the US to work on an international cybersecurity strategy with its allies. From the same document, it may be inferred that Obama wanted to improve bilateral and regional relations with emerging cyber powers. In order to deter these threats, building partnership initiatives specifically with Middle Eastern allies, Northeast Asian allies and allies from Asia-Pacific region in addition to the traditional allies –NATO- were defined as priorities for effective cybersecurity.[378] *North Korea Sanction and Policy Enhancement Act of 2016* which became law called for cooperation toward North Korea. Asian allies -the Republic of Korea, and Japan- were vital in this cooperation. Regarding the relationship with China, confidence-building measures as part of the US-China Defense Consultative Talks have been tried to be established.[379] The calls for developing bilateral and multilateral partnerships would be very important for a collective securitization move. However, the efforts generally have not been materialized so that it may be argued that the securitization move was not very clear at international level compared to national level. In order to understand this, bilateral

---

[377] Carter, "The Department of Defense Cyber Strategy."

[378] Ibid.

[379] Ibid.

relations with two major countries –Russia and China- and their effects on security strategy will be examined.

5.4.1 US-Russia: Strategic Game under the Roof of International Organizations

Russia was the first state which called international community to take actions for cyberspace under the UN by the late 1990s. Afterwards, in terms of international regulations, there were demands to strengthen cyber diplomacy among states as of 2009. The leading role in order to come up with international regulations has belonged to the US under the Obama Administration. This was the result of Obama's immediate declarations in several policy statements immediately after he took the office. For example, he already asserted the need for "a strategy for cybersecurity designed to shape the international environment and bring like-minded nations together[380]" in the *Cyberspace Policy Review* of 2009.

The US's attempt at improving international cybersecurity by strengthening UN resolution was explained by the underlining position of non-state actors as emerging threats in cyber domain.[381] This call was welcomed by the UN and also supported by Russia who was the initiator of the resolution in 1998.[382] The mutually accepted and supported attempt under the UN structure showed the willingness of two important global powers against new threats at least on paper. This may be interpreted as their aim of keeping prestigious status in cyber domain as a compliant actor despite their covert or unproven offensive use of cyberspace.

---

[380] Obama, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, p.iv.

[381] Gady and Austin, *Russia, The United States, and Cyber Diplomacy: Opening the Doors*, p.2.

[382] Ibid., p.2.

However, this does not mean that the US and the Russian Federation have a general consensus on securing cyberspace. This was understood when Russia and China came with the proposal of the International Code of Conduct for Information Security to the UN. The proposal was opposed by the US by claiming that the information security is different than cybersecurity, so that any initiative that restricts free flow of information is not acceptable for the US.[383]

Apart from the UN General Assembly resolutions, Russian attitude in cyberspace which was demonstrated by the Estonian and Georgian cases lead NATO to emphasize cybersecurity internationally. In this sense, in 2010 Lisbon Summit, NATO declared that it included cyber conflicts in NATO's doctrine and it would work for enhancing defensive capabilities of the NATO allies to promote cybersecurity.[384] In 2012 Chicago Summit, the emphasis on the cyber threats and cybersecurity became even more explicit. As stated below, the perception of common security which foresaw a collaborative approach with other organizations was tried to be established:

> We will develop further our ability to prevent, detect, defend against, and recover from cyber attacks. To address the cybersecurity threats and to improve our common security, we are committed to engage with relevant partner nations on a case-by-case basis and with international organisations, inter alia the EU, as agreed, the Council of Europe, the UN and the OSCE, in order to increase concrete cooperation.[385]

This idea was reinforced by the following 2014 Wales Summit:

---

[383] Timothy Farnsworth, "China and Russia Submit Cyber Proposal," *Arms Control Today*, November 2, 2011, https://www.armscontrol.org/act/2011_11/China_and_Russia_Submit_Cyber_Proposal.

[384] "Lisbon Summit Declaration," *North Atlantic Treaty Organization*, November 20, 2010, http://www.nato.int/cps/en/natolive/official_texts_68828.htm.

[385] "Chicago Summit Declaration," *North Atlantic Treaty Organization*, May 20, 2012, http://www.nato.int/cps/en/natohq/official_texts_87593.htm?selectedLocale=en.

> Our policy also recognises that international law, including international humanitarian law and the UN Charter, applies in cyberspace. Cyber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO's core task of collective defence. A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis.[386]

These statements were highly in parallel with the expectations of the Obama Administration which insisted upon international cooperation for cybersecurity on behalf of collective security of the US allies. Moreover, through these statements, it was emphasized that the growing vulnerabilities of both the US and its allies would be overcome by cooperation which could enhance defensive capabilities of all.

With respect to these developments, this study argues that the achievement of a global common ground with standardized law enforcement mechanism is almost impossible in cyber domain which implies grey zones especially for powerful states. In other words, states that have divergent national interests as in the case of Russia and the US cannot find the lowest common denominator to prevent exploitation of cyberspace with strategic purposes since they might have already benefited from this situation. Rather, it seems like this discrepancy has lead the US to have primary role in shaping cyber threat perception and in taking necessary actions for collective cybersecurity in its own alliance structure.

5.4.2 US-China: A Cyber Cold War?

The relationship between the US and China is different than the US-Russia relations since China can be seen as the main opponent in the cyberspace due to its everlasting

---

[386] "Wales Summit Declaration," *North Atlantic Treaty Organization*, September 5, 2014, http://www.nato.int/cps/en/natohq/official_texts_112964.htm.

cyber espionage and cyber attack attempts against the US public and private networks on daily basis.[387]

China, since Obama's election campaign, has been accused of cyber intrusions. In April 2009, the US accused China of disrupting its electricity grid.[388] According to the Wall Street Journal, Chinese hackers broke in the systems of the US Chamber of Commerce to steal data in 2011. Against accusation of the US side, Chinese used the attribution problem to de-escalate the issue. It was reported that a Chinese official said that "the allegation that the attack against the Chamber originated in China 'lacks proof and evidence and is irresponsible,' adding that the hacking issue should not be 'politicized'."[389] Therefore, the US was not able to launch a counter measure concerning Chinese attempts.

The malicious use of cyberspace by China has not stopped. But, they have continued denying every cyber incident that seemed to be originated from China. Additionally, Chinese also blamed the US by cyber espionage, too.[390] For traditional domains, these mutual actions might have lead to an escalation. However, in cyberspace, it has not brought a major conflict between the US and China. During the bilateral meeting of 2013, between President Obama and President Xi Jinping of the People's Republic of

---

[387] Paul Mozur, "Cybersecurity Firm Says Chinese Hackers Keep Attacking U.S. Companies," *New York Times*, October 19, 2015, http://www.nytimes.com/2015/10/20/technology/cybersecurity-firm-says-chinese-hackers-keep-attacking-us-companies.html; David A. Sanger, "U.S. Blames China's Military Directly for Cyberattacks," *New York Times*, May 6, 2013, http://www.nytimes.com/2013/05/07/world/asia/us-accuses-chinas-military-in-cyberattacks.html?_r=0.

[388] Siobhan Gorman, "Electricity Grid in U.S. Penetrated By Spies," *Wall Street Journal*, 2009, http://www.wsj.com/articles/SB123914805204099085.

[389] Siobhan Gorman, "China Hackers Hit U.S. Chamber," *Wall Street Journal*, December 21, 2011, http://www.wsj.com/articles/SB10001424052970204058404577110541568535300.

[390] Jacob Davidson, "China Accuses U.S. of Hypocrisy on Cyberattacks," *Time*, July 1, 2013, http://world.time.com/2013/07/01/china-accuses-u-s-of-hypocrisy-on-cyberattacks/.

China, emphasized their mutual concerns over cybersecurity which should be taken internationally not bilaterally.[391] While there have been many claims about Chinese economic theft by cyber intrusions on the US systems, no measures have been taken. Therefore, the Obama Administration has been criticized for its passive foreign policy against China.[392] However, the passive standing of the Obama Administration has not prevented further escalation since China has continued exploitation in cyberspace. This became clear when a group of cyber thieves from China who hacked computer systems for economic gain were legally accused of being responsible for cyber incidents in 2014 by the Department of Justice.[393] It was a critical action since it was released with the title "First Time Criminal Charges Are Filed Against Known State Actors for Hacking."[394] Consequently, China decided to interrupt bilateral meetings. After that, as of 2015, the US portrayed a more decisive position against Chinese hackers by preparing a sanction mechanism. It was not surprising that this attempt was not welcomed by Beijing. Moreover, some analysts from the US also believed that the

---

[391] Rancho Mirage, "Remarks by President Obama and President Xi Jinping of the People's Republic of China After Bilateral Meeting," *The White House*, 2013, https://www.whitehouse.gov/the-press-office/2013/06/08/remarks-president-obama-and-president-xi-jinping-peoples-republic-china-.

[392] Zeke J. Miller, "Obama Approaches Chinese Cybersecurity Issue With Carrot, Not Stick," *Time*, July 1, 2013, http://swampland.time.com/2013/06/08/obama-approaches-chinese-cyber-security-issue-with-carrot-not-stick/.

[393] Malcolm R. Lee, "Will the United States Impose Cyber Sanctions on China?," *Brookings*, September 22, 2015, http://www.brookings.edu/blogs/order-from-chaos/posts/2015/09/22-will-us-impose-cyber-sanctions-china-lee; "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage" Department of Justice, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

[394] Ibid.

sanctions would not deter China rather it would create a legal basis for China to impose counter-sanctions against the US firms as retaliation.[395]

Following the sanction crisis, it looked like the crisis was settled down by bilateral meeting in September 2015 since two states agreed on the issue of cyber theft:

> The United States and China agree that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.[396]

But, it was highly controversial whether this agreement would solve the problem of cyber theft. According to the Reuters, cyber intrusions have continued from the Chinese side even after the bilateral consensus.[397] In this regard, it can be said that dropping from more preventive measures like sanctions in order to pursue a diplomatic deal may not work in cyberspace.

In general, there was an ongoing deadlock to develop an international cybersecurity strategy in the Obama period too. For example, even by late 2015, it was again stated that there has been a consensus on 'peacetime norms of responsible state behavior in

---

[395] Ellen Nakashima, "U.S. Developing Sanctions Against China Over Cyberthefts," *Washington Post*, August 30, 2015, https://www.washingtonpost.com/world/national-security/administration-developing-sanctions-against-china-over-cyberespionage/2015/08/30/9b2910aa-480b-11e5-8ab4-c73967a143d3_story.html.

[396] "Fact Sheet: President Xi Jinping's State Visit to the United States," *The White House*, September 25, 2015, https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

[397] Joseph Menn, "China Tried To Hack U.S. Firms Even After Cyber Pact: Crowdstrike," *Reuters*, October 19, 2015, http://www.reuters.com/article/us-usa-china-cybersecurity-idUSKCN0SD0AT20151020.

cyberspace' which was negotiated at the 2015 G-20 Summit in Antalya, Turkey.[398] However, the summit did not define what kinds of norms were decided. Moreover, with respect to aim of the development of multilateral efforts, Cybersecurity Coordinator of the Obama Administration, Michael Daniel has declared "a new strategy to improve the US government's participation in the development and use of international standards for cybersecurity" as of 2016. It has been a bottom-up approach that includes non-governmental organizations, private sectors, as well as federal agencies. But, what the future has in store for this approach does not hold very optimistic outcomes since the bilateral side of the international cybersecurity has also been weak in developing extraordinary mechanisms. Furthermore, it may be argued that it is easier to take necessary actions against an isolated state -North Korea- than a state that has economic, diplomatic and political ties, as can be seen when North Korean case is compared to Chinese hacking issue. Therefore, despite all these statements, the US has not promoted an extraordinary measure regarding international codification of cyberspace neither in its bilateral relations nor under international organizations except North Korea.

All in all, neither bilateral relations nor multilateral initiatives have reached a final international cybersecurity strategy through a securitization move. This is caused by three interlinked reasons. Firstly, cyberspace includes wide range of actors who have varied threat perceptions and security strategies which are mostly not coincide with others. Secondly, cyberspace by its grey zones based on its characteristics offers a hidden battleground for states to use the domain strategically. Thirdly, development international law which is already difficult is more challenging in such a domain whose characteristics allow for instant changes.

---

[398] Lisa O. Monaco, "Administration Efforts on Cybersecurity: The Year in Review and Looking Forward to 2016" (Washington, DC: The White House, 2016), https://www.whitehouse.gov/blog/2016/02/02/administration-efforts-cybersecurity-year-review-and-looking-forward-2016.

5.5 Conclusion

It can be observed that the main securitizing actor during this term was the president himself, Barack Obama. Obama has clearly defined national interest of the US and thus national security as the main referent object to be protected in cyberspace. He has put national efforts to convince the audience to take emergency measures against increasing cyber threats. The efforts of Obama have been supplemented by the other federal agencies. All the bureaucratic agencies together with the Presidency have been decisive in defining cyberspace as a new battleground, and cybersecurity as one of the most important component of the national security of the US. The emphasis by bureaucratic agencies of increasing capabilities of both state and non-state actors has been crucial for more improved national security strategies. In parallel to this, the administration has worked for more inclusive legislative actions which are based on enhancing public-private partnership and information-sharing mechanism to take risk-based measures against cyber threats, although the bills and proposed laws have brought disagreement among the public. Therefore, cybersecurity has become an essential part of the US national security through the impressive speech acts of the securitizing actors, which have also been supported by some levels of extraordinary measures as it was examined in the U.S. Cyber Operations Policy.

At international securitization of cybersecurity, one cannot argue the same decisiveness, although there were three important cases with Iran, North Korea and China which could have produce a successful securitization move if they had happened in traditional domain. Sanctions which were expanded for North Korea have been the one and only extraordinary measure taken after these cases. However, this did not turn into a more comprehensive and international regulation. This shows that neither the US nor other actors favor an international cybersecurity strategy that could limit their actions. Moreover, the lack of clear securitization moves once more demonstrates the strategic importance of cyberspace since there have been no international legal

measures to prevent malicious use of cyberspace despite the clashing interests with Russia and China.

As conclusion, despite the limited efforts at international level, growing importance of cybersecurity has been in peak during the Obama Administration. This states that the pessimism over cyberspace at national level has also increased in Obama era due to the non-decremental vulnerabilities of the US and increasing capabilities of other states, while the skepticism at international level has been continuing due to the possible strategic use of cyberspace which have paved the way for opportunity-based strategies.

CHAPTER 6

CONCLUSION

Negligence of cyberspace means negligence of the digital revolution or the information revolution, while all the cultural, military, political and economic networks get more and more connected in this age. Cybersecurity ascends from the paradox of technology dependence which constitutes both advantages by new capabilities and disadvantages by new vulnerabilities. Because of that, issues related with the prefix *cyber*- have got the attention of academics, governments and the private sector. Rapid evolution of cyberspace and debates of cybersecurity have mainly showed itself in rhetoric. Then, there have been efforts to put strategies for cybersecurity at national level and international level. In other words, businessmen and statesmen have been dealing with the developing regulations and strategies to enhance protection. Recently, studies in IR also increasingly touch upon the strong link between technology revolution and information age, and their national and international effects. They can be seen as the result of articulation of technology revolution into national security. Therefore, cybersecurity is yet an important component of security studies due to new and different characteristics of cyberspace and it may be important to analyze the development of cybersecurity strategies in the context of emergence of new threats – cyber threat- with the end of the Cold War.

As it is mentioned throughout this study, literature mostly is based on the debates on severity of threats and cyber power, vulnerabilities of cyber attacks, and probability of cyberwar. There is also attribution problem in cyberspace which is a great barrier for detecting, and so then deterring the attacker. With respect to attribution problem, unless

you authenticate the aggressor, it does not seem very rational to pursue aggressive actions since you do not have an interlocutor. This makes offensive actions less valuable. But on the other hand, it could be argued that three main characteristics of cyberspace - temporality, permeation and fluidity- make defense harder because cyber attacks also have these features. Therefore, it should not be very surprising for states to have difficulty in deciding and implementing either offensive or defensive strategies in this domain.

Although cybersecurity consideration of the US mostly stems from the need to protect critical infrastructure, security understanding and strategies of an actor should not be thought apart from other actors in international system. This means the US perception of cybersecurity is highly connected with the rise of cyber strategies and capabilities of other nation-states such as China and Russia as well as non-state actors like terrorist organizations. Bringing non-state actors that are described as revisionists could diminish the traditional arguments about ambition of superpowers to preserve status-quo. In other words, security in cyberspace should not be represented in the context of securing critical infrastructures or it is not only related to the possibilities of cyberwar. It includes concerns for future of the issue by calculating capabilities and strategies of actors while Russia, Iran and China, the important triple of the regional powers, declare their intentions to increase capabilities in cyber domain. Therefore, underestimation of cyberspace does not only imply the blindness of cyber threats, but also imply ignorance of possibility of changes at power distribution at international system. In this line, cyberspace may be secured via increasing capabilities of the US in cyber domain. To put it differently, it is important for the US to keep its superpower status by sustaining its power in this extraterritorial domain. In brief, cybersecurity for the US mainly means protection of critical infrastructures which are vital for sustaining its operational capability both in physical and cyber domains; but it has also been caused by the

growing cyber capabilities of varied range of actors. These two clarify the X in the causal chain which is malicious activities of various actors in cyberspace.

In order to illustrate the Y which is outcome in this causal chain the securitization theory have been utilized in this study. Since the Clinton Administration, securitizing actors, mainly the bureaucratic agencies, sought to challenge security discourse at national level because it has been observed that cyberspace of the US have experienced many types of threats emanating from cyberspace such as DoS, cyber espionage and cyber crime due to wide range of vulnerabilities. The main securitizing actor of the Clinton Administration was the DoD. It was more active than the Presidency in defining vulnerabilities, referent objects and existential threats through effective use of the speech act. Clinton complemented the active role of the DoD by underlining the vulnerabilities of the US in cyberspace through the end of his administration. In the Bush Administration, there was an expansion of securitizing actors with the establishment of the DHS. However, the DoD continued to be the primary securitizing actor by treating cyberspace as a new battleground. The efforts of the DHS and the Presidency supported the attempts of the DoD as their speech acts were also important to convince the audience. Regarding these two eras, one could not speak of the effectiveness of the legislative branch, the Congress. The cybersecurity has been on top of the national security agenda especially during the Obama Administration as it has been examined in the reports and statements. In the Obama Administration, the main securitizing actor has been Obama, himself. The Presidency has been relatively more active in this era. Efforts of the Presidency have not only been limited by speech act but there have been also clear attempts to enhance extraordinary measures. The active role of the Presidency has played an important role in complementing the ongoing efforts of the Pentagon. Moreover, the Congress has also been more active securitizing actor in both defining existential threats and extraordinary measures through legislative acts. Therefore, in general, positions of the military personnel about the cyber threat, as the

critical official documents of the DoD illustrate, is more influential than other levels of statesmen since military domain is highly based on information infrastructure which should be kept secret and should be secured for its operational capability in both offense and defense. The Presidency, the DHS and the Congress also tried to demonstrate significance of the cybersecurity by showing the vulnerabilities of the US regarding the cyberspace and how cyberspace of the US is threatened by variety of actors. The actions of other federal agencies have been more successful when they have been supported by the top-level federal agency, the Presidency as in the case of the last administration.

All these express that at national level, there is a more successful securitization move which is based on cyber pessimism. This is explained by two factors in this study. One is related with the vulnerabilities of the US. It has been tried to be overcome by more risk-based strategies which include more defensive investments, re-designation of deterrence mechanism and enhancing information-sharing mechanism. Second factor is related to the effectiveness of the securitizing actor. The DoD, the DHS, the Presidency and finally the Congress are highly effective securitizing actors in this process. Through their speech acts, audience has become more aware of the dangers from the cyberspace. This allows the US to take risk-based emergency measures for cyberspace. Therefore, it may be argued that securitization move at national level has been steadily increasing through the efforts by the last three administrations even though we can still not talk about a successful securitization yet. The major obstacle to successful securitization at national level currently seems to be clashing interests of the public and administration which prevents developing more comprehensive extraordinary measures. The fact is also illustrative of the inherent dilemma of liberal theories of security studies. The more free and open public space may harbor security threats and challenges. Yet attempts to maintain security will be resisted by people as they may harm individual rights and liberties.

Securitization at international level differs from national level of securitization and is based on cyber skepticism. It may be claimed that although the emerging cyber threats have also been identified as an existential threat to prosperity of international community, there have been limits for the range of policies that could effectively manage international cybersecurity strategies. During presidencies of Clinton and Bush, cybersecurity strategy mainly relies on domestic actions, and there were no major international calls for cooperation or enforcement mechanism through international law. The call has become more obvious with Obama era by urging security for both the US and its allies. However, there has been still no final action which may complement the need. The lack of final action is explained by two reasons throughout the study. Firstly, at international level, the number of securitizing actors – states and non-states actors- is higher than domestic politics. Based on this, the audience that is needed to be convinced for an extraordinary measure is more diverse since threat perceptions of each actor do not always coincide with others' at cyber domain. To put it differently, although cyberspace brings new and similar vulnerabilities for each actor in the system, their opponents are not always the same. The second reason is the strategic use of cyberspace which offers grey zones for actors as a hidden battleground to complement their physical actions. Therefore, the securitization move at international level is generally limited to relatively inconsiderable speech acts of the US. Rather than working for development international law and regulations for cyberspace, the US also tries to utilize from the grey zones of the cyberspace by using cyberspace strategically as in the case of Stuxnet. Therefore, it could be argued that characteristics of cyberspace do not allow for a successful securitization at international level since the domain is more beneficial for the US as an important techno-power in the absence of extraordinary measures at international level.

In conclusion, it could be argued that the US neither wants to lose its prestigious superpower status by downgrading this new domain nor wants to get reaction by escalating tension in that ambiguous battlefield. High level of concerns at national politics which have generated risk-based strategies and non-escalatory policy choices at international politics which have produced opportunity-based strategies may be claimed being a result of this perspective. As a final word, for the terms of each president one may conclude that there has been a growing level of domestic securitization moves in the US whereas international securitization moves have been limited due to strategic interests of states.

REFERENCES

A Strategy For American Innovation: Driving Towards Sustainable Growth And Quality Jobs, 2009. https://www.whitehouse.gov/sites/default/files/microsites/ostp/innovation-whitepaper.pdf.

Albright, David, Paul Brannan, and Christina Walrond. *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment*. Washington, DC, 2010. http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/.

Aspin, Les. *Report on the Bottom-Up Review*, 1993.

Athique, Adrian. *Digital Media and Society: An Introduction*. Cambridge: Polity Press, 2013.

"Barack Obama's New Hampshire Primary Speech." *New York Times*, 2008. http://www.nytimes.com/2008/01/08/us/politics/08text-obama.html?_r=0.

"Belgrade's Cyber-Assault." *CBS New*, 1999. http://www.cbsnews.com/news/belgrades-cyber-assault/.

Blake Johnson, Nicole. "2014 Spending Bill Funds Continuous Monitoring Program." *Federal Times*, 2014. http://archive.federaltimes.com/article/20140114/CYBER/301140013/2014-spending-bill-funds-continuous-monitoring-program.

Brinkley, Douglas. "Democratic Enlargement: The Clinton Doctrine." *Foreign Policy*, no. 106 (1997): 111–27.

Bush, George W. *The National Strategy to Secure Cyberspace*. Washington, DC, 2003. https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

Buzan, Barry, Ole Weaver, and Jaap De Wilde, eds. *Security: A New Framework for Analysis*. London: Lynnie Rienner Publishers, 1998.

Carter, Ash. "The Department of Defense Cyber Strategy." Washington, DC: Department of Defense, 2015. http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

Cate, Fred H. "China and Information Security Threats: Policy Responses in the United States." In *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, edited by Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron. New York: Oxford University Press, 2015.

Choucri, Nazli. *Co-Evolution of Cyberspace and International Relations: New Challenges for the Social Sciences*, 2013.

Clarke, Richard. "War From Cyberspace." *National Interest*, no. November/December (2009): 31–37.

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

Clinton, William J. "A National Security Strategy for a New Century." *White House*, 1998.

———. "Address Before a Joint Session of the Congress on the State of the Union." *The American Presidency Project*, 1997. http://www.presidency.ucsb.edu/ws/?pid=53358.

———. "Defending America's Cyberspace: National Plan for Information Systems Protection An Invitation to a Dialogue." Washington: Government Printing Office, 2000. https://fas.org/irp/offdocs/pdd/CIP-plan.pdf.

———. *Executive Order 13010 Critical Infrastructure Protection*. Washington, DC, 1996.

———. "Presidential Decision Directive 29: Security Policy Coordination." Washington, DC: Government Printing Office, 1994.

———. *Presidential Decision Directive 63: Critical Infrastructure Protection*. *The White House*. Washington, DC, 1998. http://fas.org/irp/offdocs/pdd/pdd-63.htm.

———. *Statement of Administration Policy: H.R. 4576 - Department of Defense Appropriations Bill, FY 2001*. *White House*. Washington, 2000. http://www.presidency.ucsb.edu/ws/index.php?pid=74826&st=cyber&st1=.

Commission on Cybersecurity for the 44th Presidency. *Securing Cyberspace for the 44th Presidency*. Washington, DC, 2008. http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

Cornish, Paul. *The Vulnerabilities of Developed States to Economic Cyber Warfare*. London, 2011. https://www.chathamhouse.org/sites/files/chathamhouse/0611wp_cornish.pdf.

Critical Foundations: Protecting America's Infrastructures. Washington, DC: U.S. Government Printing Office, 1997. https://fas.org/sgp/library/pccip.pdf.

Davidson, Jacob. "China Accuses U.S. of Hypocrisy on Cyberattacks." *Time*, 2013. http://world.time.com/2013/07/01/china-accuses-u-s-of-hypocrisy-on-cyberattacks/.

Davis, Richard. *The Web of Politics: The Internet's Impact on the American Political System*. New York: Oxford University Press, 1999.

Defense Science Board. *Report of the Defense Science Board on Information Warfare*. Washington, DC, 1996.

———. *Report of the Defense Science Board Summer Study Task Force on Information Architecture for the Battlefield*. Washington, DC, 1994.

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, 239–88. Santa Monica: RAND, 2001.

Doyle, Charles. *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*. Washington, DC, 2014. https://www.fas.org/sgp/crs/misc/97-1025.pdf.

Dunn Cavelty, Myriam. *Cyber-Security and Threat Politics: US Efforts to Secure Information Age*. New York: Routledge, 2008.

———. "Is Anything Ever New?- Exploring the Specifities of Security and Governance in the Information Age." In *Power and Security in the Information Age : Investigating the Role of the State in Cyberspace*, edited by Myriam Dunn Cavelty, Victor Mauer, and Sai Felicia Krishna-Hensel. Hampshire: Ashgate, 2007.

Dunn Cavelty, Myriam, and Elgin M. Brunner. "Introduction: Information, Power and Security- An Outline of Debates and Implications." In *Power and Security in the Information Age : Investigating the Role of the State in Cyberspace*, edited by Myriam Dunn Cavelty, Victor Mauer, and Sai Felicia Krishna-Hensel. Hampshire: Ashgate, 2007.

Dunn, Myriam A. "Securing the Digital Age: The Challenges of Complexity for Critical Infrastructure Protection and IR Theory." In *International Relations and Security in the Digital Age*, edited by Johan Eriksson and Giampiero Giacomello. Oxon: Routledge, 2007.

Dutton, William. *Society on the Line: Information Politics in the Digital Age:* Oxford University Press, 1999.

Dyson, Esther. "Cyberspace and the American Dream: A Magna Carta for the Knowledge Age." *The Information Society* 12, no. 3 (August 29, 1994): 295–308.

Ellen Joan Pollock, and Andrea Petersen. "Unsolicited E-Mail Hits Targets In America in First Cyberwar." *Wall Street Journal*, 1999. http://www.wsj.com/articles/SB923519887609541882.

Erwin, Sandra I. "Cybersecurity Legislation: Solution or Distraction?" *National Defense*, 2012. https://www.hollingsworthllp.com/uploads/23/doc/media.819.pdf.

"Fact Sheet: Cybersecurity National Action Plan." *The White House*, 2016. https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

"Fact Sheet: President Xi Jinping's State Visit to the United States." *The White House*, 2015. https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

Farnsworth, Timothy. "China and Russia Submit Cyber Proposal." *Arms Control Today*, 2011. https://www.armscontrol.org/act/2011_11/China_and_Russia_Submit_Cyber_Proposal.

Farwell, James P., and Rafal Rohozinski. "The New Reality of Cyber War." *Survival* 54, no. 4 (September 2012): 107–20.

Faughnder, Ryan. "Sony Says Studio Hack Cost It $15 Million in Fiscal Third Quarter." *Los Angeles Times*, 2015. http://www.latimes.com/entertainment/envelope/cotown/la-et-ct-sony-hack-cost-20150204-story.html.

"FBI Warns of Fake Govt Sites, ISIS Defacements." *Krebs on Security*. Accessed June 29, 2015. http://krebsonsecurity.com/2015/04/fbi-warns-of-fake-govt-sites-isis-defacements/.

Fischer, Eric A. *Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions*, 2013. https://www.fas.org/sgp/crs/natsec/R42114.pdf.

Friedman, Thomas L. "Clinton and Foreign Policy/A Special Report.; Clinton's Foreign-Policy Agenda Reaches Across Broad Spectrum." *New York Times*, 1992. http://www.nytimes.com/1992/10/04/us/1992-campaign-issues-foreign-policy-looking-abroad-clinton-foreign-policy.html?pagewanted=all.

Gady, Franz-Stefan, and Greg Austin. *Russia, The United States, and Cyber Diplomacy: Opening the Doors*. New York, 2010. http://www2.ewi.info/sites/default/files/ideas-files/USRussiaCyber_WEB.pdf.

Gartzke, Erik. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security* 38, no. 2 (2013): 41–73.

Gelpi, Christopher, and Peter D. Feaver. "Speak Softly and Carry a Big Stick? Veterans in the Political Elite and the American Use of Force." *American Political Science Review* 96, no. 4 (2002): 779–93.

Glaser, Charles L., and Chairn Kaufmann. "What Is the Offense-Defense Balance and How Can We Measure It?" *International Security* 22, no. 4 (1998): 44–82.

Glendinning, Lee. "Obama, McCain Computers 'Hacked' During Election Campaign." *The Guardian*, 2008. http://www.theguardian.com/global/2008/nov/07/obama-white-house-usa.

Gorman, Siobhan. "China Hackers Hit U.S. Chamber." *Wall Street Journal*, 2011. http://www.wsj.com/articles/SB10001424052970204058404577110541568535300.

———. "Electricity Grid in U.S. Penetrated By Spies." *Wall Street Journal*, 2009. http://www.wsj.com/articles/SB123914805204099085.

Graham, Bradley. "Military Grappling With Rules For Cyber Warfare." *The Washington Post*, 1999. http://www.washingtonpost.com/wp-srv/WPcap/1999-11/08/011r-110899-idx.html.

Greenwald, Glenn, and Ewen MacAskill. "Obama Orders US to Draw Up Overseas Target List for Cyber-Attacks." *The Guardian*, 2013. http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas.

Halperin, Morton H., Priscilla A. Clapp, and Arnold Kanter. *Bureaucratic Politics and Foreign Policy*. Washington, DC: The Brookings Institution, 2006.

Hastedt, Glenn P. *American Foreign Policy*. Upper Saddle River, N.J. : Pearson/Prentice Hall, 2011.

ITU National Cybersecurity Strategy Guide. *International Telecommunication Uinon*. Geneva, 2011. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf.

Jack, Holland. "Why Is Change so Hard? Understanding *Continuity* in Barack Obama's Foreign Policy." In *Obama's Foreign Policy: Ending the War on Terror*, edited by Michelle Bentley and Holland Jack. New York: Routledge, 2014.

Johnson, Jeh Charles. "Quadrennial Homeland Security Review." Washington, DC: Department of Homeland Security, 2014. https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf.

Joint Chief of Staff. *The National Military Strategy for Cyber Operations*. Washington, DC, 2006. http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf.

Joint Security Commission. "Redefining Security: A Report to the Secretary of Defense and the Director of Central Intelligence." Washington, DC: US Government Printing Office, 1994.

Jones, Thomas. "William Gibson: Beyond Cyberspace." *The Guardian*, 2011. http://www.theguardian.com/books/2011/sep/22/william-gibson-beyond-cyberspace.

Julian Borger. "Pentagon Kept the Lid on Cyberwar in Kosovo." *The Guardian*, 1999. http://www.theguardian.com/world/1999/nov/09/balkans.

Kello, Lucas. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." *International Security* 38, no. 2 (2013): 7–40.

Klimburg, Alexander, ed. *National Cyber Security Framework Manual*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. Accessed November 13, 2015. https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf.

Kramer, Franklin D., and Larry K. Wentz. "Cyber Influence and International Security." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. Virginia: Potomac Books, Inc., 2009.

Kroft, Steve. "The Attack on Sony." *CBS New*, 2015. http://www.cbsnews.com/news/north-korean-cyberattack-on-sony-60-minutes/.

Lachow, Irving. *Active Cyber Defense A Framework for Policymakers*. Washington, DC, 2013. http://www.cnas.org/files/documents/publications/CNAS_ActiveCyberDefense_Lachow_0.pdf.

Lallana, Emmanuel C., and Margaret N. Uy. *The Information Age*. UNDP Asia-Pacific Development Information Programme, 2003. http://www.unapcict.org/ecohub/resources/the-information-age.

Lapowsky, Issie. "What We Know About the New U.S. Sanctions against North Korea in Response to Sony Hack." *Wired*, 2015. http://www.wired.com/2015/01/us-sanctions-north-korea-for-sony-hack/.

Lawson, Sean. "DOD's 'First' Cyber Strategy Is Neither First, Nor a Strategy - Forbes." *Forbes*, 2011. http://www.forbes.com/sites/seanlawson/2011/08/01/dods-first-cyber-strategy-is-neither-first-nor-a-strategy/#6d18112a33a8.

Lee, Malcolm R. "Will the United States Impose Cyber Sanctions on China?" *Brookings*, 2015. http://www.brookings.edu/blogs/order-from-chaos/posts/2015/09/22-will-us-impose-cyber-sanctions-china-lee.

Leyden, John. "US Officials Confirm Stuxnet Was a Joint US-Israeli Op." *The Register*, 2012. http://www.theregister.co.uk/2012/06/01/stuxnet_joint_us_israeli_op/.

Liff, Adam P. "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War." *Journal of Strategic Studies* 35, no. 3 (June 29, 2012): 401–28.

Lin, Herbert. "Joining Cybercrime and Cyberterrorism: A Likely Scenario." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, edited by Derek S. Reveron, 57–68. Washington: Georgetown University Press, 2012.

Lindsay, Jon R. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* 22, no. 3 (July 2013): 365–404.

Liptak, Kevin. "Obama Imposes New Sanctions on North Korea." *CNN*, 2016. http://edition.cnn.com/2016/02/18/politics/obama-north-korea-sanctions/.

Locatelli, Andrea. *The Offense/ Defense Balance in Cyberspace*. Milano, 2013. http://www.ispionline.it/sites/default/files/pubblicazioni/analysis_203_2013.pdf.

Lord, Kristin M., and Travis Sharp. *America's Cyber Future: Security and Prosperity in the Information Age*. Washington, DC, 2011.

Margolis, Michael, and David K. Resnick. *Politics as Usual: The Cyberspace `Revolution'*. London: SAGE Publications Inc., 2000.

Markoff, John. "Clinton Proposes Initiatives On the Scrambling of Data." *New York Times*, 1996. http://www.nytimes.com/1996/07/13/business/clinton-proposes-initiatives-on-the-scrambling-of-data.html.

Massari, Maurizio. "US Foreign Policy Decision-Making during the Clinton Administration." *The International Spectator* 35, no. 4 (2000). http://www.tandfonline.com/doi/pdf/10.1080/03932720008458155.

Maurer, Tim. *Cyber Norm Emergence at the United Nations - An Analysis of the Activities at the UN Regarding Cyber-Security*. Cambridge, 2011. http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf.

McCain, John. "Imagery or Purpose? The Choice in November." *Foreign Policy*, no. 103 (1996): 20–34.

McCormik, James. *American Foreign Policy and Process*. 6th ed. Wadsworth Cengage Learning, 2014.

Mehilli, Elidor. "Technology and the Cold War." In *Coordinating Committee for Multilateral Export Controls*, edited by Artemy M. Kalinovsky and Craig Daigle, 292–304. New York: Routledge, 2014.

"Memorandum For The Vice President, The Secretary Of State, The Secretary Of The Treasury, The Secretary Of Defense,The Attorney General." *White House*, 1996. http://fas.org/irp/offdocs/eo_crypt_9611_memo.htm.

Menn, Joseph. "China Tried To Hack U.S. Firms Even After Cyber Pact: Crowdstrike." *Reuters*, 2015. http://www.reuters.com/article/us-usa-china-cybersecurity-idUSKCN0SD0AT20151020.

Miller, Judith, and William J. Broad. "Exercise Finds U.S. Unable To Handle Germ War Threat." *New York Times*, 1998.

http://www.nytimes.com/1998/04/26/world/exercise-finds-us-unable-to-handle-germ-war-threat.html?pagewanted=1.

Miller, Zeke J. "Obama Approaches Chinese Cybersecurity Issue With Carrot, Not Stick." *Time*, 2013. http://swampland.time.com/2013/06/08/obama-approaches-chinese-cyber-security-issue-with-carrot-not-stick/.

Mirage, Rancho. "Remarks by President Obama and President Xi Jinping of the People's Republic of China After Bilateral Meeting." *The White House*, 2013. https://www.whitehouse.gov/the-press-office/2013/06/08/remarks-president-obama-and-president-xi-jinping-peoples-republic-china-.

Monaco, Lisa O. "Administration Efforts on Cybersecurity: The Year in Review and Looking Forward to 2016." Washington, DC: The White House, 2016. https://www.whitehouse.gov/blog/2016/02/02/administration-efforts-cybersecurity-year-review-and-looking-forward-2016.

Morag, Nadav. *Cybercrime, Cyberespionage, and Cybersabotage: Understanding Emerging Threats*. Colorado, 2014. http://www.coloradotech.edu/~/media/CTU/Files/ThoughtLeadership/cybercrime-white-paper.ashx.

Mozur, Paul. "Cybersecurity Firm Says Chinese Hackers Keep Attacking U.S. Companies." *New York Times*, 2015. http://www.nytimes.com/2015/10/20/technology/cybersecurity-firm-says-chinese-hackers-keep-attacking-us-companies.html.

Nakashima, Ellen. "Obama Signs Secret Directive to Help Thwart Cyberattacks." *The Washington Post*, 2012. https://www.washingtonpost.com/world/national-security/obama-signs-secret-cybersecurity-directive-allowing-more-aggressive-military-role/2012/11/14/7bf51512-2cde-11e2-9ac2-1c61452669c3_story.html.

———. "U.S. Developing Sanctions Against China Over Cyberthefts." *Washington Post*, 2015. https://www.washingtonpost.com/world/national-security/administration-developing-sanctions-against-china-over-cyberespionage/2015/08/30/9b2910aa-480b-11e5-8ab4-c73967a143d3_story.html.

———. “White House Declassifies Outline of Cybersecurity Program.” *The Washington Post*, 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/03/02/AR2010030202113.html.

Napolitano, Janet. “Blueprint for A Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise.” Washington, DC: Department of Homeland Security, 2011. https://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf.

———. “The Quadrennial Homeland Security Review Report (QHSR): A Strategic Framework for a Secure Homeland.” Washington, DC: Department of Homeland Security, 2010. https://www.dhs.gov/xlibrary/assets/qhsr_report.pdf.

Nye, Joseph. “Cyber Power.” Cambridge, 2010. http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.

Obama, Barack H. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. Washington, DC, 2009. https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

———. *Executive Order 13636: Improving Critical Infrastructure Cybersecurity*. Washington, DC, 2013. https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

———. *Executive Order: Commission on Enhancing National Cybersecurity*. *The White House*. Washington, DC, 2016. https://www.whitehouse.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity.

———. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. Washington, DC, 2011. https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

———. *National Security Strategy*. Washington, DC, 2010. http://nssarchive.us/NSSR/2010.pdf.

———. *Presidential Policy Directive (PPD-20): U.S. Cyber Operations Policy*. Washington, DC, 2012. http://fas.org/irp/offdocs/ppd/ppd-20.pdf.

———. *Presidential Policy Directive (PPD-21): Critical Infrastructure Security and Resilience*. Washington, DC, 2012. http://fas.org/irp/offdocs/ppd/ppd-21.pdf.

———. *Presidential Proclamation: National Cybersecurity Awareness Month*. Washington, DC, 2010. https://www.whitehouse.gov/the-press-office/2010/10/01/presidential-proclamation-national-cybersecurity-awareness-month.

———. "Remarks by the President to the United Nations General Assembly." New York: Office of the Press Secretary, 2009. https://www.whitehouse.gov/the-press-office/remarks-president-united-nations-general-assembly.

———. *Statement by the President on Executive Order "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities."* Washington, DC, 2015. https://www.whitehouse.gov/the-press-office/2015/04/01/statement-president-executive-order-blocking-property-certain-persons-en.

"Obama Speech: 'Yes, We Can Change.'" *CNN*, 2008. http://edition.cnn.com/2008/POLITICS/01/26/obama.transcript/index.html?eref=rss_latest.

"Obama to Call for Congress to Pass New Cybersecurity Legislation." *Public Broadcasting Service*, 2015. http://www.pbs.org/newshour/rundown/obama-push-new-cybersecurity-legislation/.

"Obama, McCain Campaigns' Computers Hacked for Policy Data." *CNN*, 2008. http://edition.cnn.com/2008/TECH/11/06/campaign.computers.hacked/.

Office of Science and Technology Policy National Security and International Affairs Division. *Cybernation: The American Infrastructure in the Information Age*. Washington, DC, 1998. http://fas.org/irp/threat/980107-cyber2.html.

Office, United States General Accounting. "Computer Security: Hackers Penetrate DOD Computer Systems." 1991.

"Pentagon 'at War' with Computer Hackers." *CNN*, 1999. http://edition.cnn.com/TECH/computing/9903/05/pentagon.hackers/index.html.

"Pentagon Kept the Lid on Cyberwar in Kosovo." *The Guardian*, 1999. http://www.theguardian.com/world/1999/nov/09/balkans.

Peterson, Andrea. "The Sony Pictures Hack, Explained." *Washington Post*, 2014. https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/.

"President Bill Clinton Speaks To The Naval Academy At Annapolis." *CNN*, 1998. http://edition.cnn.com/ALLPOLITICS/1998/05/22/clinton.academy/transcript.html.

Public Safety Canada. *Role of Critical Infrastructure in National Prosperity*, 2015. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-rl-crtclnfrstrctr-ntnlprsprty/2016-rl-crtclnfrstrctr-ntnlprsprty-en.pdf.

Rattray, Gregory. "An Environmental Approach to Understanding Cyberpower." In *Cyberpower and National Security*, edited by Franklin D. Kramer and Stuart H. Starr. Virginia: Potomac Books, Inc., 2009.

Reveron, Derek S. "An Introduction to National Security and Cyberspace." In *Cyberspace and National Security: Threats Opportunities and Power in a Virtual World*, edited by Derek S. Reveron. Washington, DC: Georgetown University Press, 2012.

Rid, Thomas. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35, no. 1 (February 2012): 5–32.

———. "Cyberwar and Peace." *Foreign Affairs*, 2013. https://www.foreignaffairs.org/articles/2013-10-15/cyberwar-and-peace.

Risen, Tom. "Obama Confronts Congress Deadlock on Cybersecurity." *The Us News*, 2015. http://www.usnews.com/news/articles/2015/01/13/obama-confronts-congress-deadlock-on-cybersecurity.

Róbert Ondrejcsák. *American Foreign and Security Policy under Barack Obama: Change and Continuity*. Bratislava, 2009. http://cenaa.org/analysis/american-foreign-and-security-policy-under-barack-obama-change-and-continuity/.

Rosenfeld, Everett. "The Controversial 'Surveillance' Act Obama Just Signed." *CNBC*, 2015. http://www.cnbc.com/2015/12/22/the-controversial-surveillance-act-obama-just-signed.html.

Rothkopf, David J. "Cyberpolitik: The Changing Nature of Power in the Information Age." *Journal of International Affairs* 51, no. 2 (1998): 325–59.

Sanger, David A. "U.S. Blames China's Military Directly for Cyberattacks." *New York Times*, 2013. http://www.nytimes.com/2013/05/07/world/asia/us-accuses-chinas-military-in-cyberattacks.html?_r=0.

Sanger, David A., and John Markoff. "Obama Outlines Coordinated Cyber-Security Plan." *The New York Times*, 2009. http://www.nytimes.com/2009/05/30/us/politics/30cyber.html?_r=0.

Sanger, David A., Michael S. Schmidt, and Nicole Perlroth. "Obama Vows a Response to Cyberattack on Sony." *New York Times*, 2014. http://www.nytimes.com/2014/12/20/world/fbi-accuses-north-korean-government-in-cyberattack-on-sony-pictures.html.

"Secretary Panetta's Speech About Cybersecurity." *Council on Foreign Relations*, 2012. http://www.cfr.org/cybersecurity/secretary-panettas-speech-cybersecurity/p29262.

Seltzer, Larry. "The Morris Worm: Internet Malware Turns 25." *ZDNet*, 2013. http://www.zdnet.com/article/the-morris-worm-internet-malware-turns-25/.

"Serb Supporters Sock It to NATO, U.S. Web Sites." *CNN*, 1999. http://edition.cnn.com/TECH/computing/9904/06/serbnato.idg/index.html.

Smith, Gerry. "Obama Drafts Cybersecurity Executive Order." *The Huffington Post*, 2012. http://www.huffingtonpost.com/2012/09/11/cybersecurity-executive-order-obama_n_1874250.html.

Søndergaard, Rasmus Sinding. “Bill Clinton’s ‘Democratic Enlargement’ and the Securitisation of Democracy Promotion.” *Diplomacy & Statecraft* 26, no. 3 (September 2015): 534–51.

Sorenson, Theodore C. “America’s Firt Post-Cold War President.” *Foreign Affairs* 71, no. 4 (1992): 13–30.

Stevens, Gina, Legislative Attorney, and Jonathan Miller. *The Obama Administration’s Cybersecurity Proposal: Criminal Provisions*. Washington, DC, 2011. https://www.fas.org/sgp/crs/misc/R41941.pdf.

Strohm, Chris, and Angela Greiling Keane. “President Urges Congress to Pass Bipartisan Cybersecurity Legislation.” *Insurance Journal*, 2015. http://www.insurancejournal.com/news/national/2015/01/14/354020.htm.

Tehan, Rita. *Cybersecurity: Legislation, Hearings, and Executive Branch Documents*, 2015.

“The Department of Defense Strategy for Operating in Cyberspace.” Washington, DC: Department of Defense, 2011. http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

Torres Soriano, Manuel R. “Internet as a Driver of Political Change: Cyber-Pessimists and Cyber-Optimists.” *Revista Del Instituto Español de Estudios Estratégicos* 1 (2013): 332–52.

“Transcript: ‘This Is Your Victory,’ Says Obama.” *CNN*, 2008. http://edition.cnn.com/2008/POLITICS/11/04/obama.transcript/.

U.S. Senate. “National Security and Information Age.” Washington, DC: Government Publishing Office, 1996. https://www.congress.gov/congressional-record/1996/9/28/senate-section/article/s11758-1?q=%7B%22search%22%3A%5B%22information+security%22%5D%7D&resultIndex=23.

———. “National Security and Information Technology.” Washington, DC: Government Publishing Office, 1998. https://www.congress.gov/congressional-

record/1998/10/12/senate-section/article/s12359-1?q=%7B%22search%22%3A%5B%22information+security%22%5D%7D&resultIndex=11.

U.S. Senate Permanent Subcommittee on Investigations of the Committee on Governmental Affairs. "Security in Cyberspace." 1996.

United States Code. Washington: Government Printing Office, 2008.

United States General Accounting Office. "Information Security:Computer Attacks at Department of Defense Pose Increasing Risks." 1996.

"Use Cryptography Correctly." *The Institute of Electrical and Electronics Engineers*. Accessed May 10, 2016. http://cybersecurity.ieee.org/blog/2015/11/13/use-cryptography-correctly/.

Veneris, Yannis. "Modelling the Transition from the Industrial to the Informational Revolution." *Environment and Planning A* 22, no. 3 (March 1990): 399–416.

Walker, Tim, and Lizzie Dearden. "President Obama Authorises New Sanctions Against North Korea After Sony Hack." *The Independent*, 2015. http://www.independent.co.uk/news/world/americas/sony-pictures-hack-president-obama-authorises-new-sanctions-against-north-korea-9954983.html.

Walt, Stephen M. "Two Cheers for Clinton's Foreign Policy." *Foreign Affairs* 79, no. 2 (March 2000): 63–79.

Weaver, Ole. "Aberystwyth, Paris, Copenhagen: New Schools in Security Theory and the Origins between Core and Periphery." Montreal: ISA Conference, 2004.

———. "Securitization and Desecuritization." In *On Security*, edited by Ronnie D. Lipschutz. New York: Columbia University Press, 1995.

Weiner, Tim. "Clinton as a Military Leader - Tough On-the-Job Training." *New York Times*, 1996. http://www.nytimes.com/1996/10/28/us/clinton-as-a-military-leader-tough-on-the-job-training.html?pagewanted=all.

Whittaker, Zack. "Obama's Cybersecurity Executive Order: What You Need to Know." *ZDNet*, 2013. http://www.zdnet.com/article/obamas-cybersecurity-executive-order-what-you-need-to-know/.

Wolfers, Arnold. *Discord and Collaboraiton: Essays on International Politics*. Baltimore: The Johns Hopkins University Press, 1965.

Wong, Thiong Pern. "Active Cyber Defense: Enhancing National Cyber Defense." Naval Postgraduate School, 2011. http://calhoun.nps.edu/bitstream/handle/10945/10713/11Dec%255FWong%255FT.pdf?sequence=1.

Yong, William, and Robert F. Worth. "Bombings Hit Atomic Experts in Iran Streets." *New York Times*, 2010. http://www.nytimes.com/2010/11/30/world/middleeast/30tehran.html.

Zengerle, Patricia. "Congress Passes Tougher North Korea Sanctions, Sends Bill to Obama." *Reuters*, 2016. http://www.reuters.com/article/us-northkorea-usa-sanctions-idUSKCN0VL1WD.

———. "Senate Takes Up Cybersecurity Bill This Week." *Reuters*, 2015. http://www.reuters.com/article/us-usa-cybersecurity-congress-idUSKCN0Q91XT20150804.

APPENDICES

APPENDIX A: TURKISH SUMMARY

AMERİKA BİRLEŞİK DEVLETLERİ'NİN ULUSAL VE ULUSLARARASI SİBER GÜVENLİK STRATEJİLERİ: GÜVENLİKLEŞTİRME HAREKETİ?

Uluslararası İlişkiler disiplininin önemli alanlarından biri olan Güvenlik Çalışmaları'na ait konular Soğuk Savaş'ın sona ermesiyle birlikte giderek çeşitlenmiştir. Soğuk Savaş'ın bitmesi ve Sovyetler Birliği'nin dağılması bir yandan iki kutuplu sistemin sona ermesi demekken diğer yandan nükleer tehdidin azalmasıyla birlikte askeri olmayan tehditlerin önem kazanması anlamına gelmektedir. Örneğin, çevresel sorunlar, insani meseleler ve ekonomik problemlere verilen önem bu dönem itibariyle artış göstermiştir. Diğer bir deyişle, Soğuk Savaş'ın sona ermesi, güvenlik çalışmalarında devlet ve askeri tehdit odaklı güvenlik anlayışının değişmesi ve yeni aktörlerin, tehditlerin ve hassas noktaların eklenmesiyle yeni bir dönem başlatmıştır.

Bilgi çağının başlaması, değişen ve genişleyen güvenlik çalışmalarında önemli bir dönüm noktasını temsil etmektedir. Bu bağlamda, özellikle 1990'lardan başlayarak ve 2000'lerin ortasına doğru giderek artan bir şekilde bilginin ve bilgi teknolojilerinin güvenliğini sağlamak önemli ve bir o kadar da tartışmalı bir mesele olmuştur. Böyle bir ortamda, pek çokları tarafından aktörlerin güvenlik politikalarına ve stratejilerine önemli etkileri olduğu ve olacağı öne sürülen bir çalışma alanı olarak siber alanın etkilerinin çalışılması oldukça önemlidir. Siber tehditlerin ortaya çıkmasıyla birlikte yeni zayıf noktaların neden olduğu iddia edilen bu etkilerin temel nedenleri olarak siber alanın sahip olduğu benzersiz karakteristik özellikleri ve siber tehditlerin daha önceden

tanımlanmamış ve tanımlanamayan yapısı görülmektedir. Siber alanın uluslararası politikanın parçası olan aktörlerin politikaları ve stratejileri üzerindeki etkilerinin çalışılması aynı zamanda siber güç diye adlandırılmakta olan bilgi odaklı bir güç belirleyicisinin ortaya çıkması ve bunun incelenmesi açısından da önemlidir. Öte yandan, siber alan pek çok uluslararası aktör ve siyasi isim tarafından güvenlik çalışmalarının bir parçası olarak görülürken bu alanın incelenmesi uluslararası politika açısından da önem kazanmıştır.

Bu tezde, Amerika Birleşik devlerinin Clinton, Bush ve Obama yönetimleri altında belirlediği ve belirlemeye çalıştığı siber güvenlik stratejilerinin incelenmesi hedeflenmiştir. Bu çalışmada Amerika üzerine odaklanılmasının sebepleri siber alanın önemli bir parçası olan aktörler arasında siber saldırıların en önemli hedefi olması, önemli bir teknolojik güç olması ve belirleyeceği stratejilerin diğer aktörlerin stratejileri ve siber güvenliğin gelişimi üzerinde kayda değer yansımalarının olacağı beklentisi olarak sıralanabilir.

Siber alanın, siber güvenliğin ve Amerika'nın bu alandaki artan önemi göz önünde bulundurularak bu çalışmada birbiriyle bağlantılı iki ana soruya cevap aranmıştır. Bunlar:

- Siber güvelik Amerika tarafından nasıl bir ulusal güvenlik meselesi olarak ele alınmıştır?
- Siber güveliğin sağlanması adına Amerika'da ne gibi ulusal ve uluslararası önlemler ve stratejiler geliştirilmiştir?

Bu sorulara cevap bulmak için birincil kaynakların niteliksel incelemesi yöntemin temeli olarak belirlenmiştir. Bu incelemenin nedensellik bağını açıklayıcı gücünün Kopenhag Okulu'nun Güvenlikleştirme Teorisi ile desteklenmesi hedeflenmiştir. Bu teorik yaklaşımda, bir sorunun bir güvenlik meselesi haline nasıl getirildiği çeşitli kavramlar ve aşamalarla gösterilmeye çalışılmıştır. Bir sorunun güvenlik meselesi olabilmesi için varoluşsal tehdit (existential threat) tarafından tehdit edilen bir referans

nesnesi (referent object) bulunmalıdır. Bu tehdit, söz edimi (speech act) ile güvenlikleştirici aktörler (securitizing actors) tarafından dile getirilmeli ve meselenin çözümüne yönelik alınacak olağanüstü önlemler (extraordinary measures) toplumun (audience) ikna edilmesi yoluyla meşru kılınmaya çalışılmalıdır. Bu çalışma boyunca söz edimini gösteren resmi belgeler ve raporlar gibi birincil kaynaklara ek olarak kavramları ve literatürde süregelen çalışmaları gözler önüne sermek için kitaplar ve makaleler gibi ikincil kaynaklardan da yararlanılmıştır.

Niteliksel analiz ve güvenlikleştirme teorisi ışığında yapılan incelemeler arasında nedensellik bağı açıklanacak olan X siber alanda çeşitli aktörlerin kötücül hareketleri olarak tanımlanmıştır. Bu süreçte sonuç olarak ortaya çıkan Y'yi belirleme hususunda temel rol savunma ya da saldırı temelli stratejiler ortaya koymaya çalışan bürokratik organlara aittir. Bu bağlamda, tezin temel argümanı ulusal ve uluslararası olarak ikiye ayrılarak sunulmaktadır. Amerika'nın ulusal düzlemde yeni hassas noktalarının neden olduğu ulusal güvenlik kaygılarındaki artış ekseninde bir güvenlikleştirme hareketinden bahsedilebileceği için daha risk ve tehdit odaklı stratejiler belirlemeye çalıştığı savunulur. Uluslararası düzlemde ise, net bir güvenlikleştirme hareketinin olmayışı sonucunda siber alanın gerektiğinde saldırı amaçlı kullanılması gibi daha fırsat odaklı stratejilerin belirlenmeye çalışıldığı savunulur.

Tezin araştırma sorusunun cevaplandırılması ve argümanının ortaya konulması için öncelikle tezin ikinci bölümünde siber alanın genişleyen güvenlik çalışmalarındaki ve uluslararası ilişkilerdeki yeri incelenir. Bu inceleme sırasında siber alanın karakteristik özelliklerine ve bu özelliklerin siber alanı hava, kara, deniz gibi diğer geleneksel alanlardan nasıl ayırdığına değinilir. Ardından siber savaş, siber saldırı ve siber silahların etkileri üzerindeki literatürde süregelen tartışmalar incelenir. Bu tartışmalarla birlikte siber alanın güç, hücum-savunma dengesi ve uluslararası anarşi ile belirsizlik gibi kavramlarla etkileşimi ele alınır. Bu bölümü takip eden üçüncü, dördüncü ve beşinci bölümler üç Amerikan başkanı dönemini –Clinton, Bush, Obama- inceler. Üç

bölüm boyunca, temel güvenlikleştirici aktörler olan bürokratik aktörlerin ve varsa onları destekleyen diğer aktörlerin siber güvenliğin Amerikan ulusal güvenlik meselesi olarak güvenlikleştirilmesi üzerindeki rolleri söz edimleri, referans nesnelerinin ve varoluşsal tehditlerin belirlenmesi, bunlara karşı geliştirilmeye çalışılan olağanüstü önlemler ve toplumun ikna süreçleri kapsamında incelenir. Uluslararası düzlemde ise her dönemin önemli siber güvenlik meselelerine değinilerek Amerika'nın uluslararası siber güvenlik stratejileri belirlenmesindeki tutumu ve bu tutumun nedenleri ile sonuçları incelenir.

Amerika Savunma Bakanlığı siber alanı "internet, telekomünikasyon ağları, bilgisayar sistemleri ve gömülü süreçler ve kontrolörlerden oluşan küresel bir bilgi alanı" olarak tanımlamaktadır. Bu tez de siber alanı kapsadığı unsurların çeşitliliği ve farklılığı ışığında ele almaktadır. Bu çeşitlilik ve farklılıklarla birlikte siber alanın önemli karakteristik özellikleri ortaya çıkmaktadır. Siber alan ve siber güvenlik üzerine önemli çalışmalar yürüten akademisyen Nazli Choucri bu özellikleri geçicilik (temporality), fiziksellik (physicality), yayılma (permeation), değişkenlik (fluidity), katılımcılık (participation), tanımlama (attribution) ve hesap verebilirlik (accountability) olarak sıralar. Son derece kritik yedi özellik arasında tanımlama problemi ve hesap verebilirlik sorunsalı siber alanda sorumluluğu azaltmaları ve cezalandırma mekanizmasını engelliyor olmaları bakımından ayrıca önemli ve belirleyici öneme sahiptir. Bu özellikler aynı zamanda siber alanı sınırları belirli ve bu kadar değişkenlik barındırmayan, sorumluluğun ve saldırgan tanımlamasının daha kolay olduğu diğer geleneksel alanlardan ayıran temel faktörlerdir.

Farklı özellikler sebebiyle doğan bu tür ayrıştırıcı özelliklere karşın, siber alan diğer geleneksel alanlarla önemli benzerlikler de taşımaktadır. Bunların başında süregelen anarşi durumu gelir. Öyle ki tıpkı hava, kara ve denizi kapsayan geleneksel alanlarda olduğu gibi uluslararası siber alanı yöneten ve düzenleyen bir üst otorite olmadığı için anarşi devam etmektedir. Dahası, tanımlama probleminin katkısıyla siber alandaki

belirsizlik yadsınamayacak kadar fazladır. Siber alanın anarşik doğası ve yüksek seviyedeki belirsizlik seviyesi, diğer alanlarda olduğu gibi, güvenlik ve siber alan ilişkisinin kurulmasında oldukça önemli rol oynamaktadır.

Siber alanın karakteristik özelliklerinden ve bu özelliklerin doğurduğu benzerlik ve farklılıklardan hareketle akademik literatürün siber optimistler, siber pesimistler ve siber kuşkucular olmak üzere üç gruba ayrıldığı görülür. Bu üç grup arasında esas tartışma pesimistler ve kuşkucular arasında geçmektedir. Siber optimistler, siber alanın sunduğu demokratikleştirici ve olumlu etkiler üzerinde dururken, pesimistler ve kuşkucular siber alanın savaş hali üzerinde etkileri olup olmadığı üzerinde durarak ayrışırlar. Örneğin, kuşkucular bugüne kadar görülen hiçbir siber saldırının geleneksel savaş özelliklerini taşımadığından bahsederler ve bu nedenle uluslararası politikaya pek yenilik getirmediği için yeni stratejiler belirlemenin çok gerekli olmadığını iddia ederler. Pesimistler ise siber saldırıların geleneksel savaş özelliklerini barındırmamasının bu alana gereken önemi vermemek için bir sebep olmadığının; siber saldırıların kendine has özellikleri ve farklı sonuçları olduğunun altını çizerek siber güvenlik adına yeni stratejiler belirlenmesi gerektiğini savunurlar. Literatürde pesimistler ve kuşkucular tarafından altı çizilen bu iki stratejik noktanın yansımaları Amerika'nın ulusal ve uluslararası siber güvenlik stratejilerinde gözlemlenebilir.

Ayrıca, siber güç kavramı ile birlikte gücün dağılımında değişiklik olması beklenmektedir. Öyle ki, siber silahların üretiminin konvansiyonel silah üretimine göre çok daha kolay ve ucuz olduğu siber alanda güç yalnızca devletlerin tekelinde bulunmamaktadır. Dahası, pek çok siber altyapı hizmeti kullanmak zorunda olan devletler, devlet dışı aktörlerle kıyaslandığında daha çok zayıf noktaya sahiptir. Diğer bir deyişle, gücün değişen doğası ve dağılımının değişmesiyle siber alanda birlikte asimetrik zayıflıklar ve asimetrik güç kavramları belirginleşmektedir. Bu da hücum-savunma dengesi üzerinde önemli etkiler doğurmaktadır. Örneğin, geleneksel

caydırıcılık, savunma mekanizmaları ve hatta hücum stratejileri tanımlama problemi, asimetrik güç ve zayıflıklar meseleleri sebebiyle daha karmaşık bir hal almaktadır.

Literatürde devam eden tartışmaların incelenmesi ve değerlendirimesiyle, artan belirsizlik ve gücün doğasındaki değişim sebebiyle hücum ya da savunma odaklı stratejilerin sonuçlarının tahmin edilemezliğinin siber alanda güvenlik ikilemini beslediği sonucuna varılmaktadır. Dahası, herhangi bir yasal yaptırımın zorluğu ve güçlü bir uluslararası düzenlemenin olmayışı sebebiyle anarşik durum da artış göstermektedir. Buradan anlaşılan odur ki, siber alan tanımlama sorunu ve asimetrik problemler devam ettiği sürece hem yeni zayıflıklar yaratan bir alan olacak hem de bu belirsizliklerin yarattığı gri alandan aktörlerin çıkarları ve güçleri doğrultusunda fayda sağlamasına neden olacaktır.

Amerika'da Bill Clinton'ın başkanlığı, Soğuk Savaş'ın sona ermesiyle birlikte yeni oluşan uluslararası düzen ve güvenlik kaygılarının çeşitlendiği bu ortamda başlamıştır. Bu dönemde, Clinton yönetiminden ilk beklentiler yeni uluslararası düzen kapsamında siyasi ajandanın belirlenmesi olmuştur. Beklentilere, yeni ortaya çıkan tehditlerin ve belirsizliklerin farkında olduğunun altını çizerek cevap vermiştir. Aynı konuşmada, ulusal ve uluslararası ekonomik güvenliği sağlamanın ve diplomasinin önemini vurgulayarak dış politika öncelikleri hakkında ipuçları sunmuştur. Bu demeçler ışığında, Clinton ilk yıllarında ekonomik kalkınma odaklı daha pasif politikalar izlemiş; bu nedenle sıkça eleştirilmiştir. Yönetimine ve politikalarına yöneltilen eleştirileri göz önünde bulunduran Clinton, ikinci dönemiyle birlikte uluslararası gelişmelere daha çok önem vererek dış politika meselelerinde aktifleşmiştir. Her iki dönemi boyunca gerek ekonomik gelişmeleri yönlendirmeye çalışan gerekse Bosna ve Kosova gibi yerlerde yaşanan uluslararası krizlere yönelik politikalar belirlemeye çalışan Clinton yönetiminin siber güvenlik hususundaki tutumu böylesi ulusal ve uluslararası gelişmelerin yaşandığı bir ortamda şekillenmeye başlamıştır.

Bu tez, Clinton döneminde gelişen siber güvenlik kaygılarının nedenlerini birbiriyle ilişkili iki başlık altında ele almaktadır. Bunlardan ilki, siber tehditlerin Amerika'nın kritik altyapılarına yönelik verebileceği zararların ve riskin fark edilmesidir. Daha önce de bahsedildiği üzere, bir teknolojik güç olan Amerika'nın pek çok operasyonel altyapı sisteminin çalışması siber alanın başarılı bir şekilde işlemesine bağlıdır. Bu dönem içerisinde bilgisayar korsanları tarafından saldırıya uğrayan her Amerikan sistemi ile birlikte bu farkındalık artmıştır. Ayrıca, ulaşım, finans, enerji ve telekominikasyon gibi önemli kamusal hizmetlerin de zarar görebilirliği siber güvenlik algısının gelişiminde önemli rol oynamıştır.

Bununla birlikte, Soğuk Savaş sonrasında artan teknoloji paylaşımı ve rekabet ortamı da siber tehditlerin zarar verebilirlik boyutunu artırmıştır. Bir diğer deyişle, ekonomik rekabet adına kaldırılması talep edilen her engelle birlikte Amerikan siber alanı daha çok zarar görebilir hale gelmiştir.

Siber güvenlik anlayışının Clinton döneminde yerleşmesine nedenleri olan bu iki durumla birlikte 1990'larda yaşanan siber saldırılar da yeni güvenlik kaygısının bu dönemde iyice pekişmesine katkı sağlamıştır. Bu saldırılardan en önemlisi kimileri tarafından ilk siber savaş olarak adlandırılan Kosova Krizi sırasında siber silahların hem Amerika hem de Kosova tarafından kullanılması olmuştur.

Bu gelişmeler ışığında siber alandan gelen ve gelebilecek tehditlerden etkilenmesi en olası bürokratik kurumlardan biri olan Amerika Savunma Bakanlığı, Clinton yönetiminin temel güvenlikleştirici aktörü olarak önemli rol oynamıştır. 1994 yılında yayımladıkları raporla birlikte teknolojik gelişmelerle birlikte gelen değişiklere cevap vermenin güvenlik açısından altı çizilerek güvenlikleştirme hareketine ilk katkı sağlanmıştır. Dönem boyunca çeşitli raporlarda ve demeçlerde gözlenebilen söz edimi hareketleriyle siber alanın getirdiği ve getireceği tehditler ve bu tehditlerin Amerikan ulusal güvenliğine olası zararları sürekli olarak vurgulanmıştır. 1996 yılında yayımlanan raporda olası bir bilgi savaşı durumu göz önünde bulundurularak yeni

olağanüstü önlemlerin alınması gerektiğinin altı çizilmiştir. Tüm bunlar güvenlikleştirme hareketi açısından oldukça önem taşımaktadır.

Birinci dönemi ikinci dönemine göre daha pasif olan Clinton ise siber güvenlik adına güvenlikleştirme hareketlerine ikinci dönemi ile aktif olarak başlamıştır. Yayımladığı yönergelerle birlikte siber devrimin getirdikleri ve buna karşı alınması gereken önlemlerin üzerinde durmuştur. Genellikle özel sektör elinde bulunan kritik altyapıları koruma tabanlı olan bu önlemler özel ve kamu sektörü arasında işbirliğinin ve bilgi paylaşımının önünü açmaya yönelik hamleleri içermiştir. Bu hamleler, Clinton yönetiminde Kongre'de çok da fazla yankı bulamamış olmakla birlikte yasama organının da siber güvenlik meselesine tamamen kayıtsız kalmadığı çok kısıtlı olan söz edimleri ekseninde gözlemlenmiştir.

Uluslararası siber güvenlik stratejilerinin gelişimi açısından bakıldığında ise Clinton başkanlığı güvenlikleştirme hareketinin yok denecek kadar az olduğu ve siber alanın stratejik öneminin fark edildiği bir dönemi temsil etmektedir. Öyle ki, Kosova'da kullanılan siber silahlarla birlikte bir yanda bu silahların zarar verici etkisi ortaya çıkmış diğer yanda ise siber alanın saldırı amaçlı kullanılabileceğinin de farkına açık bir şekilde varılmıştır. Bu farkındalık sebebiyle, Amerika herhangi bir uluslararası sınırlayıcı uygulamanın ne tarafı olmak istemiş ne de böyle bir uygulamanın ya da uluslararası hukuk zeminin oluşturulmasına ön ayak olmuştur.

Sonuç olarak, Clinton döneminde ulusal zeminde gözlemlenebilen güvenlikleştirme hareketiyle birlikte çeşitli risk tabanlı stratejiler ortaya konmaya iddia edilebilirken uluslararası düzlemde siber alanın sunduğu stratejik önemle birlikte daha fırsat tabanlı stratejilerin belirlendiği söylenebilir.

Siber güvenlik, Bush döneminde, 11 Eylül saldırılarıyla önemli bir değişime uğrayan Amerikan güvenlik kaygıları ve stratejileri çerçevesinde gelişim göstermiştir. Bu dönemde, temel güvenlikleştirici aktörler –Savunma Bakanlığı ve Başkanlık- ve onları daha kısıtlı bir şekilde destekleyen güvenlikleştirici aktör –Kongre- sabit olmakla

birlikte 11 Eylül ile birlikte kurulan Amerika İç Güvenlik Bakanlığı önemli bir güvenlikleştirici aktör olarak eklenmiştir. Temel güvenlikleştirici aktörlere ek olarak Bush döneminde araştırma merkezleri ve medya kuruluşları gibi hükümet dışı organların da siber güvenlik üzerinde etkisi olmuştur. Detaylı olarak incelendiğinde, İç Güvenlik Bakanlığı'nın siber güvenlik adına sürdürdüğü kurumsallaşma hareketleri göze çarpmaktadır. Bu bakanlığın siber güvenlik meselesindeki rolü daha çok kamu ve özel sektör arasındaki işbirliği mekanizmasının çalıştırılmasına yönelik olmuştur. Hem kurumsallaşma hareketleri hem işbirliği mekanizmasının geliştirilmesine yönelik girişimleri hem de yayımlanan raporlarda terörizmin böylesine yükseldiği bir noktada siber güvenliğin öneminden bahsetmesi sebebiyle İç Güvenlik Bakanlığı dönemin önemli güvenlikleştirici aktörlerinden biri sayılmıştır. Savunma Bakanlığı ise Clinton döneminde belirginleşen aktif rolüne devam etmiştir. Siber güvenliğin ve siber tehditlerin önemini vurgulamak için hem terörist örgütlerin hem de diğer devletlerin sahip olduğu gücü ortaya koymaya çalışarak bu alanda kamusal bir farkındalık yaratılmasında önemli rol oynamıştır. Ayrıca, Amerika'nın karşısında yer alabilecek aktörlere karşı yeniden düzenlenmesi gereken caydırıcılık mekanizması üzerinde durarak bir takım önlemlerin alınmasına yönelik adımlar atmıştır. Bush, bu iki önemli bürokratik kurumun oynadığı aktif rolü söz edimi hareketleriyle tamamlamaya çalışmıştır. Yayımladığı yönergelerde, Amerika'nın siber alandaki kırılganlığının terörist örgütlerce nasıl değerlendirilebileceğine vurgu yaparak siber güvenliğe karşı alınabilecek önlemleri ve yapılabilecek saldırıları terörizm temelinde meşrulaştırmaya çalışmıştır. Kongre'nin rolü Clinton dönemiyle benzerlik taşımaktadır. Yine de, siber güvenliğin terörizmle bağlantılı olarak ele alınarak güvenlikleştirilmesi hareketine bir siber terörizm tanımı sunarak katkı sağlamıştır. Hükümet dışı kurumlar ise siber güvenliğe dikkat çekmekte daha net bir tutum izlemiştir. Gerek medya gerekse diğer kurumlar siber terörizmin sebep olabileceği zararların altını çizerek daha aktif güvenlik stratejileri belirlenmesi gerektiğini savunmuşlardır. Bahsedilen kurumlar ulusal siber güvenlik stratejilerinin geliştirilmesi açısından önemli rol oynamış ve siber güvenlik

anlayışının terörizmle pekiştirilerek yerleştirilmesine katkı sağlamıştır. Böyle bir durumda güvenlikleştirme hareketinin devamından bahsedilmekle birlikte hala tamamlanmış bir güvenlikleştirme hareketinden bahsetmek mümkün değildir.

Bush dönemi, uluslararası açıdan incelendiğinde, siber alanın stratejik kullanımı açısından Clinton döneminin devamı niteliğindedir. Amerika, her ne kadar siber alanın doğurduğu zayıflıkların farkında olsa da Rusya'nın da bir kez daha gösterdiği gibi siber alanın stratejik olarak kullanımını kısıtlayacak herhangi bir uluslararası yasal düzenlemenin taraftarı olmadığını bu dönemde de göstermiştir.

Bu çalışmada, seçim kampanyası sırasında bilgisayar sistemleri siber saldırıya uğrayan Obama'nın başkanlığı siber güvenliğe ait güvenlikleştirme hareketinin en üst düzeye çıktığı dönem olarak değerlendirilmektedir. Bu dönemde tüm güvenlikleştirici aktörler ve özellikle Obama'nın aktif rol oynadığı söylenebilir. Başkan seçildikten hemen sonra yayımlanan raporlarda siber alanın önemi vurgulanarak ulusal ve uluslararası alanda daha kapsamlı stratejilerin geliştirilmesiyle hızlı bir başlangıç yapılması gerektiği vurgulanmıştır. Bunun adına, Obama, İç Güvenlik Bakanlığı'nın ulusal düzlemdeki düzenleyici rolünü genişletmeye çalışmış; Amerikan halkının siber güvenlik hususunda bilinçlenmesi için 2009 yılı Ekim ayını Ulusal Siber Güvenlik Farkındalık Ayı olarak ilan etmiş; ulusal yasal düzenlemelerin yapılması adına yetkilerini kullanmıştır. Bunlarla birlikte Obama döneminin en önemli stratejik belgelerinden biri olan Amerikan Siber Operasyon Politikaları belgesini yayımlamıştır. Bu belge, Amerika'nın siber alanı gerek savunma gerekse hücum odaklı olarak nasıl kullanacağını belirtmesi açısından oldukça önemlidir. Ayrıca, Amerika Savunma Bakanlığı gerektiğinde 'acil durum siber hareketleri' kapsamında başkanın onayına gerek duymadan hareket edebilmekle yetkilendirilmiştir. Ulusal ve uluslararası önlemlerin belirlendiği bu belge Clinton döneminden bu yana devam eden güvenlikleştirme hareketinin en somut sonuçlarından biri olarak değerlendirilebilir. Başkanlık makamının rolü, İç Güvenlik Bakanlığı'nın kamu ve özel sektör arasında işbirliğini sağlamak ve ulusal bir siber

güvenlik stratejisi belirlemek üzere inşa edilen yapılar dahilinde hızlanan kurumsallaşma hareketleriyle pekiştirilmiştir. Aynı zamanda, söz edimi ile düşman, tehdit ve zayıflıkları vurgulayarak güvenlikleştirici aktör olarak ulusal siber güvenlik stratejisinin geliştirilmesinde önemli rol oynamıştır. Savunma Bakanlığı'nın güvenlikleştirici aktör olarak rolü ise hem söz edimleri hem başkanlık makamınca verilen yetkiler hem de Amerikan Siber Komuta Merkezi'nin kurulmasıyla daha net bir hale gelmiştir. Dönemin en önemli gelişmelerinden bir diğeri ise Kongre'nin artan rolü olarak görülebilir. Amerikan halkının kişisel güvenlik kaygılarını göz önünde bulundurarak hareket etmeye çalışan ve bunun sonucunda iç siber güvenlik stratejilerinin hayata geçirilmesi hususunda çok aktif rol oynayamayan kongrenin rolü, başkanın hem yasamayı hem de halkın farkındalığını etkileyen hamleleriyle önemli bir duruma gelmiştir. Öyle ki, Clinton döneminden bu yana devam eden çok daha kısıtlı söz edimi hareketlerinin artmasına ek olarak çeşitli siber güvenlik yasaları geçirilmiştir. Beklenenden az da olsa bu tarz yasaların geçirilmesi güvenlikleştirme hareketi açısından oldukça önem taşımaktadır. Tüm bu gelişmeler ışığında, Obama'nın başkanlığı döneminde risk tabanlı bir takım olağanüstü önlemlerin geliştirilmesiyle daha da belirginleşmiş bir ulusal güvenlikleştirme hareketinden bahsedilmektedir.

Uluslararası siber güvenlik stratejileri ise bu dönemde gerçekleşen ve hava,deniz ve kara gibi alanlarda gerçekleşmesi durumunda daha farklı sonuçlar doğurabilecek olayların etkisi dahilinde net bir boyut kazanamamıştır. Bu dönemin önemli olaylarından ilki Amerika ile Kuzey Kore arasında gerçekleşen ve tanımlama probleminin neden olduğu belirsizlik dahilinde ilerleyen Amerikan film sektöründen önemli bir firmanın siber korsanlarca saldırıya maruz kalması ve önemli bir ekonomik zarara uğratılmasıdır. Buna benzer ikinci durum ise Çin'den Amerika'ya yönelen siber saldırıların sıklaşması fakat tanımlama ve hesap verebilirlik problemleri sebebiyle net bir yaptırım uygulanamamasıdır. Bu saldırılar sonrasında Amerika yine de gelişmiş bir uluslararası siber güvenlik stratejisi belirleme taraftarı olmamıştır. İki gelişmeden farklı

olarak bu dönem Amerika'nın siber alanı stratejik ve saldırı amaçlı kullanımının ortaya çıktığı dönemdir. Öyle ki, İran'ın nükleer silah geliştirmek üzere sürdürdüğü faaliyetleri kısıtlamak isteyen Amerika, İran'ın Natanz'da bulunan nükleer tesisine Stuxnet ismini verdikleri siber silahla saldırmış ve bu saldırı sonucunda tesisteki nükleer faaliyetlere belirli bir oranda zarar vermeyi başarmıştır. Amerika'nın siber alandaki gri alanlardan faydalanarak diğer alanlarda izlediği politikaları desteklemek amaçlı siber alandan stratejik olarak faydalanması ve uluslararası aktörlerin siber alandaki tehditleri farklı tanımlamaları sebebiyle oluşan farklılıklar bu dönemde de net bir uluslararası güvenlikleştirme hareketi olmayışını açıklayan sebeplerdir. Bir diğer deyişle, Amerika Clinton döneminden bu yana uluslararası düzlemde daha çok siber kuşkucular tarafından önerilen fırsat odaklı stratejik politikalar izlemektedir.

Sonuç olarak, siber alanın yükselmesi ve karakteristik özelliklerinin belirginleşmesi sonucunda özellikle Clinton döneminde ortaya çıkan siber güvenlik algısı süreç içerisinde Amerikan ulusal güvenliğinin önemli bir parçası haline gelmiştir. Bu süreçte, başkanlık kurumu, Savunma Bakanlığı, İç Güvenlik Bakanlığı ve Kongre güvenlikleştirici aktörler olarak giderek daha önemli bir rol oynamış ve risk tabanlı ulusal siber güvenlik stratejilerinin belirlenmesine olanak sağlamışlardır. Yani, ulusal düzlemde bir güvenlikleştirme hareketinden bahsedilebilse de, daha kapsamlı bir olağanüstü önlem hayata geçirilemediği için tamamlanmış bir güvenlikleştirme hareketinden bahsetmek henüz çok mümkün görünmemektedir. Uluslararası siber güvenlik ise üç başkan dönemi boyunca fırsat odaklı stratejilere odaklanmış olup net bir güvenlikleştirme hareketine dahi maruz kalamamıştır. Siber alanın stratejik olarak kullanımı ve uluslararası düzlemdeki aktörlerin fazlalığı sebebiyle belirlenemeyen – hatta belirlenmek istenmeyen- uluslararası önlemler uluslararası bir güvenlikleştirme hareketinin önündeki en önemli iki engel olarak değerlendirilmektedir. Kısaca, ulusal düzlemde siber pesimistlerin argümanlarına daha yakın olarak yeni ve risk odaklı stratejiler güvenlikleştirme hareketi kapsamında gözlemlenebilirken, uluslararası

düzlemde siber kuşkucuların argümanlarına daha yakın olarak bir güvenlikleştirme hareketinin yokluğunda fırsat odaklı stratejilere odaklanıldığı gözlemlenebilmektedir.

APPENDIX B: TEZ FOTOKOPİSİ İZİN FORMU

ENSTİTÜ

Fen Bilimleri Enstitüsü ☐

Sosyal Bilimler Enstitüsü ■

Uygulamalı Matematik Enstitüsü ☐

Enformatik Enstitüsü ☐

Deniz Bilimleri Enstitüsü ☐

YAZARIN

Soyadı : Küçükaydın
Adı : Duygu
Bölümü : Uluslararası İlişkiler

TEZİN ADI (İngilizce): NATIONAL AND INTERNATIONAL CYBERSECURITY STRATEGIES OF THE UNITED STATES: A SECURITIZATION ATTEMPT?

TEZİN TÜRÜ : Yüksek Lisans ■ Doktora ☐

1. Tezimin tamamından kaynak gösterilmek şartıyla fotokopi alınabilir. ■
2. Tezimin içindekiler sayfası, özet, indeks sayfalarından ve/veya bir bölümünden kaynak gösterilmek şartıyla fotokopi alınabilir. ☐
3. Tezimden bir bir (1) yıl süreyle fotokopi alınamaz. ☐

TEZİN KÜTÜPHANEYE TESLİM TARİHİ: