



KADIR HAS UNIVERSITY
SCHOOL OF GRADUATE STUDIES
PROGRAM OF INTERNATIONAL RELATIONS

**THE EVOLUTION OF DETERRENCE THEORY FOR A
NEW DIMENSION:
THE CHALLENGES OF CYBER DETERRENCE
STRATEGIES IN INTERNATIONAL SYSTEM**

ATAKAN YILMAZ

MASTER'S THESIS

İSTANBUL, MAY, 2019

**THE EVOLUTION OF DETERRENCE THEORY FOR A
NEW DIMENSION:
THE CHALLENGES OF CYBER DETERRENCE
STRATEGIES IN INTERNATIONAL SYSTEM**



ATAKAN YILMAZ

MASTER'S THESIS

Submitted to the School of Graduate Studies of Kadir Has University in partial
fulfilment of the requirements for the degree of Master's in the Program of International
Relations

İSTANBUL, MAY, 2019

DECLARATION OF RESEARCH ETHICS /
METHODS OF DISSEMINATION


I, Atakan YILMAZ, hereby declare that;

- this Master's Thesis is my own original work and that due references have been appropriately provided on all supporting literature and resources;
 - this Master's Thesis contains no material that has been submitted or accepted for a degree or diploma in any other educational institution;
 - I have followed "Kadir Has University Academic Ethics Principles" prepared in accordance with the "The Council of Higher Education's Ethical Conduct Principles"
- In addition, I understand that any false claim in respect of this work will result in disciplinary action in accordance with University regulations.

Furthermore, both printed and electronic copies of my work will be kept in Kadir Has Information Center under the following condition as indicated below:

- The full content of my thesis/project will be accessible from everywhere by all means.

ATAKAN YILMAZ



31 MAY, 2019

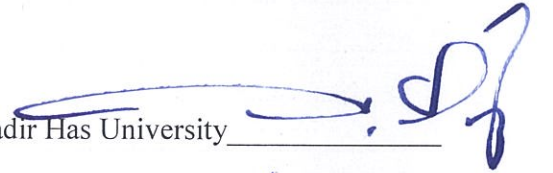
KADIR HAS UNIVERSITY
SCHOOL OF GRADUATE STUDIES

ACCEPTANCE AND APPROVAL

This work entitled **THE EVOLUTION OF DETERRENCE THEORY FOR A NEW DIMENSION: THE CHALLENGES OF CYBER DETERRENCE STRATEGIES IN INTERNATIONAL SYSTEM** prepared by **ATAKAN YILMAZ** has been judged to be successful at the defense exam held on **31 MAY, 2019** and accepted by our jury as **MASTER'S THESIS**.

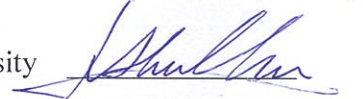
APPROVED BY:

Assoc. Prof. Dr. Ahmet Salih Bıçakcı (Advisor) Kadir Has University



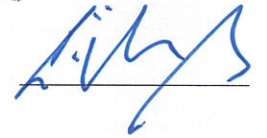
Assoc. Prof. Dr. Hamid Akın Ünver

Kadir Has University

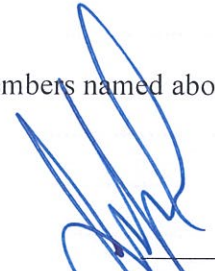


Ast.Prof. Dr. İbrahim Mazlum

Marmara University



I certify that the above signatures belong to the faculty members named above.



Prof. Dr. Sinem Akgül Açıkmeşe
Dean of School of Graduate Studies

DATE OF APPROVAL:

TABLE OF CONTENTS

ABSTRACT	v
ÖZET	vi
ACKNOWLEDGMENT	vii
LIST OF TABLES	ix
LIST OF FIGURES	x
1. INTRODUCTION	1
1.1 THE BASIC CONCEPTS OF CYBERSPACE	2
1.2 THE EMERGING RELATION BETWEEN CYBERSPACE AND INTERNATIONAL RELATIONS	4
1.3 THE PLACE OF STATE ACTOR IN THE CYBERSPACE	10
1.4 THE STRUCTURE OF THE THESIS	13
1.5 THE METHODOLOGY OF THE THESIS	15
2. FROM CLASSICAL DETERRENCE TO CYBER DETERRENCE	24
2.1. CLASSICAL DETERRENCE THEORY	24
2.1.1. The Types of Classical Deterrence	28
2.1.2. The Core Elements of Classical Deterrence	31
2.2. CYBER DETERRENCE	41
2.2.1 Main Components and Types of Cyber Deterrence Theory	43
2.2.2 Cyber Deterrence by Denial	44
2.2.3 Cyber Deterrence by Punishments	46
2.3 ALTERNATIVE CYBER DETERRENCE STRATEGIES	47
2.3.1 Cyber Deterrence by Resilience	48
2.3.2 Cyber Deterrence by Active Defense	51
2.3.3 Cyber Deterrence by Defend Forward.....	53
2.3.4 Cyber Deterrence by Norms	54
3. TYPES OF CYBER THREATS AND CYBER ATTACKS	57
3.1. CYBER THREATS WITH REGARD TO SOURCES	57
3.2. CYBER THREATS WITH RESPECT TO AGENTS	58
3.2.1. Economic Threat Agents	61
3.2.2. Political Cyber Threat Agents	62
3.3. CYBER ATTACKS	72
3.3.1. The Concepts of Cyber Attack	73
4. THE DIFFICULTIES IN IMPLEMENTING CLASSICAL DETERRENCE TO CYBERSPACE	78
4.1. THE DIFFICULTY OF ATTRIBUTING THE OFFENDERS	80

4.2.	THE DIFFICULTY OF DEMONSTRATING CYBER CAPACITY	83
4.3.	THE DIFFICULTY OF CALCULATING THE IMPACT OF THE CYBER ATTACKS AND REPEATABILITY	85
4.4.	THE DIFFICULTY OF PROPORTIONATE RESPONSE AND RISK OF ESCALATION.....	87
4.5.	THE PROBLEM OF ASYMMETRY AND ENGAGEMENT OF THIRD PARTIES INTO POLITICAL CONFLICT	89
4.6.	THE DIFFICULTY OF DRAWING RED LINES.....	93
4.7.	THE DIFFICULTY OF DISSUADING STATES FROM EXPLOITING GREY ZONES AND CREATE INTERNATIONAL NORMS IN AN ENVIRONMENT WHERE NOBODY TRUSTS EACH OTHER.....	96
4.8.	THE DIFFICULTY OF PROVIDING ABSOLUTE SECURITY.....	99
5.	WHAT CYBER ATTACKS TELL ABOUT CYBER DETERRENCE AND STATES' STRATEGIES ABOUT NEW DIMENSION?	101
5.1.	FINDINGS OF ANALYSIS AND HYPOTHESES	102
6.	CONCLUSION.....	117
	BIBLIOGRAPHY	126
	CURRICULUM VITAE.....	145
	APPENDIX A	146
A.1	260 CYBER ATTACKS WITH DETAILS.....	146

THE EVOLUTION OF DETERRENCE THEORY FOR A NEW DIMENSION:
THE CHALLENGES OF CYBER DETERRENCE STRATEGIES IN INTERNATIONAL
SYSTEM

ABSTRACT

States that have become the main actors of the international system after the Treaty of Westphalia; have seen cyberspace as a new field to carry out their traditional policies in addition to land, sea, air, and space. However, unlike other dimensions, since cyberspace is human-made and its design philosophy attaches importance to rapid and anonymous information sharing at low cost among parties rather than security; states face several non-traditional problems such as attribution problem, abundance of non-state actors that can challenge the state, and the asymmetric relations between states. Therefore, the states in which Information and Communication Technologies (ICT) are widely used, critical infrastructures are more integrated with ICT and has more intellectual properties; have started to seek security strategies to prevent cyber-attacks by adversaries. As a result of this seeking, since it is a prominent strategy in international politics during the Cold War period, the applicability of deterrence strategy has begun to be discussed. In this direction, while this thesis examining the applicability of classical deterrence theory in cyberspace, also addressing the obstacles to the implementation of cyber deterrence and possible ways to acquire successful cyber deterrence. Thus, firstly the main assumptions, necessary prerequisites, major and alternative strategies of cyber deterrence are discussed by looking at classical deterrence theory. Then, by classifying cyber threats and the materialization of threats, cyber-attacks, the major obstacles to the successful cyber deterrence strategies will be illustrated. Besides, by analyzing 260 cyber-attacks through six categories as time, victim, offender, attack type, target, and response; practices are going to be tested the theory. In this framework, since a cyber deterrence strategy that uses only cyber tools fails to prevent all cyber-attacks; by discussing the possibility of a restricted and hybrid cyber deterrence strategy that includes political, economic, military and diplomatic instruments, this study will be concluded.

Keywords: Cyber Deterrence, Cyberspace, Cyber Attacks, Deterrence, International Relations, International Security, Foreign Policy, International System,

CAYDIRICILIK TEORİSİNİN YENİ BİR BOYUT İÇİN EVRİMİ: ULUSLARARASI SİSTEMDE SİBER CAYDIRICILIK STRATEJİLERİNİN KARŞILAŞTIĞI GÜÇLÜKLER

ÖZET

Vestfalya Antlaşması sonrasında uluslararası sistemin başat aktörleri haline gelen devletler siber uzayı kara, deniz, hava ve uzaya ek olarak geleneksel politikalarını gerçekleştirecekleri yeni bir alan görmektedirler. Fakat diğer boyutların aksine siber uzay insan yapımı olduğu ve tasarım felsefesi güvenlikten daha ziyade taraflar arasında düşük maliyetle hızlı ve anonim bilgi paylaşımına önem verdiği için devletler; tespit/isnat, çok fazla devlet dışı aktörlerin devlete meydan okuyabilmesi ve devletler arasındaki asimetrik ilişkinin olması gibi geleneksel olmayan bir dizi sorunla karşılaşmaktadırlar. Bu nedenle, özellikle kritik alt yapıların bilgi ve iletişim teknolojileriyle (ICT) daha entegre olduğu, ICT'lerin daha yaygın olarak kullanıldığı ve fikri mülkiyete daha fazla sahip olan ülkelerde; diğer devletlerden ve devlet dışı aktörlerden gelebilecek siber saldırıları engellemek için güvenlik stratejileri arayışına girilmiştir. Bu arayışın bir sonucu olarak ise özellikle Soğuk Savaş döneminde uluslararası politikada oldukça ön planda yer alan caydırıcılık teorisinin siber uzaydaki uygulanabilirliği tartışılmaya başlanmıştır. Bu doğrultuda bu tez çalışması geleneksel caydırıcılık teorisinin siber uzayda uygulanabilirliğini sorgularken aynı zamanda bu teorinin siber uzayda uygulanmasının önündeki engelleri araştırmakta ve siber uzay için nasıl bir caydırıcılık stratejisinin kurgulanabileceğini tartışmaktadır. Bunun için ilk olarak klasik caydırıcılık teorisinden yola çıkarak siber caydırıcılığın temel varsayımları, gerekli ön koşulları, temel ve alternatif stratejileri ele alınırken, ikinci olarak siber uzaydaki tehditler ve tehditlerin gerçekleşmesiyle ortaya çıkan siber saldırılar sınıflandırılarak siber caydırıcılığın başarılı olmasının önündeki engellerin neler oldukları belirtilecektir. Ayrıca önemli 260 siber saldırı zaman, saldırgan ve saldırılan devlet, saldırı türü, hedef ve yanıt olmak üzere altı başlık altında incelenerek teoriğin dışında pratikte de hangi sorunlarla karşılaşıldığı analiz edilecektir. Bu çerçevede yalnızca siber araçlara başvuran bir siber caydırıcılık stratejisinin tüm siber saldırıları engellemede başarısız olduğu gerçeğinden yola çıkarak politik, ekonomik, askeri ve diplomatik araçları da içinde barındıran hibrit ve sınırlı bir siber caydırıcılık stratejisinin siber uzayda başarılı olma olasılıkları tartışılarak çalışmaya son verilecektir.

Anahtar Sözcükler: Siber Caydırıcılık, Siber Uzay, Siber Saldırı, Caydırıcılık, Uluslararası İlişkiler, Uluslararası Güvenlik, Dış Politika, Uluslararası Sistem

ACKNOWLEDGMENT

I would like to thank my thesis adviser, Dear Assoc. Professor Ahmet Salih BIÇAKÇI who has given me every kind of continuous support and encouragement in every stage of this thesis with patience, and has helped me to look at life from a broader perspective by sharing his knowledge and experiences; to thank dear faculty members of the Department of International Relations of Kadir Has University who sincerely assist me whenever I needed and gave a chance to study on a scholarship all my during the graduate study; to thank the faculty members of the Department of Political Science and International Relations of the Istanbul University for their contribution to during the my bachelor degree; to thank my dear family members Aygün, Kerim, Sibel and Pelin YILMAZ who have always with me and give all kinds of material and moral supports; to thank Gizem SOLMAZ who has always been there to unconditionally help, support and encourage me ; to thank my friends and colleagues Ali Emre ELDEM and Cem İsmail SAVAŞ, who have made things easier for me during the writing process of my thesis.



To My Family

LIST OF TABLES

Table 1.1 Six Classification of the Analyses	17
Table 1.2 Most Attack Countries Through Cyber Tools	20
Table 1.3 Number of Cyber Attacks by Suspected States.....	21
Table 1.4 Targets that Attacked by Suspected State via Cyber Tools	21
Table 1.5 Target Sectors by Cyber-Attacks.....	22
Table 1.6 Types of Cyber-Attacks.....	22
Table 1.7 Response by Victim State Against Suspended State.....	23
Table 5.1 Suspected State-Victim State Cross Tubulation.....	102
Table 5.2 Types of Cyber-Attacks by Number.....	106
Table 5.3 Suspected Actor, Type of Cyber Attacks Cross Tabulation.....	106
Table 5.4 Most Suspected States and Their First Three Targets.....	108
Table 5.5 Suspected States - Sector Cross Tabulation.....	108
Table 5.6 Top Four Countries That Carry Out DDoS Cyber Attacks.....	111
Table 5.7 Response for Total 21 Integrity Cyber-Attacks that Targets Integrity.....	114
Table 5.8 Response for Total 14 sabotage Cyber-Attacks.....	114
Table 5.9 Response for 219 Cyber-Attacks That Targets Confidentiality.....	114
Table 5.10 Response for Total 260 Cyber-Attacks.....	115
Table A.1 260 Cyber Attacks with Details.....	146

LIST OF FIGURES

Figure 3.1 Detailed Threat Agent Classification by Vidalis & Jones,.....60



1. INTRODUCTION

With the Westphalia Peace Treaty, the International System that was composed of feudal lords, princes, religious authorities and emperors had started to slowly turn into a new system which centralized states were the main actors. By many domestic, international, political and economic developments in Europe, centralized states evolved into the national states. Particularly after World War I, with the idea of national self-determination, International System was mainly made up of nation-states. In this system, states have a very central position since nation-states are regarded as an only legitimate authority in the International System (Baylis, 2008, p. 71). As Max Weber who is a sociologist and philosopher underlined that “*state was the only institution that had a monopoly of the legitimate use of force within a given territory*” (2008, pp. 161-162). Also, the famous book “*Leviathan*” written by Thomas Hobbes underlined that people renounced their power and gave all their rights to absolute power which is “*sovereign state*” (Hobbes, 1968, p. 114). All these classical works point that a sovereign state is the only absolute authority in the international system where the right of using legal force and carrying out diplomatic relations pertain to a state actor.

However, with the advent of the cyberspace, widely usage of Information and Communication Technologies (ICT) by people and, especially with cyber-attack against Estonia in 2007 and renowned Stuxnet cyber-attack against Iran in 2010, Westphalian Nation System which is used to refer sovereign state that possesses the monopoly of power inside the borders, has faced a significant challenge and even its future has been started to be questioned. The structural features of cyberspace mainly cause this situation since in cyberspace in contrast to the main structure of the nation-state system, there are no borders and limited numbers of actors but many different types of actors and complexities. In addition, according to one of the primary understanding about security, initially enemy must be recognized and its capacity should be measured. However, in case of an anonymous cyber-attack, states cannot precisely define attackers and cannot calculate the impact of cyber-attack. Also, carrying out cyber-attacks at peacetime thanks to anonymity advantage led to the loss of the meaning of war and peace concepts. Thereby, international law mechanism has started to stagger against the cyber-attacks. Therefore, the uncertainty of borders, governance, actors of cyberspace, and unbinding international law have led to change in states’ basic understanding of security, governance and

war. Moreover, many theorists who put the state at the center of their analyses, have difficulties in explaining cyberspace related cases.

While all these changes have been taken place and increased usage of cyberspace and dependency to it have started to threaten this system, the new concern appeared in the eyes of states: How can a state deter new types of threats (cyber threats)? The structure of this thesis is also built around a similar concern: *How the advent of cyberspace has affected/changed the deterrence and foreign policies of states?* Before searching for answers to this question, it is more appropriate to explain the following questions: 1) what is the concept of cyberspace? 2) How technologic developments and advent of the cyberspace have a significant impact on the field of International Relations (IR)?

1.1 THE BASIC CONCEPTS OF CYBERSPACE

Science fiction writer William Gibson first used the concept of cyberspace in his book “Burning Chrome” in 1982. However, he explained the term of cyberspace in detail in his other book, “Neuromancer” in 1984 as follow:

“Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data. Like city lights, receding” (Gibson, 1984, p. 69).

While the definition of the concept of cyberspace was firstly described as above, however, it could not escape from the changing. Many institutions and states have defined the concept of the state in line with their criteria. In these definitions, cyberspace is basically defined as the online world of computer networks (Merriam-Webster Online Dictionary, 2019) or virtual environment in which communication occurs through networks of the computer (Oxford Online Dictionary, 2019). However, these kinds of definitions of cyberspace have a notable absence: *“Social Dimension”*. People are the users of cyberspace who both most benefited and exposed to the problems from cyberspace. Therefore, to exclude social dimension from definitions causes to have difficulty in understanding and explaining the effects and the reason for problems caused by human beings and technical dimension. Hence, as Salih Bıçakcı underlines that

cyberspace could be defined as a non-physical space where information systems that interconnected each other interact and communicate with each other and people (2014, p. 106).

Cyberspace has been considered as a fifth dimension after four dimensions which are ground, sea, air and space. However, cyberspace has inherently different features from the other dimensions: Firstly, in contrast to other dimensions, cyberspace is not a given space but is a human made. This distinction makes cyberspace a place where is in a constant state of flux. Therefore, parties of the cyberspace affect not only the content of the cyberspace but also the fundamental structure cyberspace. Secondly, entering into cyberspace does not require high cost by comparison with having a presence such as in oceans and space (Fred, 2015, pp. 12-15). Hence, in cyberspace, not only states play an important role, but also non-state actors and individuals play relatively important role in comparison to other dimensions due to the low cost to enter cyberspace and easy access to cyberspace. Nevertheless, as cases will show that, although many dogs placed in cyberspace and their bites can hurt states are the real dogs in the cyberspace (Nye, 2010, p. 13). Thirdly, in contrast to Hans Morgenthau (1960, p. 62) who said that “national security relied on the integrity of a nation’s border”, cyberspace has no borders and limits. In the first place, this distinction challenges the concept of the state itself. Besides, there is no authority in the cyberspace, even to identify actors is problematic due to the attribution problem as will be explained in detail. Therefore, in cyberspace, it can be claimed that the anarchy is more visible than other dimensions. Fourthly, to calculate the impact of cyber-attacks on the target is very challenging. For instance, the impact of a bomb can approximately be calculated but if the attack is launched in the forms of manipulation as Russia did in 2016 the US Presidential Election which allegedly heavily impacted the results in favor of Donald Trump, could it be counted as *casus belli*?

Also, cyberspace should not only be considered as a virtual dimension since on the contrary to the general public discourse that is cyberspace only consists of the virtual layer; actually, it contains four layers which are “physical, codes, content and regulatory”. Hence, considering cyberspace only as virtual dimension will create severe obstacles to our understanding of the concepts and the problems and solutions to be explained by these concepts.

In this context, the physical layer can be mentioned as the first layer of cyberspace. The main elements of this layer are physical elements or in other words hardware. While these equipments can be the part of the computer such as motherboards, hard disks, however, they are not restricted to only computer parts but also as SCADA (Supervisory Control and Data

Acquisition), game console, telephone, smart watches and so forth so on. The second layer is the software. This layer has established a relation between the physical layer and the virtual world. In other words, without the layer of codes, the physical elements are not used. Therefore, these two layers compromise the frame layer of the cyberspace. While both physical and code layer are essential for cyberspace, without the layer of content, they have no meaning. It is not only the layer that conveys messages but also layer that stores the data such as the strategic information of states and secret codes of nuclear missiles. Last but not least, the regulatory layer limits the use of the internet and content through national legal regulations. While the first three layers are same all over the world, however, the regulatory layer changed by country according to concerns of the state (Bıçakcı, 2014, pp. 107-111). After these brief conceptual and technical parts of cyberspace, we can go into detail about the relation of cyberspace and the field of International Relations. For this, it is necessary to understand how such a technical concept as cyberspace has established a relationship with the social sciences. In this context, to understand this relation can shed light upon the significant points about both cyberspace and field of International Relations.

1.2 THE EMERGING RELATION BETWEEN CYBERSPACE AND INTERNATIONAL RELATIONS

Artur Suzik pointed out that Information and Communication Technologies (ICTs) have become an integral part of the continuity of our daily life in the modern age (Klimburg, 2012, p. X). Their popularity in society is mainly stemmed from their key features which are easy accessibility, affordability, the ability of effective control of complicated systems and rapid communication. Notably, Internet of Things (IoT) which is a concept to depict all devices that has an internet connection; automation devices which mainly used in complex systems where many independent and integrated parts are included in the structure; and artificial intelligence, have placed themselves within all parts of modern society. The advantages of cyberspace offer abilities to governments, individuals and organisations to obtain and exploit information at an unprecedented level. Therefore, as these devices have been appealed to govern societies, to do business and even to express freedom of speech (Geers, 2011, p. X); the dependency on these technologies has increased as well. This so-called dependency to these devices can be seen from data of Statista which that in 2017, the number of IoTs was 20.35 billion; however, it is estimated to reach 75 billion by 2025 with the rise of more than four times. (Statista, 2018) Also, while the number of these devices has been increasing, there is also a remarkable increase

in the number of people who use them actively or indirectly as well. According to Internet World Stat, the number of internet users all over world is 4,383,810,342 on the date of 31 March 2019. (Internet World Stats, 2019)

While cyberspace has enabled numerous facilitating and positive impact on modern society and become essential for states, individuals, companies to continue their daily life, on the other hand, the complexity of cyberspace and wide range of users of cyberspace bring highly negative impacts for all parts of the society as well. These problems are mainly derived from devices used in cyberspace either as software or hardware because they are prone to have vulnerabilities. In addition, studies show that the simple mistakes of people cause most of the cyber attacks. When considering the increasing of number of devices and users, the severity of the problem appears explicitly.

Moreover, advancement in technology exceeds the capacity of states, organisations and individuals to adopt new developments about technology. As the existing rate of innovations and advancements in technology continue, predictability of their impacts on all actors has significantly been decreased (Winner, 1977, p. 13). Thus, concerns such as "the fears in which are brought by the high dependency on the ICT's" and "the technology is out of the control" have emerged. On the other hand, the "concerns about the threats of technological development to society" are not unique to modern academic literature. These discussions can be traced back to 1970s and even back to 1960s (Cavelty, 2008, p. 13). Although the negative impacts of technology on society is a long-discussed topic, to evaluate the technology of old times and new millennium's technology as the same could be misleading. The main differences between the two ages are: firstly, numbers of IoTs and their users have reached significant volumes. Secondly, in the old times, the dependency on IoTs of states, peoples, organizations and private companies has never reached such level.

Furthermore, approximately all parts of the society are begun to be affected by these difficulties regardless of either use IoTs or not. As an example of this connectivity; critical infrastructure which is a vital asset for the functioning of modern daily life, are formed from numerous complex structures. Since, with the increasing usage of IoTs and automation devices within the complex structures such as critical infrastructures, they allow having easier and more comprehensive control over infrastructures. However, this situation has a significant disadvantageous point: In the case of the problem within these complex structures, the impact would be widespread all over society. In the context of this thesis, in case of a destructive cyber-

attacks to the one of the critical infrastructures such as power grid, that cyber-attack has the capacity to affect remarkable part of the society and to create chaos among society if cyber-attacks continue enough. Therefore, as Kenneth Geers asserted that with the increasing sphere of influence of cyberspace through rising of number of IoT and ICTs, and the user of them, such issue in cyberspace are now not the only problems of computer engineers or IT employees, but it is a problem of every individual in the modern society (2011, p. 9). Thus, in addition to the technical dimension, cyberspace has got a new dimension: *Social dimension*.

With the widespread effects of cyberspace, International Relations as a social science is the forefront field that affected these developments. This impact has started to be seen at the concept of the frontline since, in cyberspace, the members of the society are directly subjected to external attacks in which passing over the state. The existence of the state is almost disappearing, and anyone in society has directly become one of the parties in the attacks. At the conventional conflicts and wars, there is always frontlines where the forces of states confront each other. In other words, in order to target the ordinary people behind the frontlines in conventional conflicts and wars, it was necessary to overcome the armed forces of the state in the frontlines at first. In this way, the people who remained behind the frontlines were relatively less directly affected by war and conflicts. However, all advancement in technology not only enlarged the scope of the war but also increased the direct impact on civilians behind the frontlines. The position of the frontlines goes back further with every technological development. With the World War 1 (WW1) and especially World War 2 (WW2), the civilians become a target of the armies through the transformation of war to *total war*. Therefore, the differences between the rear and front have been increasingly blurring. However, with the advent of the cyberspace, the difference between rear and frontline has been wholly disappeared because even it is very challenging to distinguish frontline and rear in cyberspace.

Moreover, it is also problematic to designate the borders of cyberspace. So, not only military personnel but civilians have also been started to be affected by the adversaries. Also, in the modern age, no weapon but cyber-weapons have the capacity to affect 4,3 billion people at the same time. For instance, the nuclear weapon -which is known as a most destructive weapon- even has a limited sphere of influence. However, with the sophisticated cyber-attacks, all nuclear plants of a state can be concurrently damaged and unprecedented nuclear disasters may take place. Although cyber-attacks that are targeting the nuclear plants uncommon phenomenon, consequences of possible successful cyber-attack on nuclear facilities will be

quite calamitous and challenging to be tolerated (Han & Çelikpala, 2016, p. 89). Consequently, as Eric Hobsbawm well-defined the 20th century as the “*Age of Extremes*” because the war had become a total war (1995, pp. 21-53), civilians itself became a foremost front in the cyber conflicts with the advent and quick ramification of cyber tools in the 21st century. Thus, it is not wrong to assert that there *are no fronts in cyberspace; instead whole society turns into a front in the modern age.*

During the Cold War, this can be peculiar, however, especially after the allegedly joint operation of the US and Israel to nuclear plants of Iran (it will be mentioned below as s Stuxnet attack) proved that there is a possibility to come true. Thus, with the increasing concern of within the society, the state has been urged from different parts of the society to take the necessary steps for cyber threats. For instance, a group which include leading fifty American computer engineers wrote a letter to the US president of in that period George W. Bush. In their letter, they appealed to the president to establish “*Cyber-Warfare Defense Project*” which is equivalent to cyberspace version of Manhattan Project as they underlined: “*Our nation is at grave risk of a cyber-attack that could devastate the national psyche and economy more broadly than did the September 11th attack*” (Weimann, 2005, p. 130).

In the eyes of the states, especially during the 1990s and 2000s, the worrying threat is the cyber-attacks that could create devastating results in which similar attack to Japan's Pearl Harbor attack on the United States in 1941 and the sudden attack on the World Trade Organization and the Pentagon by Al-Qaeda in 2001. Nevertheless, even though technological developments and gradually increasing cyber capacities of both state and non-state actors, it has not been observed a cyber-attack which has been feared to happen. Therefore, the comparison of cyberspace and physical world is in the line of fire by many since they believe that there is no severe direct influence of cyber-attacks on the physical world as a consequence of this development. One of the forefront scholars, Myriam Dunn, put forward that fearsome cyber-attacks which cause a significant problem to national security, did not materialize as imagined. On the contrary, the developments in the last decades demonstrated that cyber threats become the primary concern of the business sector rather than the real problem of states.

On the contrary, the developments in the last decades demonstrated that cyber threats became the primary concern of the business corporations rather than the actual problem of states. For (Cavelty, 2008, p. 3) , this situation is the result of the increasing threat perception of the policymakers. Thus, many scholars and decision makers do not give enough significance to

cyberspace since the effects of cyber-attack seem to cause secondary effects as a virtual and economic rather than direct national threats. In addition, there was a widespread belief in which if the critical infrastructures and other devices were disconnected from the internet, they were immune from the cyber-attacks and their impacts. In another saying, it was perceived that "air-gap" which refers to computers or networks that are not connected directly to the internet (Zetter, 2014) was adequate for the cybersecurity measures. However, cyber incidents like Stuxnet demonstrated that even an air-gapped critical infrastructure can be the target of the cyber-attacks that even caused a damage in physical world along with virtual world. Therefore, the Stuxnet attack can be guide us to illustrate how a computer worm can cause physical destruction and the impacts on both suspected and victim states.

In 2010, the Sergey Ulasen who came across with worm that had never been seen that kind of sophisticated, target focused and highest profile worm (Kaspersky, 2017). He revealed all details and shared with their customers and other security companies about the details of malicious code -which targeted the Industrial Control systems (ICSs) that are mainly used in the pipelines or centrifuges in the nuclear plants- with their customers and other security companies (Falliere, 2010). In respect to many features of Stuxnet, it was an unprecedented code designed to launch an attack to a specific target. Also, when it was looking for a target, it did not sabotage the computers and networks that were contaminated. So, this underlined the fact that if there is no severe anomaly, the worm can spread without being noticed by experts and security software.

After security firms informed their customers about a Stuxnet worm, Siemens, revealed that their "supervisory control and data acquisition systems" (SCADA) which serves as controller role in the pipelines and nuclear plants and so forth on, were massively targeted by Stuxnet (Anon., 2010). This development was crucial for states because SCADA system has often been unconnected to networks so as to enhance the security of that infrastructure. As a result of this development, the opinion of protecting infrastructures by disconnecting them from networks has become reversed to "infrastructures are considerably vulnerable to cyber-attacks."¹

¹ The continuation of Stuxnet is given in the footnote in order not to break the coherence: Who was the real target of Stuxnet? According to Symantec, 67, 60 percentages of affected Siemens SCADA system were located in Iran (Falliere, Murchu, & Chien, 2011, p. 6). After this statement, all attention immediately turned to Iran. At the similar time, the report of International Atomic Energy Agency published a report which indicated the process of uranium enrichment at Natanz plant had been temporarily ceased by unknown reason (IAEA, 2010, pp. 3-4). All of these news and reports push Iran to explain the situation. Initially, Iran denied the allegation of Stuxnet targeted

With cyber-attacks such as Stuxnet attack and DDoS attacks to Estonia in 2007, the perception of the threats of the first wave which are cyber-attacks could create devastating damage, became a current issue again. However, at this time, due to solid evidence about the dangers of cyberspace, security in cyberspace has turned into from low-level politics to high-level politics. Moreover, even Chris C. Demchak and Peter Dombrowski claimed that if a malicious worm can take down a whole energy system at once, for states there is no choice but to respond against new weapons to protect its citizens through own governmental and military operations (2011, p. 33). In this context, the establishment of *United States Cyber Command and the 24th Air Force* was a milestone because it was the first step by a state actor to materialize cyberspace as a military domain along with four dimensions (Libicki, 2009, p. xiii). As a result of these developments, cyberspace has rapidly evolved from mere technical and virtual field to military, political and strategic field (Geers, 2011, p. 10). In other saying, “cyberspace has become a fifth dimension in which international affairs take place after the four physical dimensions land, sea, air and space” (Kasapoğlu, 2017, p. 1).

These developments attracted IR scholars’ attention to cyberspace. Joseph Nye who was the pioneer prominent IR scholar claimed that with these developments, cyberspace became an area of competition for both state and non-state actors who aims to extend their interest and power (Nye, 2011, p. 4). In addition to Nye, Reveron (2012) and Choucri, (2012, p. 6) put forward a similar idea with Nye by underlining that “Cyberspace offers new opportunities for competition, contention, and conflict — all fundamental elements of politics and the pursuit of power and influence”. As can be seen from the three scholars, in the international relations

Iran. Although scholars like (Brown, 2011, p. 71) claimed that Iran would never accept the Stuxnet attack due to embarrassment, with the increasing evidences by security experts and increasing suspicion about the unknown reason of halting the enrichment process of uranium pushed Iran to admit to Stuxnet cyber-attack by expressing that “enemies sabotaged the uranium enrichment process by sabotaging limited numbers of centrifuges in Natanz nuclear plant” (BBC News, 2010). Moreover, Iran even accused of Siemens for cooperating with the US and Israel to launch Stuxnet cyber-attacks (Dehghan, 2011). In this way, the success of Stuxnet cyber-attack were proven.

Who was the offender of the Stuxnet? Although many scholars believe that non-state actors can also create malicious computer worms as Stuxnet, many security experts support the idea of that kind of sophisticated worm necessities enormous resources and genius experts that state can provide. In addition, when the 2005-2010 regional politics is taken into consideration, the main contested states of Iran were Israel and the US. Especially harsh criticism by two sides against the Iranian uranium enrichment progress and the possibility of kinetic attacks against the nuclear plants are considered, the allegation about the attacker is the US and Israel can be convincing. Thus, according to allegations, joint cyber operation by US and Israel targeted centrifuges of Iran’s Natanz Nuclear plant by sabotaging them to turn out of control without being noticed, which was less costly and to find offender was challenging due to attribution problem. As a result of Stuxnet, according to (Broad et al., 2011), almost one-fifth of the centrifuges within the Natanz Nuclear Plant was destroyed.

literature, cyberspace has been perceived as a new area of interest competition of states. Moreover, James Adams expresses that by beyond the area of conflict of interest defined cyberspace as a new battlefield for states (Adams, 2001, p. 98). As a result of portraying cyberspace as an area of future conflicts, states have begun to alter the conventional concepts of deterrence, power, defence, offence, war, security and so forth so on compatible with the cyberspace. So, when the state is trying to make these concepts compatible with cyberspace, how is the state trying to make itself compatible with cyberspace? While cyberspace has gradually become a part of International Relations, how the major actors of IR places itself in cyberspace?

1.3 THE PLACE OF STATE ACTOR IN THE CYBERSPACE

Due to the attribution problem, low cost of entry and to stand in cyberspace, Nye claimed that “power is diffused between state and non-state actors in cyberspace” (2010, pp. 5-6). Also, unlike the other four dimensions, states have ironically turned into the most vulnerable actors when they have developed their ICTs because of asymmetrical structures of cyberspace. The metaphor of Singer and Friedman in which “*most powerful and heaviest biggest rock-throwing actors in cyberspace live in the most precise and largest glass houses*” quietly describes this environment (2014, p. 144).

Despite all these developments and the fact that the non-state actors are relatively more powerful in cyberspace unlike the other four dimensions, the state actor will be considered as the main actor in this thesis. Since firstly it should be remembered that cyberspace does not consist of only one layer but is composed of four distinct layers. That is to say that although non-state actors take role actively in the physical, codes and content layers, state actor stands alone as a regulator layer of cyberspace. Even if there are important initiatives, which consist of very different groups of actors such as Tallinn Manual 1.0 and 2.0,² that have covered much ground in terms of writing, determination and adoption of international cyber law rules; however, *international laws and norms do not become binding without the acceptance and consent of the state*. Therefore, only the regulatory layer alone is sufficient to claim that the state is the major actor of cyberspace. There is a need to open parenthesis at this point since the position of states as a regulator signals another point: *Regulatory layer allows states to draw*

² Tallinn Manual series are the “most comprehensive guide for policy advisors and legal experts on how existing International Law applies to cyber operations.” (CCDCOE, 2017)

virtual boundaries according to its internal regulations. Secondly, the state actor has also an essential place in the first three layers. As NATO (2017) pointed out that when the economic, technical and military capacities and capabilities of the state are taken into consideration, the state is the preeminent actor of cyberspace. It is highly challenging for non-state actors to provide as many opportunities as the state presents. For instance, as demonstrated in the case of Stuxnet above, only state actors were suspected from sophisticated cyber-attacks since only they can provide an opportunity to create that kind of sophisticated cyber weapon.

Moreover, even though in the short era the diffusing of power may strengthen the power of non-state actors, in the long run, this situation may turn the state into more robust than it was. *Since states will be more aggressive and exhibit more authoritarian attitude in domestic politics to regain its absolute power within its own securitized area as the state actor had in Westphalian System.* In this way, in the long run, state actor will not only regain its absolute power but also may have unprecedented power which help states to control and rule their people more efficiently and easily. The case of Edward Snowden and the high surveillance capacity of China are two appropriate cases to support this claim³.

In addition, UN's Report on Protection of the Right to Freedom of Opinion and Expression stated that while innovations in technology have facilitated and increased the communication and freedom of expression between people, fast information sharing and enabling anonymity have provided new possibilities to the government for surveillance and intervention into individuals' private life" (Rue, 2013, p. 4). For instance, China with its 176 million surveillance cameras, (it is expected to reach 626 million until 2020) keeps watching 1.3 billion citizens across China (Grenoble, 2017). ⁴Also, a UN report stated that "states have enlarged their powers to monitor individual's communication and tried to justify these surveillances by saying that monitoring of individuals' only serves law enforcement and national security interests of states" (Rue, 2013, p. 4). For instance, to prevent the spread of "fake news", France introduced a new plan of increasing to control over the social media platforms (Serhan, 2018). That is to say, in

³ Edward Snowden who was a former expert of the CIA shared classified information with media about how American National Security Agency (NSA) surveilled extensively not only adversaries but also phones and internets of Americans and collecting of their all records to analyze (BBC News, 2014)

⁴ Also, artificial intelligence used by surveillance cameras can identify people from even walking style (Grenoble, 2017). To test its capacity, BBC reporter who tried to hide from cameras was apprehended by China's authorities within just seven minutes (para 2).

order to understand who is telling the truth and lie; French authorities have to check every account. So, *"in the name of security, states are increasing their control over the people."*

Besides, the French case draws attention to another point as well: Not only authoritarian but also many liberal democratic countries have shown increasing authoritarian characteristic in domestic politics and as a result increasing their power within their borders thanks to cyberspace. Thus, all these developments prove that mass surveillance, social media filtering and so forth on are no longer the realm of authoritarian regimes, however, it is the dangerous worldwide trend (Khazan, 2013).As Freedom House explained that freedom of people over cyberspace has been decreasing since 2012 and there is no reason to halt soon. (Freedom House, 2017).

Considering all the facts mentioned above, it can be alleged easily that the state actor is at the forefront of cyberspace. The distinct superiority of the state actor over non-state actors reveals another point: How does cyberspace used by states against another state? If the states dominate cyberspace and use all idiosyncratic features as do in the international system, how this situation affects the relations of the states? As stated in other words, how the states will take positions in the face of severe cyber-attacks from the other state actors rather than from the non-state actors in an environment where there are no boundaries, to attribute cyber-attack is very challenging, and there is an asymmetrical relation between wired and not wired one. All these developments as mentioned above-compelled states to reconsider the logic of conflict and war, and to take new measures against the possible undesired results of a new environment where the concepts of peace and war are losing their conventional meaning. Besides, when taken into consideration the low cost of entry and standing, easy access to cyber weapons and the expensiveness of providing exact and effective protection mechanism due to technical challenges and the human factor (Editorial Board of Chip, 2018, p. 86), the offensive methods in cyberspace have become more popular among states rather than providing security. In parallel to the one of the main hypotheses of neorealist school which international system has anarchic structure, has become more distinguishable in cyberspace through all these developments mentioned above. Therefore, the policymakers, security analysts and scholars have tried to give proper answer the question in which *how will state provide security in an environment in which they even do not realize the cyber-attack carried out; even if it is realized they do not understand and calculate the real impacts of cyber-attacks; even if calculated, cannot attribute the offender accurately; even if attributed, it is not known how to give response.*

This situation causes to appear as a new problematic within the IR field as it is the primary and general problematic of this thesis as well: *Deterrence Theory can be applicable to cyberspace?* Especially, with the success of nuclear deterrence theory during the Cold War which is believed that it prevents the nuclear conflict between states, the desire to achieve cyber deterrence has become popular among the scholars of IR. However, due to idiosyncratic features of cyberspace, it is perceived that in contrast to the other four dimensions, to achieve successful deterrence in cyberspace is very challenging.

1.4 THE STRUCTURE OF THE THESIS

In these respects, in this thesis, before examining the applicability of deterrence theory in cyberspace, cyber deterrence is whether necessary or not is going to be discussed. Then, assumptions, right and deficient points of both claims in which cyber deterrence is applicable and non-applicable, will be discussed with a critical view. In this way, firstly, it will try to answer *the main questions of this thesis: “Why deterrence is necessary for cyberspace? Is deterrence applicable to cyberspace?”*.

While seeking answers to these questions, the following hypotheses are tried to be developed:⁵ *Apart from the attribution problem, the severe difficulties to the achieve cyber deterrence are :* 1) *The inability of defining, writing and implementing International Law Norms that binding United Nations and the imposition of a sanction against the aggressive state;* 2) *Usage of cyberspace by spaces as new interest maximization and power projection area in addition to other dimensions.* Furthermore, cyber deterrence cannot be achieved only with cyber tools. Also, even though in the short run to exploit of cyberspace provide an advantage for states, however, in the long run, the increase of exploiting cyberspace by every state make exploiting highly disadvantageous act for states through rising damage of exploiting. In other words, the two-edged sharp sword will not only cut the hands of the victim but also the owner of the sword. *Therefore, it is asserted that in the long run, the increase abusing of cyberspace may compel states to make concessions so as to ease the undesirable impact. As a result, this process can open road to international diplomacy table.*

⁵ Although these hypotheses generally are discussed through sections, there will be other sub-hypotheses in the sections as well.

At this point, in the direction of Grotian perspective⁶, it will be asserted that *while it is not possible to provide a deterrent that completely halted all cyber-attacks; cyber deterrence is possible through international rules and norms that will reduce the excesses of cyber-attacks. That is to say that, only a hybrid model which not only consists of cyber tools, but also economic, politic, military and diplomatic channels could be applicable to achieve deterrence in cyberspace.*

In this context, in the first chapter, firstly the types of classical deterrence, their assumptions and necessary elements of it will be addressed. In this way, the general outline of the classical deterrence will try to be drawn. Then, assumptions, necessary elements of the main theory of this thesis, *cyber deterrence*, will be explained in comparison with the classical deterrence. By doing this, whether the cyber deterrence is necessary and whether it can be applicable will be addressed theoretically. Lastly, by going beyond the traditional cyber strategies, the new alternative cyber strategies that emerged with the advent of cyberspace will be addressed. In this way, it will be tried to provide a broader perspective.

In the second chapter, by eluding the theoretical perspective, the main elements of cyberspace will be discussed. In this way, firstly the cyber threats which have a major role on the securitization of cyberspace will be discussed, and cyber threats will be classified in respect of sources and agents. While sources are considered as external and internal, agents are taken as economically and politically motivated threat agents. The main emphasis about agents will be on the state and state-supported actors, and the reasons for this will be discussed in detail in this chapter. Secondly, cyber-attacks which is the materialization of cyber-threats by threat agents will be addressed according to types and effects in detail.

In the third chapter, in line with those mentioned above in the first and second chapters, the main difficulties in achieving successful deterrence in cyberspace will be discussed. In this way, it is tried to be understood what pre-condition for successful deterrence strategies are.

Also, cyber deterrence studies generally concern with how deterrence can be acquired in a theoretically. In these studies, mostly the necessary elements, the reason for failures, possible

⁶ In the international relations literature, a third perspective known as Grotian does not share the same views with Hobbesian and Kantian hypotheses. Hobbesian believes that it is not possible to go beyond the world in which we live in violence. On the other hand, the Kantians argue that it is possible to transcend violent conflicts and to move towards a more peaceful way of life. On the other hand, while Grotian thinkers acknowledge that it is challenging to halt violence and war entirely; advocates that it is possible through develop rules and norms that will reduce the extremes of violence and war. (Baylis, 2008, p. 70) In this context, the Grotian were more optimistic than the Hobbesian and more pessimistic than the Kantians. (Wight, 1979)

scenarios of cyber-attacks and so forth on are analyzed with theoretical assumption rather than the with case studies of cyber-attacks. The first three chapters of this thesis are no exception. Therefore, in the fourth chapter, the difficulties in achieving successful cyber deterrence will be tried to be addressed practically rather than theoretically. In this way, firstly, 260 cyber-attacks which are classified in six categories by date, suspect state, victim state, types of cyber-attacks, target sector and response, will be reviewed. Secondly, whether a relational link can be established between 260 cyber-attacks will be tested with statistical models. Then, in the light of the obtained results from the statistical analyses, the practicability of deterrence strategies in cyberspace will be analyzed. With categorizing, statistical analyzing and case studies; hypotheses about the main problem of cyber deterrence and the necessity of cyber deterrence will be produced to guide us to acquire “*applicable cyber deterrence*”.

In the chapter of conclusion, in the light of the four chapters, *the ideal cyber deterrence strategy* will be addressed by arguing that “*why not only cyber tools but also economic, politic, military and diplomatic tools should be employed to achieve successful deterrence in cyberspace*”. By doing all these, this thesis will hopefully reach its main goal which contributes to IR literature.

1.5 THE METHODOLOGY OF THE THESIS

In this thesis, the concept of cyberspace itself and its developments throughout history were examined by a literature review of books, articles, the reports of think tanks and international organizations. Also, to show security policies of the states; the state's official security strategies (especially the United States) were used. Moreover, the number of the Internet of Things (IoT) and Information and Communication Technologies (ICT) were analyzed by using online statistical sources. Lastly, 260 Cyber Attacks were statistically analyzed to test the theory with practice. The analysis deserves more details to be mentioned.

The number of cyber-attacks included in analysis in the fifth chapter take place in the cyberspace, perhaps in even less than a split second. However, analyzing all cyber-attacks is both technically very challenging and beyond the scope of this thesis. For this reason, the time and the actors have been limited according to focus of the thesis. In this respect, firstly, cyber-attacks were chosen between the years 2005 and 2018. There are two reasons for choosing this period: The reason why it starts with 2005 is due to the fact that cyber-attacks in the sources are generally started in 2005. The reason for ending with 2018 is that the writing of this thesis is 2019. Also, only the cyber-attacks in which state or state-sponsored are publicly suspected,

have been included in this analysis. There are four reasons for this: 1) it can be very difficult to analyze the data containing all the threat actors mentioned in chapter two. Secondly, it exceeds the scope of the thesis. Thirdly, as Kenneth Waltz pointed out, there are three levels of analysis which are human, state and system. (Waltz, 2001) Therefore, when taken into consideration of the scope of this thesis which is international relations and theory of deterrence, to take second image- state- as main level of this analyses will be more proper and useful. Last but not the least, the data of state or state-backed cyber-attacks are kept more comprehensive in the report's security companies and news.

The data to be used in this analysis were taken from many open sources. These open sources are mainly from Significant Cyber Incidents report prepared by Program Technology Policy Program within Center for Strategic Studies⁷; Security Company Kaspersky's "Targeted Cyberattack Logbook"⁸; and "Digital and Cyberspace Policy program of Council of Foreign Relations (CFR)"⁹. There should be attached particular importance to CFR because of a significant portion of the 260 cyber-attacks were taken from CFR's dataset. The main reason for this is the classification of the CFR data is more appropriate for the analysis in this thesis.

Although these three open sources constitute the vast majority of the 260 attacks discussed in the analysis, the data surpasses these sources. Especially different cybersecurity companies and the media outlets have been benefited for the categorizing responds of victim state, type of the cyber-attack and the targeted sector. Also, cyber-attacks that states have responded legally were not only satisfied with the information received from the national and international press, but also tried to be verified by official statements. In addition, many articles in the literature have been used for classification.¹⁰

However, it should be accepted that most of the used data were taken from the Western sources due to easy access to them and difficulty of accessing data of Russian, Chinese and other dominant actors' sources about cyber-attacks. Therefore, the analyses have a risk of falling into bias by prejudging usual suspects. Therefore, to decrease these bias data, the many sources were tried to be applied.

⁷See: Significant Cyber Incidents, available at <https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity>

⁸ See: Targeted Cyberattack Logbook, available at <https://apt.securelist.com/#!/threats/>

⁹ See: Digital and Cyberspace Policy Program of CFR, available at <https://www.cfr.org/programs/digital-and-cyberspace-policy-program>

¹⁰ All the cyber-attacks are listed with detailed in the appendix.

Finally, all cyber-attacks discussed here have been converted into statistical data so as to establish a meaningful relationship between 260 cyber-attacks. The data which were adapted for statistical analysis were tested by chi-square test because the Chi-Square Independence Test is based on whether the difference between observed frequencies (G) and expected frequencies (B) is statistically significant (Çilan, 2013, pp. 33-34). In addition, continuous variables specified by the measurement can be applied to Chi-Square Independence Test, which is considered to be less than or equal to a significance degree. The chi-square distribution is often used to test two independent qualitative criteria. The zero hypothesis (H0) indicates that the two criteria are independent; the research hypothesis (HA) indicates the relationship between the two criteria. The data collected in this thesis are categorical data (qualitative, relatively small). Since hypotheses will be evaluated according to whether there is a relationship between the variables, it is decided that the most suitable method is Chi-square Independence Test. By selecting variables as binary, the relationship (interdependencies) between each other was tested. The hypotheses in the study were established as follows:

H0 = Two variables are independent of each other.

H1 = Two variables are interconnected.

While mostly Chi-Square test was applied for analysis, however, since the frequency of some cases were less than 5; for those cases, "Fisher Exact Test" was applied. Because the Chi-Square statistics show the distributions approaching the Chi-Square distribution because the frequencies in the contingency tables increase as the sample size increases. When the sample size is small, tests based on exact distributions can be applied as "Fisher Exact Test". However, there is no difference between the Chi-Square test and Fisher Exact Test in terms of application and results (Çilan, 2013, p. 74).

260 cyber-attacks to be analyzed in accordance with the data obtained from these sources are classified according to the following categories:

Table 1.1: Six Classification of the Analyses

Date	Victim	Suspected State	Type of Cyber Attack	Target Sector	Response
------	--------	-----------------	----------------------	---------------	----------

Date indicates when the cyber-attack first started. Reason for choosing the beginning time as a date rather than last day of the cyber-attacks is because cyber-attacks can continue for days as

in the case of Russia's cyber-attacks on Estonia in 2017. Thus, in order to find a relation between beginning time and the reasons behind the cyber-attacks, this method is adopted. Also, to increase the accuracy of the date, many different sources such as press releases, official documents and articles in the media are reviews for that cyber-attacks.

Secondly, victim state who are subject to cyber-attacks is indicated. Although it is a problematic process to find offenders due to the attribution problem, it is less problematic to detect the victim actor than to detect the suspected actor. There is a possibility of the attacked country may not realize it has been under attack; however, the states are included in the analysis as a victim in accordance with either they have acknowledged that they have been attacked or it has been stated as victim in media or articles. Moreover, in case of the target of the cyber-attack is a private company, instead of taking the company as the victim, the country where the center of that company is indicated as a victim. For example, although JP Morgan Chase is a private company, an attack on JPMorgan Chase was included in the analysis as an attack on the United States. However, in order to prevent confusion about real target cyber-attacks, such attacks are mentioned as attacks on the private sector by creating another category, *the target sector*. Another reason to indicate the state rather than the company is because in case cyber-attacks on private companies, the tension between the two countries has been transformed into a situation in which it concerns the whole country. For example, American comedy movie "The Interview" that depicts a fictional assassination plot against Kim Jong Un who is the leader of North Korea got a heavy reaction by North Korea. Also, hacker group "Guardians of Peace" who believed in relationship with North Korean government, urged and threaten the Sony Pictures Entertainment not to release the movie. A few days ago before the official release date, Sony Pictures Entertainment were hacked by the Guardians of Peace.(Miller, 2015) However, an attack on Sony Pictures Entertainment Inc. by North Korea-supported actors was treated as an attack on the US rather than an attack on the company as it can be seen from the official statement by White House:

"We take seriously North Korea's attack that aimed to create destructive financial effects on a US company and to threaten artists and other individuals with the goal of restricting their right to free expression" (Roberts, 2015).

The sanction imposed by the US government for this cyber-attack confirms this claim (Roberts, 2015). Therefore, this classification method is adopted in this thesis.

While the cyberattacks in the sources were included in data, it was stipulated that the country to be included in the victim category should be attacked at least four times in accordance with the analysis in the sources. A country which has undergone less than four attacks is left out of the data. The reason for setting limits to include to the data is the aim of establishing a more accurate relationship between the variables. Moreover, in some cases, countries are not classified as single but are classified within the groups if they have common characteristics. For instance, Saudi Arabia and Israel are included in the analysis as two separate countries. However, there are usually joint attacks by Iran on these two countries. Since these two countries are allies of the United States and unite against Iran in the Middle East, Middle Eastern Allies of the US group was created apart from the two countries. Another classification was applied for Asian countries. In particular, the Asian Allies of the United States group was created in the East Asian region because of the military and political support of these states in the East Asian region by the US. Another group is the “European Union”. Not all countries current European Union countries are included but England, Germany, France, Italy, Netherlands, Belgium, Spain, Portugal and Austria. The post-Soviet states in Central Asia and the Caucasus which are Armenia, Azerbaijan, Georgia, Kazakhstan, Kyrgyzstan and Uzbekistan are classified as East Sphere of Russia.

Besides, if a country has less than four cyber-attacks in accordance with the analysis but can be included in any of the above groups, the country has not been taken separately within the data, but the number of cyber-attacks of that group has been increased. For instance, one cyber-attack to Estonia was carried out appropriately for the analysis, but because there are less than four cyber-attacks for Estonia, it was excluded from the first classification outside the analysis. However, since it was in line with the West Sphere of Russia group, one cyber-attack was increased for this group. By creating these groups, it is firstly aimed to test the relation between politics and cyber-attack and secondly to deepen and increase the accuracy of the analysis. In this context, the state and state groups are classified from most attacked to least attacked as the following table shows:

Table 1.2: Most Attack Countries Through Cyber Tools

NO	Victim State/ Group	Number of The Cyber Attacks	NO	Victim State/ Group	Number of The Cyber Attacks
1	United States	94	9	Japan	10
2	Asian Allies of United States	55	10	Russia	9
3	European Union	41	11	Israel	9
4	South Korea	20	12	Iran	8
5	West Sphere of Russia	15	13	China	7
6	Middle Eastern Allies of United States	15	14	India	7
7	Saudi Arabia	12	15	Turkey	6
8	Ukraine	11	16	East Sphere of Russia	4

All classification methods for victim state also adopted for category of the suspected state. However, when applying similar methods, it is encountered additional problems. The foremost reason for additional problem is mainly stemmed from the attribution problem. Since why attribution is a problematic task is mentioned in the third chapter in detail, attribution problem will not be repeated. In order to overcome the attribution problem, the following method is adopted: when the cyber-attacks are including analyses, only if the suspected actor is same actor in the press, articles, and states' official institutions; that actor is indicated as a suspected actor in the analyses by using a similar method to Rid & Buchanan, article that is titled as "*Attributing Cyber Attacks*". To set an example, even though there is no solid evidence that Israel and the US carried out Stuxnet, almost all the media and academic studies accepted that the United States and Israel were behind the Stuxnet. For this reason, Israel and United States were considered as a suspected state in the analyses for Stuxnet attack.

At this point, it should be emphasized that the suspected actor can use false flag operation to put blame another actor. ¹¹ Especially false flag operations can be applied when the attacked state has a crisis with third parties, in order to put blame third party for attacks. For instance, ISIS was first the suspected actor of the cyber-attack on the French TV5 Monde channel

¹¹ False flag is a deliberate misrepresentation, especially a covert military or political operation carried out to appear as if it was carried out by another party. (Online Oxford Dictionary, 2019)

(Campbell, 2015), however, with the increasing obtained evidence, it was revealed by studies and findings that the attack was carried out by Russian state sponsored actors (Menn & Thomas, 2015). Although there are difficulties about correctly identifying the attacker due to the attribution problem as in this example; by considering the explanations in the media, reports and official documents, it is tried to minimize the risk of attributing the wrong actor.

Table 1.3: Number of Cyber Attacks by Suspected States

No	Suspended States	Number of Cyber Attacks
1	China	114+1(China)
2	Russia	67+1(Russia)
3	North Korea	20
4	Iran	35
5	United States	17+1 (Israel)
6	Israel	5+1 (United States)

The number and country after + indicate the number of attacks carried out together with that country.

Another category included in the analysis is the target sector. Target indicates in which sector of victim country is targeted by suspected state rather than which victim country/ country group is targeted. The primary purpose of including target sector to analysis is to test whether there is a relationship between target sector, suspected state, the victim state and if deterrence can be established. According to the data that is obtained from open sources, four main targets appears as follow:

Table 1.4: Targets that Attacked by Suspected State via Cyber Tools

Private Sector	Government	Military	Civil Society
----------------	------------	----------	---------------

In cases where attacks hit multiple sectors at the same time, only the most affected place was written, However, in case of uncertainty about the comparison which sector is mostly affected, all targets were written. Nevertheless, in order to prevent the excessive number of cyber-attacks in case of multiple sectors are targeted, other sectors are written in parenthesis. For instance, if the attack targets the private sector and military, it is written as 1 Private sector + (military 1)

which means that two cyber-attacks target private sector, but one of them targets military as well. In statistical analyses, target sector is categorized as follow:

Table 1.5: Target Sectors by Cyber-Attacks

Private Sector	Government	Military	Civil Society	P+G	P+M	P+C	G+M	G+C	G+P+C ¹²
----------------	------------	----------	---------------	-----	-----	-----	-----	-----	---------------------

As a fifth category, *types of cyber-attack* is one of the essential elements for the interpretation of this analysis because the following questions are tried to be answered with classification: Is there a particularly preferred type of attack by states; is there a relationship between -type of attack, date of attacks, suspected and victim states. Therefore, it will be tried to analyze whether there is a relationship between the failure-success of deterrence and the type of attack. In this respect, the three main elements of cybersecurity which are "confidentiality, integrity and availability", are taken as cyber-attack types. Although in open sources, especially in CFR, six types of cyber-attacks which are espionage, data destruction, DDoS, doxing, defacement, sabotage are mentioned; since all of these attacks aim to damage at least one of the three elements of security, they are categorized in accordance with CIA Triad model rather than by taking six types of cyber-attacks.

Since the espionage attacks and the doxing attacks violate the confidentiality of systems and computers; DDoS attacks threaten the availability of the systems and computers; and the defacement, sabotage and data destruction threaten the integrity of the systems and computer; this classification will facilitate to obtain more accurate interpretation. In case it is necessary to go into detail about types of cyber-attacks, these three elements will be analyzed with its sub-elements as follows:

Table 1.6: Types of Cyber-Attacks

Confidentiality		Integrity		Availability	
Espionage	Doxing	DDoS	Defacement	Sabotage	Data Destruction

Response that indicates how the victim state responds against suspected actor is the last category in the analysis. The major problems of deterrence related to response can be listed as

¹² P= Private Sector; G: Government; M: Military; C: Civil Society.

inability to determine/know how to respond after the cyber-attack, the inability of judging the state-sponsored actors, and the inability to determine the suspected state due to the attribution problem. With this analysis, the cyber-attacks will be able to be discussed not only theoretically but also practically by analyzing how states should proceed after the attacks. It will also try to be given answers to questions such as how a different response is given in the context of the victim state and the suspected state, or whether there is a connection between the type of cyber-attacks and the response to those cyber-attacks. In line with the data obtained from open sources, there are four different responses as:

Table 1.7: Response by Victim State Against Suspected State

Criminal Charges	Sanction	Denouncement	Unknown
------------------	----------	--------------	---------

If there is no response publicly (at least in the media, legal channels or official statements) to the suspected state/actor after the cyber-attack, response to cyber-attacks are taken as "unknown". If the victim state imposes a sanction to suspected actors in terms of political, economic or legal, the response is taken as "sanction". If there is no decision of imposing a sanction, but the victim state takes criminal action against suspected actor, it is included in the category of criminal charges. If victim state only denounces suspected state by official means the response is taken as *denouncement*. In order to increase the accuracy of the responses in cyber-attacks discussed in the analysis; the official statement is taken as a source for criminal charges and sanction, on the other hand, a press release and official statement are taken as a source for the denouncement as well. Finally, there is always the possibility that states can also give responses through other tools in which it would never reveal publicly. Therefore, it is admitted that this situation decreases the accuracy of analysis. Nevertheless, so as to minimize that risk, the explicit cases are included in the analysis by comparing different sources.

2. FROM CLASSICAL DETERRENCE TO CYBER DETERRENCE

2.1. CLASSICAL DETERRENCE THEORY

“Deterrence is the art of producing in the mind of the enemy the fear to attack.” (Dr. Strangelove, 1964). Etymology does not only the study of discovering the meaning of words but also the art of explaining the history of the words by examining the historical, cultural processes that lead to the emergence of the words. Deterrence is no exception. Before going into details of deterrence, studying at the root of a word of deterrence can be useful to examine the deterrence in detail. The roots of the deterrence originated from the combination of "terrere" or terror, which means to frighten and "de" means away (Merriam Webster Online Dictionary, 2018). The root of the deterrence word is a good illustration of how fear is a vital component in the deterrence. Since any definition that ignores the fear, that definition ignores its original concept as it will be discussed below in detail.

The deterrence is a longstanding theory and concept which is the manipulation of cost/benefit calculation of potential action of adverse parties by causing hesitation and fear on that actor (Long, 2008, p. 7) In other words, deterrence is persuading opponent that possible risk and cost can be higher than the perceived benefit of the planned attack in the cost/benefit calculation of the actors (Mearsheimer, 2017, p. 14). Given these definitions, it can be claimed that even if the defender state does not have enough capacity to compete with offender state, but its threat is credible in the eyes of states, deterrence is successful. Thus, deterrence is certainly a psychological game between actors.

Since deterrence is a psychological game, not only fear and punishment change the idea of the opponents, but also a prize can effects the decision-making mechanism. Therefore, a reward is also an option for the defender to change an offender's idea. The concession may not be good for the defender; however, as Snyder points out, the deterrence would be successful because of the defender is persuaded to give up its idea (1961, p. 9).

Also, a defender may try to dissuade the offender from attacking by whether by fear or reward, it should be delivered to offenders. In this context, Michael McCaules who analyses the II Principe of Machiavelli who first formulated the doctrine of deterrence, claims that deterrence is a communication in which depends on possessing the military capability and the willingness

to use it (1984, p. 12). In other words, without textualization of the power or demonstration of power, it cannot be mentioned about the deterrence.

An analogy from Machiavelli about deterrence points out another point apart from communication: The ideas of the Machiavelli prove that even though deterrence is mainly linked to the Cold War period, however, historically many theorists, analysts, policy makers and decision makers have tried to re-conceptualize the deterrence by that era. Deterrence, rather than the concept that only pertains to the 20th century, is a concept that tried to dissuade the idea of the opponents through both the threat and the reward in every period of history.

States have always faced threats and wanted to deter these threats. When a new type of threat emerged, states endeavour to develop a new understanding of deterrence. From this point of view, throughout history, while military strategic and technological developments have changed the form of war, it has also led to new deterrence strategies in accordance with new types of threats. For instance, how mounted archers, inventions of cannons, application of steel and internal combustion engine on heavy armament combat vehicles, could create different types of deterrence until the 20th century; at the age of extremes, with the invention of the fighter jet and especially second-strike capacity of nuclear weapons creates a different kind of deterrence as well.

However, even though this historical process shows that deterrence strategy does not only pertain to the Cold War, still deterrence theory is considered as nuclear deterrence. According to Stephen Walt, the main reason of why the first thing that comes to mind about deterrence is nuclear deterrence is because security studies became popular with civilians engaged the military planning after the perception that "war is too serious to be left to the generals." especially with World War II (1991, pp. 213-214). Thus, he understood the 20th century as the "*The Golden Age*" of security studies. In addition, with the enormous influence of nuclear weapons in security studies, nuclear weapons can be used as political instruments in the probability of nuclear exchange (pp. 213-214). As a result, the theory of deterrence is perceived as the nuclear deterrence theory. Secondly, deterrence has taken into consideration as a "nuclear deterrence" in literature because nuclear missiles magnified the "perception of threat" not only in the eyes of the states but also an entire society by creating "*existential threat of states*". Thirdly, it not only changed the perception of threat but also the logic and structure of war have changed. The level of the destructive capacity of a new weapon can deter more powerful rivalries and allow for protection against the destructive surprising any attack. In this way, the

aim of military and political strategies “shifted from the defeating oppositions to preventing wars” as Bernard Brodie who was the American military strategies, put forwarded (Brodie, et al., 1946). Fourthly, as Austin Long asserted that with the great destruction capacity of nuclear wars makes war less possible since the cost exceeds the benefits in every case (Long, 2008, p.8). With this transformation of the structure of the security, security studies have also begun to implement these new weapons into an instrument of the policy of states (Walt, 1991, pp. 213-214).

When the historical development of deterrence theory is examined, three waves are stood out. However, this does not mean that there are three different theoretical stances, rather, this implies that policy and decision makers have adopted different strategies.¹³ Even though literature is abundant about the three waves, in this paper, Jervis’s (1979) review is taken into consideration for proper review of the literature.

With the usage of nuclear bomb on two major cities of Japan, World War II came to an end. The massive destruction capacity of atomic bombs immediately attracted interest from scholars. In 1946, the book called “*The Absolute Weapon; Atomic Power and World Order*” was written by Frederick S. Dunn, Bernard Brodie, Arnold Wolfers, Percy E. Corbett and William Fox. The main point of the book was to explain the impact of atomic weapons on military strategies and international politics and law. For instance, Dunn argues the abolishing and restricting the use of nuclear weapons; Brodie argues the impact of the atomic bombs on military and war strategies; and Wolfers analyses the role of nuclear weapons the foreign policies (Brodie, et al., 1946). Thus, this book and its authors could be referred as the initiators of the first wave of deterrence theory that came after World War II and was driven by the need to respond to a real-world problem – the invention of the atom bomb. The main implication was the analyses of the power of nuclear weapons and its usage in strategic ways.

However, the first wave analyses were lack of systemization. In the 1950s and early 60s, the second wave emerged by the systemization effort of Glenn Snyder, Bernard Brodie, Albert Wohlstetter, Thomas Schelling. In the studies of second wave analyses, there was an enhanced understanding between rational actors which led to calculate the opponent's tactics and evaluate

¹³ While the strategy of deterrence principally focuses on the specific threats, a posture of military and the varieties of communication that state accepted to deter; theory only concerns the main principles as any strategy is relied on (Morgan, 2003, p. 8). Therefore, while there can be various kind of strategies of deterrence, there is only one theory. The theory may have different interpretations and fragmentations, but the essential elements and concepts are built on the same assumptions.

the possibility of bargaining through Game Theory (Jervis, 1979, p. 291). Despite its popularity and wide range of the usage of the second wave, as the first wave, it was no free from criticisms. According to Jervis, the foremost reason for the criticisms is the lack of details about how theory changes the motivation of actors (p. 292). In other words, the second wave theorist could not explain accurately changes of intentions of actors such as how aggressive relations change into peaceful relations.

Thus, the third wave was developed so as to overcome second waves' deficiencies -such as depending heavily on deductive approaches and the lack of empirical and supporting evidence- by inclusion of bureaucratic and domestic politics, misperceptions, risks and irrational decision-making process into the deterrence theory (Lupovici, 2010, p. 707). Moreover, the third wave adopted the case-study and statistical methods to empirically test deterrence theory by challenging the rational actor assumption that was employed in second-wave deterrence theory (Knopf, 2010, p. 1). As the previous two waves have been criticized, the third wave also is not an exception.

After the end of the Cold War, some scholars believe that there is an emerging fourth wave of deterrence. For instance, Knopf believes that especially after the 11 September attacks, the perception of threat has started to change dramatically. Even if there were many studies which consider the terrorist and rogue states attacks in the Cold War Era, these papers mainly still concern interstate relations. Thus, according to Knopf, the most vital distinction from the Cold War context of the three waves is a switch of focus from symmetrical relationships to asymmetric threats (Knopf, 2010, p. 3). One can claim that during the Cold War, there were asymmetrical relations, for instance, in the Vietnam War as well. However, the security studies mainly concern the bipolar international order.

On the other hand, Amir Lupovici also claims that with the end of the Cold War, the new threats and the increasing importance of the constructivists approach led to the fourth wave of deterrence (Lupovici, 2010, p. 710). However, distinctness of Lupovici from the Knopf is that he criticizes the paradigms of realist schools and suggests that the new threats should be taken into consideration with the constructivist approaches by the learning process, identity and constitutive elements (2010, p. 721). Moreover, Tim Prior (2018, p. 68). asserts that with the change of security approach, the resilience that will be discussed below has become the headstone of security policies and denotes the fifth wave of deterrence

2.1.1. The Types of Classical Deterrence

In deterrence literature, deterrence theory itself is generally mistaken for strategy. Therefore, it is perceived as there are numerous types of deterrence. While the strategy of deterrence principally focuses on the specific threats, a posture of military and the varieties of communication that state accepted to deter; theory only concerns the main principles as any strategy is relied on (Morgan, 2003, p. 8). The theory may have different interpretations and fragmentations, but the essential elements and concepts are built on the same assumptions. Therefore, while there can be various kind of strategies of deterrence, there is only one theory. Also, it is not obligatory to adopt only one strategy in each case. While some scholars prefer to focus on the scope of deterrence, some focus on the time of deterrence.

However, when the literature is examined in detail, it is observed that there are two primary classifications of classical deterrence which are *deterrence by denial* and *deterrence by punishment* (Nye, 2017, p. 58). While deterrence by denial strategy tries to prevent undesired actions by persuading opponents of possible gain is unlikely to succeed, and the result will be costly due to strong defensive measures and capacity; deterrence by punishment refers to threats that result with retaliations such as penalties, economic sanctions, and nuclear escalation if an undesired action takes place (Mazarr, 2018, pp. 2 ; Nye, 2017, pp. 55-56).¹⁴

Suez Canal Crises is one good examples about deterrence by denial. After the Egyptian leader Jamal Nasser who nationalized the Suez Canal in 1956, the alliance formed by Israel, France and the UK carried out an operation against Egypt. However, the Soviet Union's nuclear attack threat on London and Paris, and economic sanction threat of the United States resulted in Britain and France taking a step back and withdrew from the war. When the USSR and the US involved in the conflict, the allies knew that even if they would have taken back the control of the Suez Canal, it was impossible to retain control over long time. Therefore, before any retaliation of punishment, allies decided to withdraw from the conflict. On the other hand, for deterrence by

¹⁴ In the literature there is divergency about which one of these two deterrence strategies is more reliable. There is no direct and easy answer. However, the case study of Paul Huth and Bruce Russett which analyses the interstate crises between 1885-1984 shows that deterrence by denial has more success according to the result of cases (Russett, 1988, p. 42). However, it should be noted that every case contains different elements such as the different interest, actors, technology, developments in international system and so forth on. In sum, one case cannot be applied to another case. Therefore, the history is abundant with the failure of the application of deterrence theory as seen again in the study of Huth and Russett.

punishment, the example can be given from missile strikes of the US, France and UK to a so-called arsenal of chemical weapons of the Syrian government as a response to chemical weapons attack of Syrian Government (Borger & Beaumont, 2018). Even though many warning signals by the US against Syria to stop using the chemical weapons against civilians, The US, France and UK have believed that Syrian regime ignored the warning and used chemical weapons again. Since deterrence by denial was unsuccessful, the only way to deter Syria is punishment.

In addition to these two primary deterrence strategies, scholars have not confined themselves with them. In this context, Thomas Rid (2012, p. 126) assumes that “*Firstly, deterrence can be general or specific; secondly, it can be restrictive or absolute*”. While specific deterrence is a kind of deterrence against a potential action of an actor, rather than a variety of threats and actors. In other words, *specific deterrence* underlines certain target and set of punishment. For instance, the aforementioned missiles attacks of US, UK and France against the Syrian government only aim to destroy the chemical arsenal. In *general deterrence*, there are no limitations on the set of actions or targeted country. Instead, in response to an undesired action can cause to applying of deterrence by a defender to any offender.

Secondly, *absolute deterrence* indicates total prevention of undesired action in any case. Therefore, it is often applied to threats that are quite important for national security. For example, the launch of nuclear missiles is directly posing a risk for the survival of the state. Therefore, to launch of nuclear missiles definitely be deterred. Similarly, attacks on critical infrastructures have the same importance for the national security of any state. On the other hand, *restrictive deterrence* takes places when an offender intentionally minimizes the severity of punishment by restraining the quantity or quality of offences (Rid, 2012, p. 126). In other words, as Gibbs (1968) underlined that restrictive deterrence is a curtailment of a specific type of activity during some period since in part or whole the curtailment is perceived by the state as limiting the risk that someone would be punished as a response to the activity. In this way, even if the offender will continue to its planned attack, a defender at least encourages the offenders to restrict the severity of attacks.

In addition, Morgan (1977, p. 28) focuses on the degree of urgency of deterrence and classified deterrence as “*immediate deterrence and general deterrence*”. While *general deterrence* refers to maintaining of vast military capability in response to any broad, serious attack action; *immediate deterrence* refers to the effort of preventing immediate crises. Immediate deterrence

is adopted against a situation in which conflict or war is on the verge. At this stage, the defender has to pull out the big guns in order to discourage the offender. In contrast, in general deterrence, the state draws certain red lines and plays a passive role unless thresholds are crossed.

Thirdly, Mazarr focuses on the territory of the deterrence and classified deterrence as *Extended Deterrence and Direct Deterrence* (2018, pp. 3-4). *Direct deterrence* is an effort of the state to prevent any attacks on its own territory. In fact, direct deterrence is the basic principle of every deterrence strategy; the main reason why Mazarr made this classification is the emergence of collective defense concepts such as North Atlantic Treaty Organization (NATO) and Warsaw Pact. In this direction, deterring of undesired actions on the third parties is *extended deterrence*. For instance, the desire of USSR to deter any nuclear attack on its own territory was a direct deterrence, however, to deter any unwanted action on members of Warsaw Pact was a good example of extended deterrence.

Fourthly, Glenn Snyder focuses on the scope of the deterrence by making the classification of *narrow deterrence* and *broad deterrence* (1961, pp. 9-10). *Narrow deterrence* basically implies the solely military threat against to aggression of adversaries. This type of deterrence is the first thing that comes to mind about classical deterrence. However, as one of the grand arguments in IR, implies that the cost of carrying out military action exceeds the benefits due to interdependent states in the globalized world.¹⁵ Thus, in addition to the conventional narrow deterrence, Snyder introduces new deterrence strategy: *broad deterrence* which contains not only military tools but also non-military threats such as economic sanction, discrediting by damaging the reputation of state to restrain unwelcome actions of adversaries.

¹⁵ In this context, it can be said that the economic developments in the International arena brings new type of deterrence. For instance, in the 70s, the withdrawal of US from Vietnam, the OPEC crises and the collapse of the Breton Woods Systems demonstrated that the power, especially military power was not the only asset that affects the political process in the International System. Even military weak states could possess enough influence on the international system, and the hegemon states were also vulnerable in an interdependent world. In this atmosphere, as a natural result, the critics against Realist theory were emerged. One of the prominent studies at that time was the "Power and Interdependence" by Joseph Nye and Robert Keohane (Keohane & Nye, 1977). Their main idea was that the complex and international connections thanks to technological developments or in other words the interdependencies between states creates a complex interdependence which prevent wars or decrease the possibility of conflict between states because this situation lead to rising economic and other forms of interdependence among states even though the force of military remains vital. In sum, the concept of complex interdependence is assuming that economic interdependence among states creates deterrence for states by laying the base for the liberal theory in International Relations.

Also, with the asymmetrical relations of actors such as among state and sub-state organizations to apply deterrence strategies becoming troublesome. It is because, throughout history, states had considered the rival states as a source of the threats. Therefore, the agent whom to be deterred was the only state actor in the deterrence game. However, with the increasing role of non-state actors in the international systems, especially when they challenged the states, the asymmetrical relationship has started between states and non-state actors. However, this asymmetrical relation is very complicated for states. First of all, states accustomed to establishing a deterrence dialogue between rival states not with a non-state actor. When states want to end the war, to make a deal, the state has known what to do. However, they did not know how to get into a dialogue with a suicide bomber who wanted to blow up her/himself (!). Thus, to have deterrence stance against non-state actors is very challenging. Therefore, the new types of deterrence strategies are evolving to tackle these new types of threats. The deterrence *by resilience* is one of them. The main point of resilience by deterrence is to acknowledge that there is always a security breach even if that plan and organization are excellent (Holling, 1973, p. 4). Thus, it does not focus only on vulnerabilities but adaptation, identifying and solutions for vulnerabilities by trying to mitigate 'predictably unpredictable' threats. In this way, even though the secured things get damages due to vulnerabilities, it is still functioning. So, what are the requirements for deterrence to succeed? In the next part, this question will be discussed.

2.1.2. The Core Elements of Classical Deterrence

In literature, there are different types of classification about significant elements for the deterrence theory. In this sense, Morgan's six elements are widely accepted as fundamental elements for the deterrence theory which are 1) serious conflict 2) rational actor or rationality; 3) retaliatory threat; 4) excessive damage; 5) accurate signaling of the defender's capabilities; and 6) total deterrence stability (Morgan, 2003, pp. 8-22). However, it is not satisfied with six elements in the literature. In this respect, for Freedman (2004 , p. 22) the foremost element of deterrence is defining of the offenders to understand which actors pose a threat since he believes that to signal and communicate with the offender, firstly the source of threat should be known. In addition to Freedman, Huth (1999, pp. 25-48) refers to another element apart from those mentioned here: the reputation of the actor. According to him, although the elements mentioned above are important, it is possible to predict how a state will behave in crises through its previous behaviors. Therefore, reputation is also an essential element. However, Freedman

(p.22) does not agree with the Huth because reputation can be misleading if defenders' interest is nominal from the conflict and therefore the deterrence can be unsuccessful. On the other hand, if the interest of defender is the survival from the conflict, then, deterrence would be a success. In addition, Freedman says that not only external factors influence the practicality of deterrence, but also the internal factors of state affect the decision-making behind the deterrence (p.22). In another saying, although deterrence is always perceived as an external issue, the internal dynamics of a state are also important elements for the success of deterrence. For instance, in case of reassignment of the decision makers in the government, the priorities of latter government can implement different decision than the former.

Although the basic elements that scholars give importance differ from each other, the main elements that they emphasize are the equivalent. When these elements are considered, three primary elements emerge: Credibility, Capacity and Signaling or Communication. However, in this section, instead of focusing on only three essential elements, to find a most appropriate deterrence model for cyberspace; rationality, retaliatory threat and reputation, credibility, capacity, interest, communication and signaling, and attribution-mutual learning and common understanding will be examined in order. Now, it can be started with the rationality to examine the main elements of the classical deterrence.

Rationality

Nobody is driven into war by ignorance, and no one who thinks that he will gain anything from it is deterred by fear. The truth is that the aggressor deems the advantage to be greater than the suffering, and the side [that] is attacked would sooner run any risk than suffer the smallest immediate loss . . . [W]hen there is mutual fear, men think twice before they make aggression upon one another (Thucydides, 1998).

In deterrence theory, it is assumed that the decisions are taken by the rational actors who estimate the benefits/costs of possible results of actions. To stress the importance of cost/benefit calculations, Downs asks what defines and shapes the expectation of actors if the calculation of cost/benefit does not (Downs, 1989). Also, Morgan claims that rationality is a main point of departure for the deterrence theory (Morgan, 2003, p. 11). The mentality of the rational actor model in deterrence theory relied on the level of destruction of nuclear weapons especially during the Cold War era. This means that regardless of identities, cultures and structure of the decision-making process, conducting the nuclear missile was perceived as irrational behavior.

Thus, all parties would try to avoid conducting any offence act due to possible retaliation of opponents via nuclear weapons.

For a better analysis of rationality in the deterrence theory, W. Knopf chooses to explain both strengths and weaknesses of rationality (2013, pp. 12-14). The strength of rationalism can be varied as: Firstly; rationality can be practical to avoid the stereotype against adversaries which help to decrease the risk of undermining threats that to let guard down of defense, makes the situation more manageable. As Dowding asserted that acting irrational and becoming unpredictable weaken the deterrence posture of actors. Secondly, the assumption of rationality helps to focus on strategic estimation in any conflict situation. Thirdly, the assumption of rationality can be helpful by simplifying the situation. In sum, rational actor underlines that the actors are alike each other in case of the self-interest and maximizing their interest in every situation.

The weaknesses of rationalism can be listed as: Firstly, even if decision-makers are rational, they usually do not have adequate knowledge about other parties to precisely analyze the cost/benefit estimation. Therefore, the lack of information may lead to a miscalculation and failure of deterrence as Bajema (2016, p. 2) underlined. For instance, if the Jamal Nasser would have known that the military unit of the United Nations withdraw from the buffer zone when he threatened to attack Israel, could he again do the same action? Secondly, every decision maker and every leader have different standards and value system (Payne, 2003, p. 412). In this way, the perceived rational behavior could be different in the eyes of every individual, sub-state groups or states. So, to determine which action is rational from the perspective of adversaries could be very challenging. Thirdly, Richard Ned Lebow and Janice Gross Stein (1989, p. 223) believe that itself of rationality is inadequate since domestic constraints are often neglected, and actors are assumed as always risk-prone gain maximizes as well as to identify actors as a putative challenger or defenders is challenging. In addition, Jervis claims that irrationality does not undermine the standing of theory; moreover, rationality can be neither enough nor necessary for the deterrence theory because being rational also can result with the conflict or war (Jervis, 1979). For instance, a state might be confident about the opposite party will not engage in that action because that action is not rational, on the other hand, the opponents may consider the opposite and assume that the action is the right choice. Therefore, the action that is considered as an irrational behavior can result with the successful deterrence. It is not necessarily true that being rational brings successful deterrence.

Fourthly, as the striking assumption of Daniel Kahneman underlines that decision makers do not behave as rational in their daily life because they do not strive to gather all available information to maximize expected utility. Instead of behaving in this way, actors implement the rules of thumb by categorizing the former and limited information about the adversaries (Blackwell, 2011, p. 35). Fifthly, the opponents can be so-called rogue states or terrorists who are regarded as an irrational actor.

Actually, the last fact is the proof that rationality is internalized within the deterrence theory even though there are many strengths and weaknesses of rationality. For instance, the United States started a war against Iraq since Saddam Hussein was portrayed as an irrational actor. As Mearsheimer and Walt asserted that the willingness of Saddam Hussein to employ force is the proof that Saddam is an undeterrable actor so that the deterrence would always fail (Mearsheimer & Walt, 2003). As can be seen in this example, rationality plays such an essential role in the theory of deterrence and internalized with theory so that the attack on non-rational actors can be justified. Moreover, Schelling even discussed whether U.S. leaders should adopt the irrationality and act like an insane in order to increase credibility in some cases because "there may be rationality in the irrationality." However, he concluded that leaders should substitute rationality for craziness and insanity (Schelling, 1966, pp. 38-42).

As can be seen from the above, due to many deficiencies of the concept of rationality, it has been tried to develop alternative concepts for rationality. For instance, while developing a *sensible decision-making* model that underlines "the constraints of political realities (Morgan, 1977, p. 101)", on the other hand, "*strategic culture model* (Knopf, 2013, p. 22)" mainly emphasizes the differences of all actors who make different choices due to different cultural perspective. According to strategic culture model, even if states perfectly calculate the cost-benefits, challenges, threats; in practice, states can behave differently due to limit of cognitional and social norms about oppositions that leads to "limited rationality".

Retaliatory Threat and Reputation

Another essential element is the retaliatory threat because, in deterrence theory, the primary purpose of actors is to inhibit a conflict instead of triumphing over adversaries in the conflict. The way that to deter adversaries from carrying out of undesired action is the manipulation of thinking of adversaries. In other words, between parties, there is a psychological relationship.

To manipulate the thinking process of the opponents comes by denial that preventing an attack in defensive ways, or by punishment threat that the result will be fierce if undesired action takes place. As Morgan alleged that the success of the retaliatory threat of nuclear weapon comes from the plausibility of its threat (2003, p. 14). In other words, the catastrophic threat of state that possesses nuclear capacity can be regarded notable.

In this point, Austin Long asks the right question: How a state can decide a threat whether is credible or not? (Long, 2008, p. 14) With the formulation of Schelling which distinguishing warning and threat, can help to distinguish the real intention of the state. As Schelling pointed out that while with the warning, the deterrent actor's true intention can be interpreted, on the other hand, with the threat, it is not clear what the inherent and real intention of the deterrent is (Schelling, 1960, pp. 123-124). For instance, while direct deterrence is a warning (the declaration of retaliating against any attack on the U.S territory is a warning), on the other hand, the extended deterrence (a declaration of retaliating against on the third parties) is a threat (Schelling, 1960, pp. 123-124). Therefore, according to many authors, the threat by extended deterrence creates difficulty for the delivering credible intention for the opponents (Kaufmann, 1956, p. 19; Brodie, 1958, p. 5).

The second way is what an actor did in previous resembles incidents; one can expect the same behavior for the next crises from that actor. This means that the *reputation* is another aspect for the rational actor model to predict the possible action of actors (Schelling, 1966, p. 93). However, James Blackwell (2011) claims that the reputation is not essential, however, eagerness and current perceptions of capability matters for the success or failure of deterrence. In this context, Press proposed possible ways to assess the eagerness and intention of the opponents: the analyses of "the private conversation, statements and declaration" about the perspective of actor's reasoning of policies, intention and capacity (2005, pp. 140-142). If the adversary's decisions are in favor of the hardline policy, they do not have a belief about the credibility of threats. On the contrary, if the decision makers adopt more moderate discourse in their statements, it can be said that the threat is credible.

On the other hand, how much damage would be unacceptable for the deterrer? To determine the threshold of unacceptableness is vital for creating a credible threat for adversaries because it justifies the retaliation. Also, for the successful deterrence threat, one should convince opponents as the retaliation will result in unacceptable damage to them. However, in many cases, such as in cyberspace, to determine the level and effects of attack could be very

problematic. So, if the deterrence heavily depends on psychology, then, the successful threat necessitates another central element: *Credibility*.

Credibility

The question of Soviet intentions and attendant objectives was the fundamental element of threat assessment. Soviet military forces and capabilities to carry out Soviet leaders' intentions necessarily constituted the second, but crucial element of that assessment" (Garthoff, 2003).

As per emphasized by the quotation, credibility is one of the forefront necessary conditions for the successful deterrence. Credibility is the power of being believable or convincing (Online Oxford Dictionary, 2019). In other words, the threat of deterrer should be convincing by the potential attacker as the deterrer has adequate capacity to execute the retaliation in case of an attack or solid threat. Without the convincing of opponents, in other words without credibility; the rational decisions, capacity, interest and other necessary factors (will be discussed in the following) might fail. Therefore, Patrick Morgan (2003, p. 15) claims that it is the most prominent elements for both the practice and theory of deterrence. Moreover, Daryl Press - who conducted comparative case studies over the threats of Great Britain and France before the World War, threats of US and Great Britain over the Berlin Crises and the threats of USSR during the Cuban Crises- put forwarded that the successful deterrence considerably relies on the belief of adversaries in which the deterrent actor has enough capacity to protect its crucial strategic interest in doing so (2005, pp. 140-142). This induction demonstrates that the successful practice of credibility is dependent on another two essential elements for the credibility which are *capacity* and *interest*.

Capacity

Capacity is another vital element for successful deterrence because if a state does not have sufficient military and economic; in other words, if there is no capacity to threaten opponents, then it is very tough for possessing credibility in the eyes of adversaries. Even though in the purest version of the encountering, the more powerful states or actors always be in favor of their interest without taking into consideration opposition's threats, there are other options such as allying or balancing to have deterrence posture against relatively more powerful states as in the case of Eastern European members of NATO. Also, it should be noted that sometimes the

success can come with credible bluff even the deterrent actor has not adequate capacity and other elements to deter aggressors. For instance, during the Cold War, while USSR exaggerated its capacity to increase its credibility in the 1950s, the US applied the same technics in the context of ballistic missiles during the 1980s.

Also, in some cases, the weaker actor also might defeat the more powerful actors. In addition, Toft alleged that states that possess nuclear weapons could cause terrible and destructive damage to each other via conventional weapons, however, with the end of the Cold War, they have been more worried or damaged from the weaker actors rather than by equal opponents (2001, p. 96). So, for great powers, weaker actors might create more threat than equal states in some cases due to asymmetrical relations as in the cyberspace. For instance, the US was forced to withdraw its soldiers even though it had superiority over North Vietnam. Thus, as NATO underlined that this fact illustrates that not only the military balance among states but also the *interest* of states is a crucial element for the successful deterrence (Rühle, 2015).

Interest and Reputation

Deterrence may fail if the interest of defender in achieving a specific aim is higher than the offender's aim even if there is a power gap between defender and offender. In contrary to tools of high politics such as the strategies of Schelling which are “pressure and forced persuasion”, many authors such as Quackenbush, (2011), Danilovic (2001) believe that interest is the key for the credibility for the successful deterrence. For instance, Ivan Arreguín-Toft examines how the weaker one can win the fight against a stronger one with the example of a boxing match between Muhammed Ali and George Foreman when there is a considerable power gap (Tfoft, 2001, p. 96). According to his interpretation, the answer is considerably dependent on whether a strong party has high or low interest for the conflict. Also, if the survival of the stronger party is not at stake while weaker states’ survival relies on the only victory which makes interest higher for the weaker party, the bet can be on in favor of the weaker party. In sum, when high interest is at stake, parties cannot refrain from the acting irrational, loss of soldiers and costly results. ¹⁶

¹⁶ See: Glenn H. Snyder and Paul Diesing, “*Conflict among Nations: Bargaining, Decision Making, and System Structure in International Crises*” Princeton, New Jersey, Princeton University Press, 1977, p. 190; Andrew Mack. “Why Big Nations Lose Small Wars: The Politics of Asymmetric Conflict.” *World Politics*, vol. 27, no. 2, 1975, pp. 175–200

In addition, to decide without taking into consideration the interest of rival state but its reputation from unsuccessful deterrence previous events might be misleading because defender may have different interest in previous events due to many different reasons. Therefore, to evaluate the progress and development of each incident individually is essential for accurate analysis. For example, the Falkland War between the United Kingdom and Argentina in 1982 is a good example of how only reliance on the reputation can cause damage to the reputation of a state. The fact that Leopoldo Galtieri who was general and president of Argentina at that time considered that Britain could not send troops for a small island when withdrawing its soldiers from the region. However, during those times, the UK was on the eve of the election and the Margaret Thatcher needed a support for the forthcoming election. Thus, it is not surprising that while the Leopoldo Galtieri regime was overthrown after the war, in the UK, Margaret Thatcher won the overwhelming majority of the 1983 United Kingdom general elections.

Signaling and Communication

So far, the essential elements for successful deterrence have been presented. However, if these elements do not reach to attacker from deterrer, deterrence is very difficult to succeed. At this point, another essential element emerges: Signaling and communication. As mentioned above, according to Machiavelli, deterrence is a communication which depends on possessing the military capability and the willingness to use it (McCanles, 1984, p. 11). Thus, it can be asserted that signaling and communication are one of the most prominent elements for successful deterrence because if the capacity, threat, interest and other necessary element are not delivered by deterrer; the success of deterrence can be undermined or completely fail. To achieve successful deterrence, adversaries should have information about the deterrent and should believe in the credibility of the deterrent.

In addition, what kind of message should be signaled to the other side? According to Lieberman (2013, p. 236), to deliver threats successfully, it should be costly since opponents can presume that the threat of deterrer is real and deterrer does not hesitate to carry out necessary action to prevent opponents. The primary point of this view is that sending a threat signal can only become convincing when it creates cost because if the deterrer does not want to perform the threat, it can be perceived as deterrer will be reluctant to be exposed to the financial sanctions or even in some cases loss of lives and properties. Therefore, to be convincing, the signal must contain some costs and risks that an irrational actor would not dare to (Huth, 1992).

Besides, what if opponents close all gates for the communication? For this issue, the forefront example is that deterring terrorists and rogue states because of the hardship of getting in contact with them. Moreover, even if the credible threat is explicitly signaled to sub-state groups, how states deter a man who wants to blow himself for his ideology or how to deter an actor who wants to be a target so as to enhance its legitimacy after the attack (Freedman, 2004 , p. 122). To overcome these issues, firstly the attribution, which is described as identifying actors and secondly, mutual learning and common understanding which social constructivism dwells upon, should be discussed.

Attribution-Mutual Learning and Common Understanding

One of the essential elements for the deterrence strategy for a sub-state organization is attribution. Attribution is an act of regarding something as being caused by a person or thing (Online Oxford Dictionary, 2019). Thus, it is historically one of the essential elements for both the uncovering of crimes and punishment of the offenders. Although attribution is simply a response to the question of "who did it" (Libicki, 2009, p. 41s), the statement of "it" can be everything. It is also essential because it can lead to a security weakness that could endanger the lives of thousands of people. Since the attribution constitutes the core of any form of coercion, the existence of an attribution problem does not only diminish the credibility and impact of the state's deterrence: It moves it to a much higher level: Security and liberty of the state (Rid & Buchanan, 2015, p. 4).

Even if the attribution problem has become a more visible and controversial concept with the advent of cyberspace, but it is an essential concept in every period of history. In particular, the attribution problem is one of the core elements in criminal justice throughout history. How are many attacks in history carried out by unknown assailants? The concept of the triggerman, which can be witnessed excessively, is also a problem of attribution. So, even if the assailant of an attack is caught, to find out the person who took the order of attack is essential as capturing the assailant. Besides, Rid (2013, pp. 140-141) underlined that "*attribution problem is less well explored in International Relations, where conventional state-on-state offences mostly left little doubt about the attacker's identity.*" In other words, there are no examples of the great war in which the parties of war unrevealed themselves. It cannot be wrong to assert that the attribution

problem has started to take place in IR with the concepts of terrorist attacks, guerrilla warfare and proxy war.

Moreover, the symbolic reason of The Great War, which caused the deaths of more than 16 million people, was the assassination of the heir to the throne of Austro-Hungarian by a Serbian nationalist. Was the Serbian nationalist who carried out the chain of events that initiated such a great catastrophe, did he kill the heir only according to his will and desire, or was it an order given by the Serbian state? If the perpetrators of the many cases have been attributed, perhaps many chains of events have not been experienced, and the world may have become a very different place than today. Although last statement is quite an exaggeration, it is a matter of great importance not to be ignored entirely.

Also, attribution is highly complicated for a single person or institution unless there is a talented and intelligent detective like Sherlock Holmes. In this direction, whether in cyberspace or any other field, there are at least three primary characteristics of attribution: Firstly, attribution necessities more than one individual and institutions because it is too complicated. Secondly, attribution necessities task sharing between the parties during the attribution process. Thirdly, attribution progresses gradually on different levels: From the immediate collection of technical proof, investigations and analyses with the obtained evidence to a legal process which starts with the submission of all data and analysis to the official authorities (Rid & Buchanan, 2015, p. 5).

In short, the importance of attribution stems from two factors: Strategically; accurate attribution forms basis coercive deterrence by directing retaliation to the right offender. If attribution is incorrect, this could result in new escalation and frictions or moreover the conflict (Taddeo, 2018, p. 6). Legally; defenders can justify its retaliation against the offenders (Clark & Landau, 2011). Especially in cyberspace, attribution plays major role in the success of credibility of threats as it will be discussed below.

On the other hand, in some cases, although the assailant is known, and despite the possession of crucial elements as mentioned above, deterrence may continuously frustrated. This fact highlights another essential element: Mutual learning and common understanding. When we look at political history, the Arab-Israeli conflict, which has witnessed many constant conflicts in a short period, can be a remarkable example of failure to understand deterrence. It is remarkable how did Egypt attack Israel in 1973 after devastating Six Days War in 1967 and

concluded the peace treaty in 1979? One of the most basic given explanation of this positive process as Maoz policy (2003, p. 44) asserted is Israel's nuclear policy which has led to Arab states adopting limited conflict policies instead of global war. On the other hand, the fact that nuclear weapons were built to be employed in war rather than deterrence in the early stages. Therefore, this situation brings us to another important fact which is deterrence also built on common understanding and norms between actors. As seen in the examples, even though in the form of conflict, there is a common construction of norms among the actors through continuous interaction and communication. So, it can be claimed that as Amir Lupovici stated the deterrence is a social construction and it is constructed via learning, socialization in contrast to an empirical path (2010, pp. 705-706).

The general terms of classical deterrence theory can be reviewed as above. Even though the main topic of this thesis is the cyber deterrence, however, without the knowledge of basic terms of classical deterrence, to understand the cyber deterrence accurately can be misleading. Thus, the review of deterrence theory was reviewed broadly. Now, as outlined in the introduction, with the securitization of cyberspace, the discussion of whether the theory of deterrence applicable to cyberspace will be discussed in the next section.

2.2. CYBER DETERRENCE

Before proceeding to explain and elaborate the understanding of cyber deterrence; the meaning of it must be clarified because there have been several definitions of cyber deterrence and similar concepts such as deterrence of cyber-attacks or deterrence of cyber warfare. In this thesis, cyber deterrence is concerned with the preventing cyber-attacks by aggressors and against the valued computer, networks and critical infrastructure. At this point, a small parenthesis should be opened since it is necessary to mark the distinction between cyber-attack and cyberwar. In literature, both terms are frequently applied interchangeably. Thus, the clarification of both terms will be essential to discuss more accurately the types and necessities of deterrence. Basically, in this research, cyber-attack that is intended to point the usage of malicious computer code to intervene in the functionality of a network or computer system for the political, military and strategic aim” as Kello (2013, p. 18) underlined. On the other hand, cyberwar is considered as the intentional usage of cyber-attacks by states against other states for the aim of creating damage on valued assets.

For a more general definition, cyber deterrence is the deterrence of “cyber-attacks” in which adversarial computer codes mediated actions against the critical information infrastructures and other networked national assets which includes the military and security services. The other leading conventional definition of cyber deterrence is propounded by Martin Libicki (2009, pp. 27-35) as cyber deterrence aims to enhance cybersecurity through reducing the “possible risks of cyber-attacks to an acceptable level at an acceptable cost”. Goodman (2010, p. 107) made a broader definition by identifying cyber deterrence as “like all other deterrence, it aims to dissuade opponents from the acting aggressively. Probably, Buchanan made the most general definition as stating that cyber deterrence is the art of deterring an opponent's cyber activities (2014, p. 131). James Lewis draws attention to towards another significant point: For him, these definitions have missed an essential element: “cognitive aspect” (2018, p. 40). Because, with the proliferation of Information and Communication Technologies, people have begun to communicate with each other quickly and without any intervention. Also, with the advent of social media platforms and their widespread usage by people, the control mechanism of information considerably reduced, and the manipulation of information has become prevalent. Particularly users of social media platforms have been exposed to fake news. Therefore, as Cambridge Analytica Data Crises which revealed how the company abused information of Facebook users for elections and the so-called Russian manipulation of the 2016 Presidential Election of US presidential election demonstrate that manipulation also must be called as a cyber-attack. However, there is a crucial problem for this kind of cyber-attack: Even though states want to act against manipulation news, they do not know how to create a deterrent principle.

The cognitive aspect of Lewis touches on another solid issue for cyber deterrence. In the literature, unfortunately, cyber-attacks are handled in a broad framework, which makes it seem as though there is only one type of cyber-attack. For instance, the cyber-attacks on critical infrastructure, stealing the private information of bank customers and leaking data are all considered as only similar forms of cyber-attack. However, all types of cyber-attacks have been carried out by different methods and motivations. Therefore, this situation obliges states to make actor and threats typology as it will be examined in the second chapter.

Another important issue about cyber deterrence is the scope of deterrence. Just because attacks occur in cyberspace, is it necessary to respond only with cyber tools? In this respect, Kugler

(2009, p. 328) pointed out that cyber deterrence should not only consist of cyber-attacks but also kinetic tools. He means that the United States or other nuclear capability states use nuclear deterrence strategy to deter all kinds of attacks. On the other hand, in the case of the use of a kinetic tool against a cyber-attack, the states may exceed the proportional response level. In this case, in the international arena, states may be in the line of fire and even encounter a sanction by the United Nations due to disproportionate force usage. Also, Lupovici (2016, p. 327) claims that how the usage of conventional tools to strengthen cyber deterrence, in a similar way, development of cyber deterrence enhances the general deterrence of the state as well. This means that cyber deterrence could also be employed to deter a conventional attack so as to enhance the general deterrence posture of the state. However, it should be noted that this formalization of Kugler contradicts with the “retaliation in kind” that implies the “only way to retaliate is to use same weapons” (Harknett, 1996, p. 102). After this brief introduction over cyber deterrence, it is now appropriate to examine the types of deterrence in detail.

2.2.1 Main Components and Types of Cyber Deterrence Theory

At the beginning of this chapter, the main types and necessary elements of conventional deterrence were addressed. In line with those discussions; important elements and factors, and types of cyber deterrence will be mentioned in detail in this section. One can certainly ask why the two deterrence are not examined together? The main reason for a separate examination of classical and cyber deterrence is stemmed from the inherent features of cyberspace as it will be discussed in proceeding sections. In other words, as (Libicki, 2009, p. 5) emphasized that cyber deterrence should be examined by the idiosyncrasy of cyberspace.

As in the case with classical deterrence, scholars generally reach on two main cyber deterrence strategy which are deterrence by denial and deterrence by punishment. However, since the cyberspace related security studies are increasing, types of cyber deterrence strategies have been emerging such as deterrence by resilience, active defense, defend forward and deterrence by norms. Although some of these models were used as subtypes of classical deterrence, such as deterrence by resilience; with the increasing number of studies about cyber deterrence, they have been gradually re-formulated in accord with cyberspace. In this section, unlike the classical deterrence theory section, the core elements of cyber deterrence will not be discussed

separately. Instead, the main elements are addressed in accordance with each cyber deterrence strategies in order to explain show their importance each strategy.

2.2.2 Cyber Deterrence by Denial

As Goodman (2010, p. 106) pointed out that the deterrence by denial is a defensive facet of deterrence and it aims to persuade attackers to change their decision by convincing them as its defensive systems would prevent any attacks, and as a result, aggressors gain less benefit than expected ones. Even if the attack breaches the defensive system, the aggressor would not able to reach its aim (Kugler, 2009, p. 327). In this way, it is tried to persuade offenders of launching an attack does not bring the benefit, but brings costs due to defensive capacities and measures (Goodman, 2010, p. 106). In other words, cyber deterrence by denial means that deterring an undesired cyber action by convincing adversaries as defense is credible.¹⁷ Thus, one can allege that the vital element of this strategy is to discourage the other parties rather than punish or impose sanctions. Additionally, deterrence by denial is frequently regarded as *passive deterrence* because this strategy tries to enhance internal security rather than influencing external actors by focusing on technical defense measures such as active monitoring of unusual activities in systems and networks, advanced encryption and multi-layered firewalls (Meer, 2017, p. 86).

The focus on the internal process helps to ease one of the major problems of cyber deterrence: Attribution Problem. (which will be mentioned in more detail in the second chapter). To identify the attacker is still a substantial element of deterrence by denial; however, even if attribution is not taken place, still deterrence can be implemented by the defensive measures. In addition to the attribution problem, disproportionate response against an offender may escalate the crises. If the irrelevant third party is affected from retaliation by defender due to misattribution, it brings a new problem with third parties. Thus, some scholars even claimed that denial by deterrence is more appropriate strategy than punishment for cyberspace (Ryan, 2018, p. 334 ; Arquilla & Ronfeldt, 1996, p. 94 ; Elliot, 2011, pp. 38-39).

¹⁷ One can also claim that in the broader perspective, as it will be discussed below, the cyber deterrence not only attach to cyber actions but also it helps to enhance the general deterrence posture of states. So, the part of the definition in which “deterring an undesired cyber action” might be re-organized as “deterring an undesired action”.

To claim deterrence by denial is more advantageous, initially it should be mentioned from core elements for deterrence by denial. Firstly, the mainstay of deterrence by denial is the capacity. If the defense of systems, networks and computers are not sufficient to prevent cyber-attacks which leads that attackers could relatively easily carry their actions; the offenders may believe that they will not be spotted by deterrer in the following cyber-attacks. Thus, there is a risk of being widely adopted as an idea in which there is no reason to drop the idea of attack. Secondly, James Clapper claims that unlike the conventional capacity, the assessment of cyber capacities is problematic. Since the deterrence is a psychological game and to assess the defensive capacities is challenging, this defensive capacity creates a less psychological effect on the adversaries. Therefore, when the adversaries perceive defensive capacities as insufficient, other important elements, especially credibility, are damaged as well.

Thirdly, states and especially companies, in order to prevent any possible vulnerabilities which could result with loss of physical, economic, reputational and so forth, are investing billions of dollars. These kinds of losses even might stem from unimportant vulnerabilities. From basic mistakes of people such as clicking the link of spear-phisher in spam emails, setting easily guessable passwords, using cracked software and so forth on, which create fundamental vulnerabilities of cyberspace, whole system or network might be hacked, and proper attack can be carried out against planned devices or network. For instance, Emma Woods (2019) underlined that over 90 percent of all cybersecurity vulnerabilities stem from human mistakes. As a result, all efforts of security might go down the drain. In addition, in case of a possible attack that could result in losing control of the whole system, network or computer, deliberately backdoor is placed within it.

On the other hand, it is claimed that especially with the technological developments, the rapid development of artificial intelligence (AI) field promise significant improvements in the defensive technics though its infancy era. For instance, Symantec claims that defenders will progressively rely on artificial intelligence to prevent attacks and identify the vulnerabilities. As a result, With AI, the mistakes by the individuals are considerably anticipated to decline because AI will be capable of doing outstanding rapid and comprehensive analysis than a regular security specialist (Thompson & Trilling, 2018). Thus, it offers significant advantages in the field of security as well the deterrence by denial.

However, as it has been experienced through the years, any technological invention or development has both pros and cons. While these technological developments in terms of defensive area are developing, at the same time, these methods are also using for the cyber-attacks. Thus, to have enhancement of defensive capacities can be quite economically costly which compel the state to adopt another strategy. With this general framework of denial strategy, another important and prominent deterrence strategy, retaliation/punishment can be examined.

2.2.3 Cyber Deterrence by Punishments

Cyber Deterrence by punishments/ retaliation is a strategy of last resort (Geers, 2010, p. 301). This strategy aims to prevent undesired action by threatening severe punishment (in the form of *penalties, crises escalation, severe economic sanctions, and so forth on*) that cost of retaliation will surpass the expected benefits from the cyber-activities. Therefore, this strategy is the offensive aspect of deterrence that contains “retaliation, interdependency, and counterproductivity” (Goodman, 2010, p. 106).

The deterrence by punishment has several ways of being exercised. Firstly, the deterrence by punishment as in the form of counterattacks to alter the cost-benefit calculation of potential offenders (Meer, 2017, p. 87). Secondly, even though it is assumed that to retaliate against cyber-attacks, the cyber tools should be applied due to the concept of retaliation in kind, however, as (Lupovici, 2016, p. 327) asserted, threatening or responding to the threats by adversaries via retaliation with other forms can also improve deterrence credibility and efficiency of states as mentioned above. For instance, former U.S. President of Bill Clinton declared that in response to a cyber-attack, U.S. would retaliate with also military tools that might be based on kinetic tools (Cavelty, 2008, p. 96). Until the 6th May 2019, kinetic response to cyber-attack seemed very unlikely. However, on 6th May 2019, Israel responds to a cyber-attack with an air strike on cyber-attacks of Hamas (Doffman, 2019). Although Israel has constantly been attacking the settlements of Hamas through kinetic tools, however, it is paid exclusive attention to this strike because it is the first time a state applies kinetic tools to respond a cyber-attack.

On the other hand, there are two main challenges¹⁸ to employ cyber deterrence through punishment: Attribution problem and asymmetrical relations (Geers, 2010, p. 301). Firstly, to identify an offender is quite problematic in cyberspace due to the design philosophy of the internet that gives priority to the anonymity of users. This situation creates significant obstacles for communication, which is a crucial element for the success of deterrence. If the deterrent message is not signaled, the deterrence could not be achieved in the relations between states. In the case of misattribution, as mentioned above, the crisis can escalate with an undesirable actor, and it might lead to unforeseen consequences.

Secondly, in cyberspace, all states are not dependent on Information and Communication Technologies (ICTs) at the same level. For instance, while the government institutions, private and civil sector of the United States are heavily dependent on ICTs, on the other hand, it is hard to mention for similar environment for Kazakhstan. Because of this asymmetrical structure of cyberspace, while a cyber-attack can paralyze the daily life of the United States, a cyber-attack may even not be noticed by authorities in Kazakhstan. Also, in contrast to the other four dimensions, non-state actors have more opportunity to possess cyber tools. However, as Geers (2010, p. 302) underlined that that just because non-state actors possess cyber weapons, it does not imply they have "computer network" or other "identifiable infrastructure" worth being attacked by retaliation. Therefore, asymmetry undermines a state's credibility and jeopardizes the success of deterrence by punishment. After this general framework of deterrence by punishment/retaliation, alternative deterrence strategies can be mentioned in the next sub-chapter.

2.3 ALTERNATIVE CYBER DETERRENCE STRATEGIES

In the literature, there is still no consensus over either deterrence by denial or punishment is more appropriate for cyberspace. While some scholars asserted that deterrence by denial is a more effective strategy due to attribution problem (Ryan, 2018, p. 334) the risk of escalation, low credibility of retaliation threat (Ronfeldt, 1996, p. 94), on the other hand "quick evolution of cyber tools vis-à-vis strategies and policies," (Geers, 2010, p. 300), ubiquity of ICTs, low cost of to possess cyber weapons, lack of controlling authority; make deterrence by denial also problematic. Also, even though supporters of deterrence by denial claims that the technological

¹⁸ Other major challenges will be discussed in detail in the chapter of "*The Difficulties in Implementing Classical Deterrence to Cyberspace*"

developments will considerably enhance the defense; these technological developments also assist in reaching cyber-attacks to the level of an unprecedented new scale that can cause incalculable damage on critical systems and individuals (Johnson, 2018). Moreover, it is not wrong to claim that the firstly offensive tools are developed since defensive strategies are developed according to offensive strategies. For instance, the anti-ballistic missiles are designed to counter ballistic missiles or anti-virus companies and developers design a patch when they found a new kind of vulnerabilities and cyber-weapon. Thus, (2010, p. 302) even though deterrence by punishment lack credibility due to asymmetry and attribution problem, still only real option is deterrence by punishment. However, in recent years, due to the continuing challenges of denial and punishment strategies, scholars have begun to develop new alternative strategies to enhance deterrence postures of states. In this context, *cyber deterrence by resilience*, *cyber deterrence by the active defense*, *cyber deterrence by defend forward* and *cyber deterrence by norms* will be mentioned in sequence.

2.3.1 Cyber Deterrence by Resilience

With the further development in technology such as automation of cyber-attack by artificial intelligence, the prevalence of the Internet of Things and the increasing number of users of IoTs in both ways, the threats have been turning rapidly into further sophisticated forms as mentioned above. With various complex and sophisticated threats, to provide absolute security by preventing or punishing all threats has become troublesome in the eyes of cyber actors. In other saying, in cyberspace, it is almost impractical to obtain absolute security. Also, as it will be discussed in the second chapter, most of the security issues stem from the basic human error that can result in dangerous consequences. In addition, as Salih Bıçakcı (2014) asserts that the new generation grows up with the tablets, computers and electronic devices, and playing strategy games and looking for vulnerabilities to breach the rules. The underlying point of Bıçakcı is that the new generations will have the more technical and strategic capacity to surpass the security barriers. In addition, with the problem of attribution- as it will be discussed elaborately- even in some cases, the attacker can hide its identity which creates problematizing for the application of the deterrence. In sum, the policymakers should cope with the asymmetric relations of various actors and universal networked threats in the dynamic and thorny international environment of the new millennium (Wenger & Wilner, 2012, p. 301).

So, all the combination of these illustrates that there will always be security vulnerabilities. In this point, one can rightly allege that there has never been perfect security posture of states and there have always been vulnerabilities throughout history. The second one can rightly claim that the nuclear capacity has led to a strong deterrence posture for states. The question which is “why the US could not deter the 11 September attacks even though the possession of nuclear weapons?” is the proper response for the second claims. Secondly, for the first claim, the proper answer might be that the difference between at that times and millennium age is that there have never been such connectivity and the involvement of individuals to security issues. For instance, according to Statista (2018), while the number of IoTs was 20.35 billion in 2017, with the increase of more than four times, by 2025, it is estimated to reach 75 billion. This fact is enough to prove both the rising number of users and their dependency on these devices have naturally created severe vulnerabilities.

Hence, while threats are developing, defense methods should make progress as well. In other words, threats and challenges are evolving; recipes should also keep pace with progress. When the structure of war has been changing, so the concepts of defense must progress as well (Kramer, et al., 2015, p. 1). Therefore states, organizations and other actors embark on a quest new approaches to increase their security posture: *Cyber Deterrence by Resilience*.

Tim Ridout comprehensively defines the deterrence of resilience as strategy and actions that aim to ease the possible damage at a minimal level, to provide continuation of operation process without losing function of affected computers and networks or information systems when the attack takes place (2016, p. 78). The main idea of this strategy is instead of pursuing absolute denial, to minimize the threats and risks to an acceptable level since to deter all attacks and behavior is almost impossible. Thus, with the increase of risk perception from cyberspace, the focus point is shifted from deterring than easing the possible consequences of cyber-attacks (Lasconjarias, 2017, p. 2). In this way, to implement resilience, there are two basic requirements: “*Recovery and redundancy*”. While recovery means the defense system can be saved even if it is damaged and in this way the aggressors give up to re-attack; redundancy means to prevent cyber-attacks that cause system utterly inoperable in the event of disturbances (Taipale, 2009, pp. 36-37). In addition, to successfully work of resilience, the five pillars which are “identifying, protecting, detecting, responding and recovering” successively takes place in the resilience process (Symantec, 2015, p. 1). Also, in deterrence by resilience, the “Honey-Mon strategy which the attack can be displayed in protected place by limited access to

understand capabilities of attacks. In this way, the characteristics of a cyber-weapon are attempted to be investigated and to halt the attacks which consist of the same structure in the future. For instance, according to an analysis of Kevin Townsend (2018), the Honeypot experiments demonstrate that the near future threat will be the automation of Bots that controlled by artificial intelligence.

Also, cyber deterrence has become a more complex system due to various types of cyber actors and their asymmetric relations, the challenge of noticing the vulnerabilities, the uncertain problems which are troublesome to assess, and ongoing decentralization of states. As a feature of complex systems, cyberspace is also not hierarchical, but it is composed of various interconnected sub-systems in which their relationship is unpredictable (Prior, 2018, p. 69). Therefore, any changes might lead to more nuanced and inconstant changes while it is predictable and linear for the complicated systems. For instance, to defeat sub-state organizations, state-sponsored cyber hackers are the proper illustration of complex systems. Thus, as a complex system, the resilience is remarkably necessary for cyberspace. Even Tim Prior asserts that resilience has become the headstone of security policies and denotes the fifth wave of deterrence (p. 70). Also, NATO also sees resilience as the core element of the defense of allies or in other saying collective defense (Shea, 2016). Since the globalized world requires rapid adaptation as new threats and vulnerabilities are emerged as well as increasing possession of sophisticated technologic devices of people.

Given these facts, it should not be wrong to say that deterrence by resilience focuses on internal process rather than the external factors and actors. In this way, it endeavors to overcome the problem of attribution. In some cases, deterrer might find no one behind the attack or enough evidence to blame someone for the cyber action. However, to focus on internal factors assists states to save time through only concentrating on minimizing the risks. So, in this way, a state can also have a “quick win” that all political actors wish for it (Klimburg, 2012, p. 86). The only necessary factor for the quick win is to “clean” the attacked place. However, it is not as easy as it is said to clean and obtain a quick win. It is a costly task, and in some cases the cost of cleaning or restricting the attack might extend the actual damage of the attack (p.86). In short, based on the definitions and examples, to approach cyber deterrence by resilience as a subunit of deterrence by denial is valid. So, what said in deterrence by denial about its requirements, is appropriate for resilience as well.

In conclusion, the resilience by deterrence assumes that it is not possible to completely prevent all cyber-attacks. Thus, the only way to discourage attackers is making critical infrastructures, networks and systems more resilient to cyber-attacks. In this way, the attackers might abandon the attack if it is realized that the time, money, reputation is being wasted for ineffective attempts.

2.3.2 Cyber Deterrence by Active Defense

The active defense is a proactive defense approach which implies that limited counterattacks against the aggressor to change its behavior without giving irrevocable damage. The strategy of cyber-active defense was envisaged in the 2011 U.S. Department of Defense Strategy for Operations in Cyberspace. (U.S. Department of Defense, 2011) According to a report, active cyber defense is explicated as Department of Defense's (DOD) synchronized, real-time capability to discover, detect, analyze, to mitigate vulnerabilities and threat to supplement best practices by adopting software, sensors, and intelligence to prevent malicious activities before the malicious actor's strike affect the networks and systems (U.S. Department of Defense, 2011, p. 7). Similar to the above-mentioned resilience strategy, one of the main objectives of this strategy is the continuation and prevention of disruption of the systems, networks, critical infrastructure by active defense strategies. However, the main difference is while the measure making cyber assets more resilient as asserted in resilience strategy, is considered as passive cyber defense (Gökçe, 2017, p. 121), on the other hand, as Dictionary of Secretary of Defense of United States emphasizes that active defense is to deny malicious threats and actors and to employ restricted offensive action counterattacks (U.S. Department of Defense, 2018b, p. 7). In addition, for NATO, active cyber defense is a proactive measure for detecting or obtaining information about cyber-intrusion, cyber-attack, or impending cyber operation or for determining the origin of an operation that involves launching a pre-emptive, preventive, or cyber counter-operation against the source" (Denning & Lee, 2018). As a matter of fact, this definition underlines the concepts of pre-emptive strikes or surgical strikes because one of the main underlying points of this strategy is to collect data to analyze and then if there is a suspicious action, to prevent before the launch of the cyber-attacks (Gökçe, 2017, p. 121). From this fact, as Denning and Strawser claims, cyber active defense is "derived from the concept of air and missile defense" as a "direct defensive action taken to destroy, nullify, or reduce the effectiveness of cyber threats against friendly forces and assets" (2017, pp. 193-194).

The framework, which has been so far drawn, was that cyber active defense is an offensive strategy. However, according to the active defense is defensive action since it is a reaction against detected infiltration. To reinforce this claim, they refer to a simple example:

For instance, one desires to actively respond against malicious actors who have crossed into one's borders. In this case, to send missiles into borders of someone is offense action. While to monitor missiles, which are coming into border is passive defense, on the other hand, to shot missiles down when they cross the border is active defines. For the cyberspace version of examples, while identifying and shutting down a botnet which is used so as to carry out DDoS attack is an active defense, on the other hand, to encrypt systems by making data useless in the eyes of malicious actors is passive defense (Denning & Lee, 2018).

In short, their claim is that active defense is not offensive because it is employed when there is a solid threat.

For the success of this strategy, there are two requirements¹⁹ in terms of successful, legal and ethical way (Gökçe, 2017, pp. 121-122). Firstly, the threat should be imminent which correspondences to the “instant and overwhelming” that implies that threat is on the brink of taking place. This means that the response should be necessary that implies that there are no other means to prevent threat rather than strike firstly. Secondly, the response against the threat should be proportional which means that the response should not exceed the expected results of prevented actions.

On the other hand, this strategy encounters a serious problem: Unlike the physical world, to obtain intelligence in cyberspace, states should hack the adversaries. Thus, it is quite problematic to obtain this information without launching cyber intrusion. At this point, a cybersecurity dilemma occurs as Ben Buchanan (2016, p. 5) underlined: States must launch a cyber-intrusion for their security. So, the defensive action requires an offensive action. With taken into consideration the abundance of cyber actors (they will be discussed in the next chapter in detail), the question is which actor should be hacked. Also, with the decreasing confidence to a cyber-actor, states increase their hacking activities against the possible adversaries. However, there is a situation in which there is an attack from the actor who is not

¹⁹ These requirements are originated from Caroline Affairs. See: Howard Jones, The Caroline Affair, *The Historian*, Vol. 38, No. 3 (1976), pp. 485-502

worried or even not aware of being targeted. In addition, as Buchanan pointed out that to attribute the activities of sophisticated states have been becoming more difficult (Buchanan, 2016, p. 146). Thus, this situation reduces the trust among states and even cause the escalation of the crises among them by increasing the arms race in cyberspace. For instance, harsh cyber policies have already started to be implemented by states as in the case of the that while China has adopted an active cyber strategic defense as its military doctrine, (The State Council Information Office of the People's Republic of China, 2015) the US abandoned this strategy for "defend forward doctrine" which will be discussed now.

2.3.3 Cyber Deterrence by Defend Forward

With significant economic losses of the private sector that only strives to prevent offence actions, costly cyber-attacks and the hardship of implement deterrence posture by states, new alternatives have been looked for by states. With these challenges of preventing cyber-attacks - especially below the level of conflict- before they are carried out and possessing a deterrence stance, it has suggested by many scholars that states should find new security strategies. One of these calls found its answer at Foreign Policy Magazine: The article titled "How the U.S. Can Play Cyber-Offense: Deterrence Is not Enough" by Micheal Sulmeyer²⁰ was the prominent study since most underlined requirements and wishes found a place themselves in the summary of the Department of Defense of U.S. Cyber Strategy Plan 2018 as a *concept of Defend Forward*. The primary idea of this doctrine is to disrupt or halt malicious cyber threats and activities at their sources before they reach their targets (U.S. Department of Defense, 2018b, pp. 1-2) and to punish those who prepared before attempting dangerous activities. In this respect, it will not be wrong to say that there are important similarities with active defense. However, between two strategies, there is a significant difference, which is the central premise of the defend forward: *Disrupting or halting malicious activities not only at the level of armed conflict but also below the level of armed conflict.*

Besides, this strategy also has provocative parts. For instance, there is a direct reference of malicious actors for the US. In this context, China and Russia are directly blamed as malicious actors who are threats to advantages of the US along with Iran and North Korea. Secondly, not

²⁰ See: Micheal Sulmeyer, How the U.S. Can Play Cyber-Offense Deterrence Isn't Enough, Foreign Affairs, 22.04.2018 retrieved 10.01.2019 from https://www.foreignaffairs.com/articles/world/2018-03-22/how-us-can-play-cyber-offense?cid=nlc-fa_fatoday-20180322

only malicious activities but also counter cyber campaigns which threaten the advantages of U.S. military are listed as a reason of practice of "defend forward."

Given the facts of summary of US cyber strategy 2018, it would not be wrong to claim that the necessary elements for this strategy resemble elements of active defense. In the same way, it can be deduced that the relations between these listed states and US supposedly would deteriorate in the near future if this strategy is applied. Moreover, as Lyu Jinghua who is a former colonel at Chinese People's Liberation Army and Senior fellow at Pangoal Institution, claims that this strategy will have negative impact not only on the relations between these states but also on international cyber stability because defense forward doctrine lead other states to feel anxious about their own cybersecurity after one of the most powerful cyber forces is expanding its range of operation with regard to potential adversaries, timing and geography (Jinghua, 2018). In parallel to ideas of Jinghua, Ben Buchanan and Robert Williams (2018) also believe that this doctrine deepens cybersecurity dilemma and intensifies the cyber arms race as it does in active defense strategy.

However, this strategy has great importance to understand the evolution of cyber deterrence. To understand, one can look the Cyber Strategies of US as the main source. For instance, while the previous strategy of US which was published in 2015 underlines the *active defense strategy* as discussed above, however, with the failure of active defense strategy in the eyes of US, the main doctrine has evolved as "defend forward strategy" in 2018 Cyber Strategy of US." When the date of writing process of this thesis (2018-2019) is taken into consideration, to analyze the possible effects of this strategy can be misleading for now, however, most likely, as Jinghua (2018) asserted that more adoption of proactive policies by states might require to take additional risks which could impair the stability of international systems.

2.3.4 Cyber Deterrence by Norms

The models of deterrence by punishment described so far were generally about economic, physical or diplomatic ways. On the contrary, deterrence by norms is emphasizing the importance of normative factors for cyber deterrence. Thus, as mentioned in the types of classical deterrence models, it is not wrong to claim this model is classified within the broad deterrence due to point of focus. Also, this strategy is developed based on Joseph Nye's soft power theory because it strives to create a reputational cost on the attacker's soft power and

stance on international systems as a punishment (2017, p. 60). In particular, there are some situations such as disproportionate employment of hard power, brutality, and corruption that damage the state's soft power.

In this context, this strategy is also appealing to cyber deterrence as a new alternative. Especially in some respects, it can offer important solutions to the problems experienced by others. For instance, states can reduce the potential of the escalation of crises in case of incorrect attribution. Since the main purpose is to damage the soft power of the attacker, a covert operation is not executed, and punishment tried to be carried out publicly. So, if the wrong actor is targeted, the smear campaign or the initiatives that can damage the reputation of the actor can be abandoned. However, to launch secret cyber-attacks to punish aggressors might cause undesired escalation. Probably, all the accusations would be denied by the other state; whether it is true or not, however, accused states have the opportunity to exonerate themselves by cooperating or by other means. On the contrary, if the state stays silent, it can be interpreted as acceptance of the accusations.

Also, states in the cyberspace avoid revealing how they have acquired information because explanation means the exposing techniques and capacities. In this deterrence model, generally states are unwilling to explain how they collect the information or which government organizations, institutions or private companies, are targeted. As in the case of Jamal Khashoggi, Turkey always indicates that the pieces of evidence are shared with the allies but reluctant to explain how the state acquired the video or voice record of incidents. In a similar example, both the UK and the US accused China of breach and espionage of commercial secrets of themselves. Even according to the UK James Hunt who was the former Foreign Minister of UK, the cyber campaigns of the Chinese government were the most comprehensive and significant cyber intrusions against the United Kingdom (BBC News, 2018). As these statements underline that they do not explain specifically what activities China is doing in detail or which companies are targeted, but it is an important illustration of the of placing China as an untrustworthy and norm-violator actor in the international system. Especially when the official talks are taken into consideration, which are between US and China in 2015 “to refrain from cyber theft of intellectual property for commercial gain”, China was labelled as breaking the agreements and the only way to deal with China is to apply offensive policies as it is discussed in the defend forward (Davis & Sanger, 2015). However, As Brian Barrett (2018) underlined

that the methods of naming and shaming is an increasingly popular method by the Western states against not only for China but also for Russia and North Korea.

Although deterrence by norm offers a different way than other deterrence models, it is particularly uncertain about the functionality of punishment in a normative manner. In other words, if it is accepted that China has launched all these alleged cyber activities, is the only punishment naming and shaming? Is it an effective punishment? In addition, if the revealing attacks or threats are serious, the public expects a severe retaliation. As a result, even if the state has no intention of severe retaliation, it may have to attack because of the expectation of the public opinion. If it does not take place, it reduces the credibility of that state and can seriously undermine its deterrent posture.

With these general frameworks of classical deterrence and cyber deterrence, now we can move to the second chapter to examine cyber threat with respect to sources, agents and types of cyber-attacks in detail.

3. TYPES OF CYBER THREATS AND CYBER ATTACKS

As with all other sub-security branches, it is essential to perform actor and threat analysis for cybersecurity. In particular, given the hardship of employing deterrence strategies into cyberspace, to identify and analyse the threats and actors is vital to implement the right deterrence model. Besides, as a distinction from other spaces, there is a significant problem in cyberspace: *Generalization of the threat and threat actors*. Even though it is gradually decreasing thanks to increasing attention to cyberspace from academic, state and private sectors; still cyber actors are seen only as “hacker”. No matter what kinds of attacks they carry out, no matter what technique they possess to attack, they are called “hackers” (Vidalis & Jones, 2005, p. 375). However, this simplification and generalisation cause challenges in understanding and solving the causes of problems, particularly understanding of motivation and intention of cyber agents. In addition, given the changing nature of the risk and threats in the new millennium, to identify new threats and risks, it is necessary to analyze the threats and threat agent. Therefore, in this chapter, cyber threats will be classified according to sources as well as agents and then types of cyber attacks will be examined in detail.

3.1. CYBER THREATS WITH REGARD TO SOURCES

The threat is a representation of the intention to give undesired results to adversaries. For cyber threats, a definition can be re-organized as the probability of a malicious attempt to disrupt or damage a system or computer network. According to Fenrich (2008, p. 44), threats are divided into two groups as internal and external threats in terms of the source. Although in some cases both sources can be merged; in this thesis, it will be focused on only internal and external sources.

First of all, according to the report written by Andy McCue, even though 90% of cyber security controls are mainly concerned with external threats, 70% of frauds are carried out by insiders who have authorized access to computer and systems (McCue, 2008). For instance, defenders mainly focus on the technical or physical measures such as developing detection systems and great firewalls against the external threats, (Andersen, et al., 2004, p. 8) however; in contrast to external actors, insiders can bypass all measures and can carry out attacks by her/himself or with the external actors. Also, the internal threats are significantly dangerous since an insider

can find vulnerabilities in the systems and can extend the vulnerabilities by analyzing what is more valuable.

Besides, to label an agent as an insider, the threat should be intentional. For instance, if an employee unintentionally clicks a malicious link or plug into USB and run the application that contains a trojan virus, that employee is not classified as insider even though that employee creates an internal threat. In contrast, if an employee is aware of the malicious link or other threat elements and still proceeds, that employee is called the insider. These kinds of cyber threat agents generally work in the public sector and private enterprises. Their skills can range from medium to high level with low resources, and their motivations are mainly listed as ideological, economic and personal (Bruijne, et al., 2017, p. 61).

Secondly, external threats are posed by individuals, organizations, states, environmental issues or technological issues so on and so forth. The common point of all these external threats is that they do not have authorized access to computer systems or networks (Jouinia, et al., 2014, p. 494). Also, it should be noted that even though some external threats posed by hostile intention, external threats can be unintentional threats as in the case of natural disasters such as earthquake and flood.

3.2. CYBER THREATS WITH RESPECT TO AGENTS

“Know the enemy and know yourself, you need not fear the result of a hundred battles. When you are ignorant the enemy but know yourself, your chances of winning or losing are equal. If ignorant both of your enemy and of yourself, you are certain in every battle to be in peril” (Tzu, 1963).

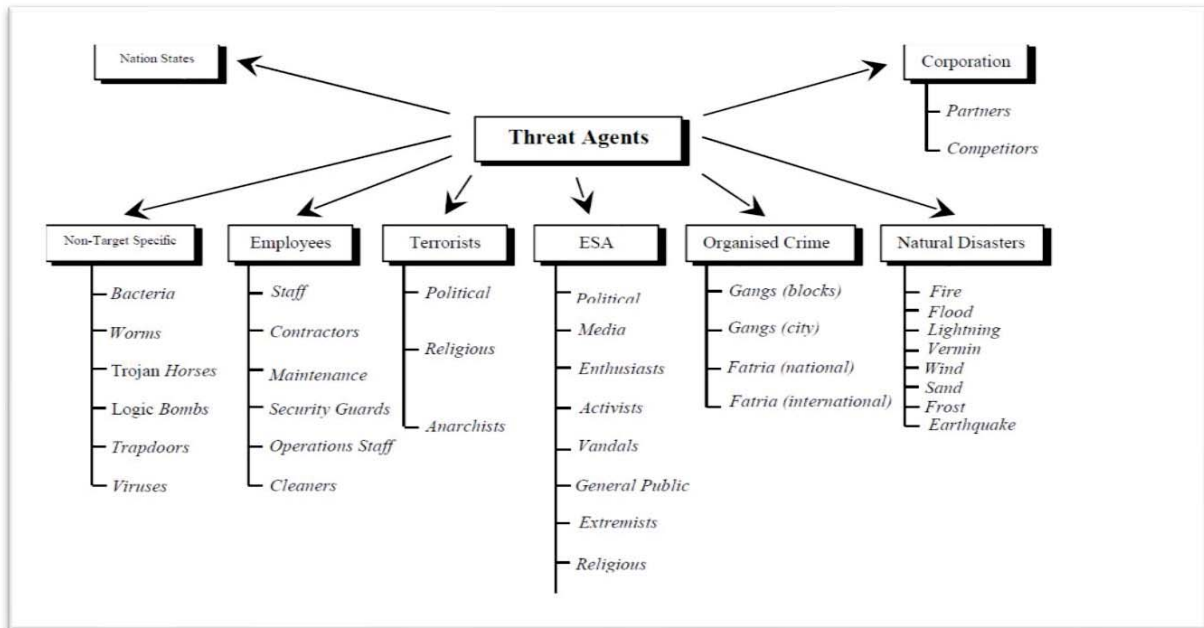
Nothing but Shakespeare’s line from the "As You Like It" explains the necessity of actor typology of the cyberspace: *"All the world is a stage, and all the men and women merely players"* (Shakespeare, 2005, p. 52). As Nicholas Ismail (2017) underlines the resemblance between the line of Shakespeare and cyberspace, in contrast to the generalization of cyber actors as hackers, each actor has their own intention, interest and different roles to perform. Also, considering rapid advancement and diversity of threats and actors who carry out those threats, there is a need for classification of actors because every actor has different capacity, object and intention. When taken into consideration the abundance of cyber actors and the importance of identifying of the enemies, there is no necessity to underline the requisite of actor analyzes for successful cyber deterrence.

In addition, human being plays a primary role in the cyberspace. Since, even though technical points such as anonymity, attribution problem and asymmetrical nature of cyberspace are the forefront challenges of cyberspace, however, in some point, it can be argued that all the roots of problems stem from the design philosophy which aims anonymity, fast information sharing and preventing government intervenes. In other words, the technical challenges of cyberspace derive from the design philosophy of human being. Moreover, unlike the assumption that cyber-attacks are carried out with developed techniques and technologies, many successful cyber-attacks are launched by most basic tactics which target the weakest point in cybersecurity: Humanity itself. For instance, most of the cyber-attacks are the result of the carelessness of people such as clicking phishing links and setting easily predictable passwords. Also, not only ordinary people but also specialists in cyber-related areas can be sold as a pig in a poke. For instance, large-scale attacks that targeted Ukraine's power grid by so-called Black Energy malware by using spear phishing attacks were successful because one employee was tricked and downloaded it from mock emails (Cerulus, 2019). As a result, the parts of the grid were destroyed.

In this topic, although there are many different types of threat agents as it can be seen below at Figure 1, threat actors who symbolize a group or an individual who executes the threat will be divided to two groups which are firstly economic cyber threat agents and secondly political cyber threat agents. Indeed, mother nature can be evaluated as a third; however, for the deterrence strategy, there can nothing to do to deter the nature but to take necessary measures. Therefore, it is content with the only emphasizing that nature also can be a threat agent for cybersecurity. Another reason for limiting the actors is stemmed from the fact that to discuss all these threat agents would be very challenging, and some actors are out of the context of this thesis. Therefore, the only actors who are the subject of direct deterrence will be discussed.

Also, a threat agent does not have to pertain only one group. It can take part in different categories according to the situations. However, since the primary goal is to draw a general framework, the actors are included in the group that they mainly take place. For example, the crime facilitator may provide support for economic activities as well as for the political activities, however, taken into consideration that they engage in economic activities in general; it is more accurate to include them within the economic threat agents.

Figure 3.1: Detailed Threat Agent Classification (Vidalis & Jones, 2005)



In sum, all these mentioned indicate that appropriate security strategies in accordance with threats and actor types help to increase chances of success of cybersecurity. But, how the analysis and classification of the threat actor for cyberspace should be? In literature, there are various classifications of cyber actors. For instance, Neil Robinson, Luke Gribbon, Veronica Horvath, and Kate Robertson compared cybersecurity strategies of countries in their book *Cyber-Security Threat Characterization from RAND Cooperation: A Rapid Comparative Analysis*. In their comparison, there are ten countries as well North Atlantic Treaty Organization (NATO), The European Union and Supranational Initiatives; however, among these countries, it can quite easily be notable that the Netherlands is a frontrunner in the context of categorizing *cyber actors*. Thus, the model of the Netherlands for categorizing cyber actors will be appealed. Secondly, in the report titled as “*Towards a new cyber threat actor typology*” by Bruijne, et al., (2017) systematically categorized the cyber threat actors in terms of intentions, capacities and objects of actors. Therefore, it is very useful for this chapter. Thirdly, Vidalis & Jones (2005) identified the cyber threat actors and calculated their capacities. In short, in this thesis, these three studies are used as reference guides to discuss threat agents.

3.2.1. Economic Threat Agents

The common point of economically motivated cyber actors is that they carry out their cyber activities with economic motivations. The threat agents of this group might be completely different from each other in terms of technical capacities, numbers, resources and objectives. However, despite these differences, it is the same motivation of the elements that bring these actors together. This group of cyber threat agents are composed of an extortionist, information brokers, crime facilitators, digital robbers, scammers and fraudsters, and crackers. Therefore, to call this group as cybercriminals would not be wrong. They mainly aim to access financial, personal or health data so as to monetize them (Ablon, 2018, p. 4). They mainly operate behind anonymous and peer-to-peer networks (for instance they use Tor Browser and OpenBazaar,) and employ encryption technologies and virtual currencies (especially Bitcoin) to cover their transactions and communications (Ablon, 2018, p. 4). In the light of this information, it can be stated that these actors do not directly threaten the national security or survival of the state but they are economically threatening to both state institutions and private companies. Nevertheless, states cannot easily deter economically motivated cyber actors because of the inherent features of cyberspace. As a result, this situation decreases not only the domestic deterrence posture but overall credibility of deterrence because how can the state, which cannot deter and prevent these cyber-attacks in their own country, deter the attacks from a rival country? When we look at who these actors are, it is encountered the following actors:

The first actor is the *extortionists* who are practicing of extorting mainly money or another important asset (Merriam-Webster Online Dictionary, 2019). In cyberspace, the extortion can be encountered in many various types, but mainly, it is encountered as someone who threatens other parties to meet her/him request (Posey, 2017). Although extortionists mainly demand money, their demands may change according to context. Their level of expertise is ranged from low to medium, and they are carrying out cyber-attacks with economic motivations. Thus, this threat actor poses a risk, especially for private companies. As Grossman (2014) underlined that extortionists generally use Distributed Denial of Service (DDoS) attack as a weapon to block access websites and demand for money to stop the attack from the company. Such attacks are increasing at an alarming level, both in terms of numbers and damage. For instance, WannaCry ransomware attack or WannaCry software that targeted Microsoft Windows by encrypting files and data of victim and demanded payments to de-encrypting files and data took place in 2017 all around the world and affected thousands of computers (Lee, 2017).

Secondly, *information brokers* or called as data brokers are mainly interested in gathering secret information and trading them (Bruijne, et al., 2017, p. 55). Information brokers mainly target the private sector, citizens and the public sector and they steal the information of credit card, social media and private emails to sell them to clientele in the dark web. Thirdly, *crime facilitators* are the organizations, groups or individuals who provide necessary technical support to actors who do not have enough skills and expertise to conduct cyber-attack but have the desire to carry out the attack. Thus, crime facilitators have high skill expertise and can give serious damage to targets. Fourthly, *digital robbers* are economically motivated actors (Bruijne, et al., 2017, p. 60) that mainly target the banks or financial organizations. Thus, they are also called as “*Bank Robber 2.0*” (Arntz, 2018). Even though major financial organizations have high-level security and to breach their security necessity plenty of time and effort, these actors have sufficient skills to orchestrate the attack. For instance, even Evans (2015) claimed that Russian digital robbers had stolen as much as 650 million pounds from British banks by spending two years to carry out an attack that is called as the largest cybercrime ever uncovered. Fifthly, as digital robbers, *scammers and fraudsters* are also carrying their cyber-attack with economic motivations. However, the difference between the two parties is social engineering. Instead of directly breach the security of banks, enterprises or individuals, they use different types of tools to deceive people since they have low and medium skill capacity (Bruijne, et al., 2017, p. 60). Last but not the least, crackers who are formed from cyber vandals and script kiddies who generally alter the pre-existing scripts and codes to carry out cyber-attack (p.60). Although crackers generally do not have the expertise, they might cause severe consequences since they might attack to make fun or harm in accordance with personal motivations. Their motivation is generally to show their skills. Therefore, their primary targets are enterprises, public sectors and rarely critical infrastructures.

3.2.2. Political Cyber Threat Agents

The actions of the actors in this group are carried out by political motivations. Their actions aim to leave the impression on decision-makers, politicians and the public through using cyberspace as a tool. When the cases of these actors are taken into consideration, even though they additionally might have social and economic motivations, it is more appropriate to include political cyber threat agents. First of all, terrorists and hacktivists will be discussed because the activities of these two actors in cyberspace can be used for each other and overlap in some

cases. After the clarification of their distinction, then itself of political, state actor will be addressed. Last but not least, state-sponsored actors who are perhaps the most prominent actors in the failure of deterrence in cyberspace will be addressed. Although it would not be improper to consider state-sponsored actors as a state actor, to admit that “they are a distinct actor” would be more appropriate because they might have different goals and interest from the state. They cooperate with the state actor mainly because they have a common interest in some cases. After this brief introduction, now, these actors can be examined in detail.

Terrorists

How with the prevailing of IoTs and increasing users of them draw attention to academics and security pundits, in the same way, the terrorists also benefit from cyberspace. As Behr, et al. (2013, p. 3) pointed out that with the information revolution, especially since the 1990s, the internet has given terrorists same ability and opportunity that it has given for the rest of society: to interact, cooperate and convince. In addition, while 11 September terrorist attacks underline the problem of asymmetric relation between state and terrorists; when we take into consideration one of the prominent structural features of cyberspace, “the asymmetric structure”, the benefit of the usage of cyberspace for a terrorist is a significant issue. Before addressing cyber terrorists, the definition of cyberterrorism is requisite. According to Denning (2001, p. 241), cyber terrorism is the conjunction of cyberspace and terrorism. This means that illegal attack or threats of attack against networks, systems, and computers to threaten or force a government or its people for social or political aims. For instance, when the cyber-attacks such as web vandalism, DDoS attacks, stealing secret information are carried out with political motivation in order to generate fear and terror in society, these cyber-attacks are regarded as cyber-terrorist attacks (Simanjuntak, et al., 2010, p. 198). In parallel to this definition, cyber terrorists are can be defined as are the socially or politically motivated nonstate actors who use cyber techniques to threaten, coerce, force a political alteration, influence an audience through causing fear or physical damage (Ablon, 2018, p. 2 ; Ahmad & Yunos, 2012, p. 209). One of the distinct features of cyber-terrorism from other threats is that the result of attack should be violent enough to create sufficient harm that causes fear in the eyes of states, individuals and organizations.

Cyber terrorists, especially in the media and movies are portrayed as detonating critical infrastructure and buildings, disrupting the daily lives with cyber-attacks; however, there has

been no cyber terror attack which is in accordance with the definition of cyberterrorism so far. Moreover, according to the report National Coordinator for Security and Counterterrorism (2018, p. 17), there are no actual terrorist attacks that have been identified in cyberspace so far. On the contrary, instead of committing violence act through cyberspace, terrorist use cyberspace as a tool to reach their aims through spreading propaganda, recruiting new members, learning to build of new kind of destructive weapons and to gather information (Behr, et al., 2013, p. 3). For instance, the control of French television network Tv5Monde and 11 other channels with their social media platforms were taken by ISIS, and threat message on Facebook was written: “*Soldiers of France, stay away from the Islamic State! You have the chance to save your families, take advantage of it*”²¹ (Chrisafis & Gibbs, 2015)

This cyber-attack was considered a terrorist attack by French Authorities (Breedon & Rubin, 2015), however, what was attributed to cyber terrorism is more related to hacktivism in this thesis as it will be discussed shortly after. As Lillian Ablon pointed out when just terrorists are active in cyberspace, it does not mean terrorists are cyberterrorists (2018, p. 2). However, just because they have not carried out yet destructive cyber-attack, it does not mean they will not. No one also expected the 9/11 terrorist attacks in the soul of the US. Also, their level of expertise can range from medium to high and they can access the great resource that makes their attack serious by ideological and political motivation. Because of these reasons, cyber terrorists should also have been taken seriously into consideration as a threat agent in cyberspace.

Hacktivists

The rules of political and cultural resistance have dramatically changed. The revolution in technology brought about by the rapid advancement of computers and video has formed a new geography of power relations in the first world that could only be envisioned as little as twenty years ago: people are reduced to data, surveillance occurs on a global scale, minds are melded to screenal reality, and an authoritarian power appears that thrives on absence. The new geography is virtual geography, and the center of political and cultural resistance must assert itself in this electronic space. (Critical Art Ensemble, 1994, p. 3)

Martin Luther appealed to the revolutionary power of the printing press to spread his messages in the 16th century; after four centuries later, Martin Luther King Jr. appealed to television to spread his messages, and with the information revolution, hacktivists are tapping into the latest

²¹ Even a short time later, another investigation suggested that the cyber-attack was actually carried out by a group of Russian hackers (Gordon Corera, 2016)

technologies to share their messages and to assist civil disobedience and protest (Singer & Friedman, 2014, p. 77). However, unlike the other technological revolutions, this technology allows the ability to operate suddenly, internationally and anonymously (p.77). In this thesis, hacktivism is basically defined as “conjoining of hacking with political activism so as to underline the perennial relations between technological structures and human agency” as Paul Taylor (2005, p. 626) put forwards. In other words, hacktivism is an individual or grassroots political protest through computer hacking or more generally, hacktivism is an activism which is gone electronic (Jordan & Paul, 2004, p. 1). The traditional forms of protests such as staging a sit-in, street demonstrations, boycotts and strikes so forth on have been reinvented in concordance with cyberspace (p.1). For instance, instead of the street demonstrations about the anti-nuclear policies, Australian activists without going to Washington DC, demonstrated their message on the screen of Department of Energy of United States of America and NASA in 1989 by the *WANK worm* which has been accepted as the first example of hacktivism (Dreyfus & Assange, 1997, pp. 14-17).

Hacktivism is politically motivated activism who demonstrated their manifesto in cyberspace. The term of hacktivist, which is the combination hacker and activism was coined in 1996 by the Omega who was the member of Cult of the Dead Cow or as known cDc Communications (Mills, 2012). In addition, even though there are distinct features of hacktivist, it is debatable that hacktivists are entirely different from hacker groups. The main reason for this claim is that hacktivists are borrowing the computer techniques from the pre-existing hackers which makes it harder to draw a line between hackers and hacktivists (Jordan & Paul, 2004, p. 2). Moreover, the hacktivists are accepted as the seven generations of hackers after chronologically 1) true hackers, 2) hardware hackers, 3) game hackers, 4) hacker/crackers, 5) micro serfs, 6) open source movement.²² Even though the hacktivists are in close relations with hackers, their differences are stemmed from their concerns and interests such as free-speech, resistance to censorships of totalitarian and authoritarian states, to assist the protest and social movements, all over the world. Actually, this underlines another important point. There is not one type of hacktivists. According to their political priority, they choose different practices. However, in

²² For more detailed information about these hackers, see: Steven Levy, *Hackers: Heroes of the Computer Revolution*, New York: Bantam Doubleday Dell, 1984; Tim Jordan and Taylor Paul, *Hacktivism and cyberwars: Rebels with a cause?*, New Fetter Lane, London: Routledge, 2004; Paul A. Taylor, *From Hackers to Hacktivists: Speed Bumps on the Global Superhighway?*; *New Media & Society*, Vol.7, No.5, pp. 625–646, 2005.

general, there are two main hacktivist groups, which are mass action hacktivists and digitally correct hacktivists.

Mass action hacktivists try to combine politics and inefficient technology to support their actions. They strive to perform the mass protest in the cyberspace along with the street protest. In other words, mass action hacktivists support street movements or political protests simultaneously to ensure the success of actions in general. For instance, during the uprisings of Arab states, many states endeavored to censor or surveil opponents during the protests. As a response, hacktivists provided necessary assistance and instructions to help protesters to express their speech freely (Goode, 2015, p. 77). Also, as an example, while the street demonstrators try to prevent a meeting of an organization, the hacktivists try to prevent the access of that organization's networks by appealing to DDoS attacks as in the case of 1999 Seattle World Trade Organizations protests. Thus, hacktivist is also called as a "cyberlibertarian entity (Golumbia, 2013, p. 13). On the other hand, digitally correct hacktivists try to ensure cyberspace as a place where information is freely and securely accessible for everyone. In this perspective, these hacktivists remain close to the hacking community; however, due to their concern about censorship of the internet and human rights, they have become distinct from the hacking community (Jordan & Paul, 2004, p. 4). Also, they protest states by revealing confidential documents to leave the state in a difficult situation in the eyes of the public. For instance, they generally target the confidential data that is more embarrassing than significant documents, and then they publish it to the world. (Singer & Friedman, 2014, p. 79)

As it was underlined, the range of actions of hacktivists varies from small individual protests- such as hacking websites and writing a message on the front page of the website- to revealing of thousands of secret government documents. The tactics of hacktivists can be diversified as defacing websites, Botnet and DDoS attacks, complicated hacking and social engineering and so forth on (Goode, 2015, p. 77). Therefore, in contrast to general public knowledge, they are not expert, and their skills and expertise can range from low to medium because they generally use existing scripts by altering them or using same scripts (Singer & Friedman, 2014, p. 79).

State Actors

The modern nation-state concept as known today was emerged with the treaties of Münster and Osnabrücke or together as known Peace of Westphalia in 1648. Also, with this treaty, not only

modern states but it also ushered in the emergence of international relations where nation-state became the dominant form of social organization (Demchak & Dombrowski, 2011, p. 37). In other words, the state turned into the Leviathan with Peace of Westphalia. While the dominance of state as an actor in the international system is obvious, however, in cyberspace state is a controversial actor in terms of power in cyberspace. Even some authors such as Joseph Nye claims that the power in cyberspace is diffusing between state and non-state actors (Nye, 2010, pp. 5-6). In particular, there are various actors in cyberspace due to prominent features of cyberspace such as asymmetric structure, the low cost of entry and the anonymity. Also, considering the role of leading private companies in cyberspace such as Google, Apple, Samsung, Huawei, IBM and Siemens and so on so forth, it might be said the dominance of state is decreased in comparison to rest of the other dimensions. However, as Nye, (2010, p. 13) acknowledged that although many dogs placed in cyberspace and their bites can hurt, states are the real dogs in the cyberspace. Non-state actors' performance can compete with the state in some cases, however; due to the limits of capacity, resource, interest, the ability of control physical domains, right to regulate international norms and use of force, the state is the considered as the most dominant actor in cyberspace.

For instance, the capacity of using kinetic tools along with cyber capacities (another actor which use kinetic weapons is terrorist) underlines the capacity of the hybridity of states that makes the state more powerful vis-a-vis rest of the other actors in cyberspace. On the other hand, this situation underlines another issue that no matter one state has great cyber capacity, if that state does not support its cyber capacity with kinetic capacity, that state might not compete for relatively more powerful states in terms of kinetic worlds. For instance, as in the case of Estonia-Russia in 2007, Estonia was more wired and developed than Russia in terms of cyber technology. However, after the so-called cyberwar between the two countries, Estonia could not give enough response to Russia due to the power gap between the two countries.²³

Another distinctive feature of state from the rest of the actors is “the right to use force” in the cyberspace. The right of using force is not only about using weapons or damaging on things that are seen by the state as a dangerous but also right of surveillance on its people. As Snowden case that former National Security Agency (NSA) of the U.S expert revealed thousands of confidential documents over mass surveillance by NSA, demonstrated that even one of the most

²³ The power gap is not the only reason. The other reason will be discussed in *chapter of “The Difficulties in Implementing Classical Deterrence to Cyberspace”*

democratic nations in the world also uses cyber espionage over its citizens. On the other hand, this case also proves that states are vulnerable to the leak of secret documents by individuals or organizations.

However, it should be admitted that the state did not directly adopt active and effective policies with the advent of cyberspace. Increasing the perception of threat and the severe impact of cyber-attacks compelled states to become more active and effective in cyberspace. As William Marmon underlined that states, awakened to the perils and awards of the cyberspace, have started to mobilize their resources and powers to pursue the "politics by other means" as Clausewitz defined war, in the domain of cyber warfare (Marmon, 2018). In addition to these developments, with the establishment of U.S. Cyber Command that depended to 24th Air force made a breakthrough by making cyberspace as a for the first-time military domain in addition to domains of air, land, space and sea in the eyes of states (Libicki, 2009, p. xiii). However, until Stuxnet, the severity of cyber-attacks was not clear, and every state did not believe the possibility that cyber-attacks led to severe damage. After Stuxnet, which proved malicious worms could give physical damage even without an internet connection, perception of states about the threats and vulnerabilities were dramatically altered. Therefore, according to Demchak & Dombrowski (2011, p. 35), Stuxnet indicates the official beginning of a new cyber Westphalian world of virtual boundaries. This means that with the Stuxnet attack, states which aim to protect their citizens from the threats that come from cyberspace started to build national virtual fences. So, states have been compelled to become the most dominant actor in cyberspace.

Lastly, unlike the other actors mentioned above, the state has a different task than other actors along with private companies: Responsibility to its people. Even though many critical infrastructures are under the control of private companies, in the eyes of people, the continuous distribution of service is assumed as a task of states, not the private sector. Being aware of this responsibility, the state plays a vital role in the preservation of the stability of critical infrastructures which are very important for the continuation of daily life. However, the increasing number of new threats and vulnerabilities and their changing and evolving nature in critical infrastructures lay the extra burden on the state and force states to take a role an active and effective role in cyberspace (Schreier, 2015, p. 41). In conclusion, even though there are abundance of essential actors in cyberspace, due to mentioned reasons above, the state comes to the fore in this thesis along with the state-sponsored actors who will be discussed below.

State Sponsored Actors

The seas around the world are, much like the cyber domain, not governed by one single nation. We have created maritime norms and have to do the same in the cyberspace to ensure a flow of information and ideas (Rogers, 2015).

With the development of shipping techniques, the states wished to take an active role in the high seas and oceans. However, due to many challenges, states agreed with the pirates instead of sending their own troops directly to tackle the challenges. While states are securing their fleets and trade ships by sharing a certain amount of spoils with pirates, they were also discovering new places and searching the boundaries of the oceans and high seas. Also, whilst states were assisting pirates in terms of technical and material aspects, they were utilizing the skills and experiences of pirates in the areas where it was dangerous to deploy the navy. Therefore, in some cases, skilled pirates were recruited to enhance the capacity and capability of the national navy of state. For instance, Barbaros Kheireddin Pasha who was the grand admiral of the Ottoman Fleet was one of the most famous and successful privateers in the Mediterranean Sea in the 16th century. After the conquest of Egypt by the Ottoman Empire, he sought out the assistance of the Ottoman Empire to recruit sailors in Anatolia and secure cannon and gunpowder to enhance his fleet. In return, he offered annexing of Algeria to Ottomans and recognition as its governor (Shaw & Shaw, 1976, p. 95). From the earliest times to 19th century, although all nations were carried out this practice which called as privateering, particularly Britain and then France and USA actively collaborated with privateer who is person or ship which commissioned by a belligerent state to attack enemy ships (Encyclopaedia Britannica, 2018). Privateers aimed to explore, proselytize, and conquer new territories for the states that they were in relations (Kennedy, 2004, p. 38). For instance, English authorities and merchandisers appealed the experiences and skills of the privateers so as to increase the defensive capacity of Britain (p.38). Hence, while they were being recruited by the great merchandisers so as to secure the safety for merchandisers' ships during the travel in the offshores, privateers were employed by states in the national wars to cause damage fleet of enemy nations as well. For instance, privateers took an active role during the Anglo-Spanish War. Moreover, with the relations of Anglo-Spanish was deteriorating, Elizabeth I went further and authorized a branch of privateers- called the Sea Dogs- in order to reduce the size of Spanish Navy through attacking and looting Spanish fleets (Rasor, 2004, p. 247).

Giving the brief information about privateering, Halvar Flake underlines that there is a resemblance between the developments of navies in the 16th and 17th centuries and development of the cyber community in the 1990s and 2000s (Flake, 2013). Moreover, there is an also analogy between privateers and state-sponsored actors who undertake the similar roles of privateers in modern cybered world. Even, after the cyber-attacks against Estonia in 2007, the Estonian Defense Minister made an analogy between privateering and state-sponsored cyber actors by suggesting that similar norms of the maritime were necessary in cyberspace as in the case of 1865 Declaration Respecting Maritime Law that abolished privateering:

Firstly, the analogy provides an insight into the relationships of the system in which lines between state-sponsored and state actors are blurred. Secondly, this analogy indicates that the political and economic areas are not separated. Therefore, it underlines peacetime challenges of cyberspace- cyber-enabled commercial espionage and cybercrime. Last but not least, this analogy enhances the understanding of security dynamics in a system in which capabilities are diffused amid several actors (Egloff, 2017, p. 232).

State-sponsored actors are one of the most active and effective actors in cyberspace because they are employed by the state or companies that have relationships with state officials due to their high skill expertise. Even though they can be classified as a semi-state actor or non-state actor partially, they deserve the additional attention because they have sufficient capacity and resource to specialize in launching cyber-attacks thanks to assists from states. Also, the employment of these actors is being carried out carefully by states according to states' current interest. Thus, state-sponsored actors take various directions to enhance state's particular interest such as to degrade, disrupt, deny, destroy computing systems through technical assistance and funding from a state (Ablon, 2018, p. 3).

How the Britain and France were using privateers in 17th and 18th centuries, according to Charles Hymas (2018), China is the country which carried out most significant state-sponsored cyber-attack that is mostly stealing commercial secrets against Western World along with Russia. Although it is a very low probability, in some cases, state-sponsored actors employ detrimental strategies that cause several damages in the direction of interests of the state so as to prevent the possible retaliation or vicious reputation of states. In this way, while the desired

attack is carried out, states also have the opportunity to pass the buck to state-sponsored actors in case of the disclosure of the attacks.²⁴

Although states currently employ state-sponsored actors, as there are always two sides of a coin, there are the disadvantages of a state-sponsored actors as well. Firstly, even though state-sponsored actors act in accordance with the directions of the states, the state may not be able to control these actors entirely in every situation. While they are carrying out strategies in line with the plan of the state, the collision of interest between state and state-sponsored actor might occur. Secondly, even they may defect during the operation if the advantages outweigh the disadvantages such as staying loyal. Thirdly, in some cases, during the operation, they can seize valuable information but can hide from the state so as to sell for money at the black market. Fourthly, the planned action of state via state-sponsored actor for the political message may exceed the given restriction, and it could lead to a riskier process through getting state into a scrape. Fifthly, as a result of increasing disadvantageous role of state-sponsored actors, the state may impose penalties on these actors. However, this policy has a severe risk since these actors could leak all the details about the plan of the state in return. Therefore, unless their activities cause significant damages and decrease the possible interest of the state, states generally have to overlook their activities which exceed the planned level of attack. Sixthly, the state might attempt to define legal norms of cyberspace that to pave the way for more certain boundaries of cyberspace as will be discussed in the following sections. As a result, the state may completely dissolve the state-sponsored actors and may try to assign these actors in the security units. However, they might object to take place within the official security units and demonstrate an uncompromising attitude for new rules. This seems to be particularly painful for states because as in the case of privateers, when states tried to limit the activities privateers, most of them did not recognize the rules and acted by themselves.

Moreover, Privateering was adopted as a policy of the challengers, not the great powers. For instance, when Great Britain had become the dominant naval and trading power, the United States and France heavily relied on Privateering. Thus, the British were so eager to see privateering to be banned (Lemnitzer, 2014, p. 63). As England's PM Henry John Temple or known as Lord Palmerston in 1865, pointed out that:

²⁴ For instance, Russia blamed the patriotic hackers for the famous Estonia cyber-attacks (Leyden, 2009).

Privateering is a practice most inconvenient to the Power which has the largest number of merchantmen at sea, and the least useful to the Power which has the largest war navy. England is that Power and we should therefore willingly agree to abolish that Practice regarding all Powers which would enter into the same Engagement towards us (Lemnitzer, 2014, p. 64)

As a result, modern nation states can make similar decisions for state sponsors actors as the 1865 Declaration Respecting Maritime Law abolished privateers. Although it is a time when state-sponsored actors are actively and intensively deployed similar to the 18th century, there is no reason why similar agreement in the future should not be made for state-sponsored actors. For all these reasons, although there are many deficient elements in comparing cyberspace and ocean; privateers and state-sponsored actors; and today's environment and 17th century's policies, it is still a useful analogy since at least it helps the increase understanding the relations between states and non/semi- state actors. After this general framework of the both economically and politically motivated threat actors, the materialization of their threats- cyber-attacks- can be examined.

3.3. CYBER ATTACKS

One of the main problems with the security of cyberspace is the use of the concept of cyber-attack as very inclusive. It is defined as the cyber-attack varies from creating physically damage of the country's critical infrastructures to stealing the country's trade secrets; from the internet fraud to changing the home page of a websites, from manipulation of Facebook users to stealing the customer information of banks or stealing prototype of weapons and so on so forth. However, this general usage of cyber-attacks definition can cause the misconception about cyber-attacks so that all cyber-attacks are similar in terms of motivation, technique, resources. Just because activities take place in the cyberspace, it does not necessarily assume all cyber-attacks are in the same category. As Singer & Friedman (2014, p. 68) asserted that to assume all cyber-attacks are in the same category is alike to treat the actions of a joker with fireworks, a bank robber with a rifle, a guerrilla with a roadside bomb, and a state with a cruise missile as if they were all the identical phenomenon since all included the same chemistry of gunpowder. Moreover, states also use different types of cyber-attack definition, which decreases the chance of states to meet at the common ground to create international norms about cyberspace. For instance, China even considers the spreading of rumors as a cyber-attack (Li, 2015, p. 193). Therefore, firstly, the concept of cyber-attack will be defined. Secondly, to comprehend the

cyber-attacks, the similarities and differences with the kinetic attacks will be explained. Lastly, it will be discussed how to classify cyber-attacks to improve cyber deterrence strategies better.

3.3.1. The Concepts of Cyber Attack

If there is information, or if there is a computer running the infrastructure, there is a certain number of usernames and passwords that everyone can access to the ongoing data flowing within that network. Given this fact, Bıçakcı (2018) defines cyber-attacks as someone who does not have user right to the data within the computer network, wants to access and to try to disrupt the integrity of data or to add information that is not there is called a cyber-attack. In addition, Akin Ünver (2018) defines cyber-attack as “all digital and physical attacks on computers, information and digital networks of a country are called cyber-attacks”. As he underlined that cyber-attacks are not the attacks that took place only in computers but also in the physical environment. Even though a cyber-attack aims to target the digital place, the attack can take place digital or physical. Two scholars give an example of the Stuxnet to explain the concept of cyber-attacks. While the reason for using Stuxnet example by Bıçakcı is to illustrate the discovery of cyber-attack related to irregularity and anomaly, and Stuxnet was realized too late because of irregularity and anomaly is very low, and in some cases, there is a risk of not being noticed, Ünver refers to the Stuxnet case to indicate that physicality comes to the forefront in attacks that target the systems which are not connected to the Internet, as in the example in Stuxnet. In addition to these two scholars, Singer & Friedman (2014, p. 68) underlined that to comprehend what a cyber-attack is, firstly cyberattacks should be distinguished from conventional attacks. In this direction, the primary differences between the cyber-attack and the conventional attack can be listed as a source, speed, impact, soldiers, cost, weapons, technology need, signs of an attack and damage assessment (Çiftçi, 2017, p. 23). Examining all the given differences in detail here may digress from the subject, but never mentioning them may make the subject unclear. Therefore, the most proper option seems to make an overall assessment of these differences.

Fundamentally, cyber-attacks use digital means instead of kinetic force. This difference creates a fundamental distinction since cyberattack is not restrained to the physics of kinetic attacks. Therefore, while a kinetic attack is directed to a single target, there is the possibility of attacking to more than one target simultaneously in the cyberspace. Secondly, the target of kinetic

weapons is a specific actor and the damage can be inflicted to that actor, on the other hand, even though cyber weapon may design to attack specific actor as in the case of Stuxnet, with that cyber-attacks, many independent actors can be affected. For instance, in an air strike, without vital coordination or system failure, the strike is unintentionally hit another target. In addition, the damage of air strike can be estimated with a few mistakes. (It is the exception that the exact number of civilians might be so different from the expectation.) However, in the cyber-attack, it is difficult to know what the impacts of cyber weapons are. Even though the cyber-attack is designed for a specific target, it can spread to another computer or systems. For instance, although Stuxnet had a specific target which programmable logic controllers (PLCs) of centrifuges were placed at Natanz Nuclear facility in Iran, however, according to report of anti-virus software company- Symantec- about Stuxnet, there were close to 100,000 affected hosts, and only %58 percentage hosted in Iran. Rest of them were spread range from Indonesia (%17, 83), to India (%9, 96) (Falliere, et al., 2011, pp. 5-6). After these general reviews about the distinctions between cyber weapons and kinetic weapons, now we can pass to the main issue: How can these cyber-attacks be classified?

In fact, the definition of the concept of cyber-attack by Bıçakcı gives an important clue about the answer because his definition fundamentally underlines the three elements which are “*confidentiality, integrity and availability*” that are the cornerstones of the CIA Triad model. As Shon Harris who is computer security consultant underlines that all security mechanism, controls and safeguards are implemented to provide at least one or more of these elements. Thus, threats and risks are measured for their potential capability to endanger one or all of the CIA principles (2013, p. 22). Although there are cyber-attacks with a large number of different techniques and capacities such as espionage, data destruction, DDoS, doxing, defacement, sabotage; fundamentally, cyber-attacks are carried out in parallel to these three elements. For instance, since the espionage attacks and the doxing attacks violate the confidentiality of systems and computers; DDoS attacks threaten the availability of the systems and computers; and the defacement, sabotage and data destruction threaten the integrity of the systems and computer; this classification will facilitate to obtain a more accurate classification.²⁵ Therefore, it would be more appropriate to classify threats according to this three security element that they have targeted. In another saying, CIA Triad model can be a guideway to possess effective

²⁵ To see more detailed review about these types of cyber-attack, see Glossary of Cyber Operations by Council of Foreign Relations. It is available at <https://www.cfr.org/interactive/cyber-operations#Glossary>

cyber-attack categorizing because what is under the danger among these three elements, the cyber-attacks aim to threaten those elements.

Cyber Attacks that Endanger the Confidentiality

Confidentiality provides the required level of privacy that is enforced at each data processing and prevents the unauthorized disclosure of sensitive information which are the characteristics of infrastructures and the knowledge of the functioning (Harris, 2013, p. 24 ;Whitman & Mattord, 2004, p. 513) Therefore, regardless of whether cyber-attack is social engineering, breaking the encryption, network monitoring and espionage, if that cyber-attack puts confidentiality at risk, it is classified as a threat of confidentiality. With these kinds of cyber-attacks, classified information can be captured, and it can be used to design to create a cyber-attack which could create a threat for the integrity of the systems or information technologies' as it will be mentioned in the following. Moreover, the obtained information can be revealed publicly to cause damage to that actor. For instance, the exposure of private e-mail of the former secretary of state of United States, Hillary Clinton, by WikiLeaks, was the major exposing scandal of the classified information by cyber-attacks. Also, cyber-attacks that are included in this group, mainly target the economic actors. Even though the economically motivated threat agents particularly perform confidentiality attacks, there are also examples of the stealing of commercial and economic secrets in large scale by the state-sponsored actors. For instance, The Federal Bureau of Investigation (FBI) claimed that from at least 2006 until 2018, hackers were extensively supported by Chinese Government to sneak into computer systems with the aim of stealing intellectual property and confidential business and technological information from particularly US- UK origin companies (BBC, 2018).

Another appropriate example of the confidential attack can be given about F35 Fighter Jet. Regardless of the country, "every F-35 has at least two secure networks which are Autonomic Logistic Information System (ALIS) and Joint Reprogramming Enterprise (JRE). ALIS works like a computerized logistical assistance system that tracks issues in each F-35, the location of spare parts, and repair assets worldwide. Each F-35 shares logistical data through the national center and then to the international center server in Texas (Hollings, 2018). During this process, since so much data such as about information about the operation of F-35 are shared, some states underline the danger of this issue. Thus, in the case of a cyber-attacks, the adversaries can gain access to the location of F-35s, their weak and strong aspects, scheduling and

information about the operation detail (Hollings, 2018). So, as these examples demonstrate that the confidentiality attacks are ranged from the leak of private e-mails to endangering the capability of armies in case of war.

Cyber Attacks that Endanger the Integrity

Integrity provides the efficiency and reliability of information against any unauthorized alteration of information technologies and information or system settings (Niekerk & Maharaj, 2011, p. 107). A system, software, hardware, and communication mechanism must work in harmony to sustain data accurately and to transfer data to intended targets without unexpected modification (Harris, 2013, p. 23). Therefore, the cyber-attacks that aims to alter the information in the systems, hardware, and software by deleting or adding, or in other words modifying, they target the integrity element of the security. While mistakes can cause the threat for confidentiality, cyber-attacks that target the integrity of the system are generally carried out with intention through planting a virus, back door or logic bomb and so on so forth.

Stuxnet worm is a good example to illustrate how a cyber-attack targets the integrity of security. When Stuxnet infected a computer, it looked for the computer that was connected to PLC which took a role as spinner centrifuges that enables enrichment of Uranium. When it reached the target, the worm altered the programming of PLC, and centrifuges started to spin too fast until destroying or giving damage to the equipment in the process of uranium enrichment. The most striking point about the worm was that while the centrifuges were being manipulated, the computers that controlled PLC showed everything worked fine (Fruhlinger, 2017). As Bıçakcı underlined, with the increase of anomaly and irregularity, the Stuxnet worm was discovered. So, as long as the anomaly of the cyber-attack that target the integrity is low; there is always a risk of not being noticed by authorities.

Another example can be given again about the F-35 Fighter Jets. As mentioned above, there are two main networks of F-35, which are Joint Reprogramming Enterprise (JRE) and Autonomic Logistic Information System (ALIS). Joint Reprogramming Enterprise (JRE), provides a continuously updated library of capabilities of enemies and their weapon systems so as to inform pilots when they are in battle. Also, JRE is taking major role in the planning of strategies through assessing the distance of anti-air weapons and identifying the vulnerabilities of the

defense system of opponents (Hollings, 2018). However, a cyber-attack that targets the integrity of the JTR could bring F-35 Fighter Jet down by altering the shared data between each F-35. For instance, with a cyber-attack, enemy states could introduce malicious worm in the JRE that could compromise the safety of a mission, shortening the range of a weapon system so that a pilot thinks s/he is safely outside the danger zone when s/he is actually not. In another word, the pilot could fall into a trap and fighter jet could be hit by hostile missiles. Also, with the alteration of data, the target can be changed, and the wrong target can be shot. So, given these facts, it could be claimed that there is no necessary to shut down the aircraft to prevent of flight of F-35, but it is enough to bring down of ALIS or JRE that leads to F-35 stay in the hangar either in peace or wartime.

Cyber Attacks that Endanger the Availability

Availability ensures the reliability and authorized access to data and resources when authorized individuals required to access that information (Harris, 2013, p. 23). For the availability, the many components such as a network (routers, DNS servers, firewalls, proxies, and switches), software (operating systems, antimalware software and applications) must be running in a healthy manner (p.23). Therefore, the cyber-attacks that aims to prevent the continuity of the data transferring process, target the availability of the security components. Denial of Service (DoS) which is the intentional blocking of the machine or network resource by making unavailable in a short time or indefinitely for the authorized users, and Distributed Denial of Service (DDoS) which is computer or network is flooded with information from various sources so as to force it to malfunction or bring down (Klimburg, 2012, p. 76), is the most prominent cyber-attack which targets the availability.

Dmitri Alperovitch (2011, p.8) who is a prominent cybersecurity expert, underlined that “scale and impact” are the key for the attacks that target the availability. While the one-hour DDoS attack on the news website might be considered remarkable, but it is not a strategic issue. On the other hand, DDoS attack that targets the availability of systems of governmental institutions and private companies as in the case of cyber-attack against Estonia is not only remarkable but also a strategic attack that states want to deter.

After all these knowledge about cyber deterrence, types of deterrence, threat, threat actors, types of cyber attacks; now the main issues of implementing cyber deterrence strategies can be addressed.

4. THE DIFFICULTIES IN IMPLEMENTING CLASSICAL DETERRENCE TO CYBERSPACE

As can be seen in the first chapter, there are many different perspectives about both classical deterrence and cyber deterrence. However, all scholars only reached a consensus on one point: Application of classical deterrence theory to cyberspace brings numerous challenges that endanger its success. While some problems are taking place only in the case of retaliation and denial, there are also problems that affect both retaliation and denial strategies. When the main concerns about the application of deterrence to cyberspace are sought out, it is confronted with the following common difficulties (Denning, 2015, p. 8):

The first and foremost difficulty for deterrence is the attribution problem which is the struggle of attributing cyber-attacks to their perpetrators. Attribution plays a major role in limiting the credibility of retaliation threat especially in terms of sending threat messages and communication with the adversaries. Secondly, to realize the cyber-attack is troublesome unless anomaly level increases. Even if authorities notice it, calculating the cyber weapon, and its impacts are very tedious. Also, there is no guarantee that cyber vulnerabilities still exist another time. Thus, the repeatability or stability of cyber- weapons are also problematic. Thirdly, to establish a threshold or to draw red lines for cyber-attacks is difficult. In cyberspace, since to deter all cyber-aggressions is technically impossible, states opt for classification of cyber-attacks according to the level of threats. While some attacks stem from mistakes, some may be intended to cause severe damage. However, states have hesitation about at which stage they will respond. Even if there are ones, who do not want to draw red lines because the withdrawal of the red lines amounts to legalization the attacks below the thresholds, the lack of withdrawal of these lines creates a negative impact on the cyber deterrence as will be discussed.

Fourthly, the perpetrators of cyber-attack can consist of not only state but also non-state actors. The asymmetric nature of cyberspace, the broader participation due to low entry barriers and easy access to cyber tools, and low cost in case of retaliation for non-state actors pave the way for active engagements of the third parties into particularly politically motivated cyber-attacks. Fifthly, while the aggressor could be penalized according to domestic legal arrangements, the international law and the norms on how to punish states after cyber-attack are not fully established in the international arena. Although there are important initiatives such as Tallinn Manual 1.0 and 2.0, it is hard to mention the legally binding agreement and enforcing

international norms over cyber-attacks. Hence, there is a possibility that the attacking country will not give up cyber-attacks because it knows that the possibility of facing a sanction is very low. Last but not the least, given the fact that deterrence by denial is defense facet of deterrence, it is almost impracticable to obtain absolute security in cyberspace.

Besides all of these main difficulties, why are these difficulties taking place in cyberspace rather than the other four dimensions? Even though some scholars (Lupovici, 2016 ; Rid & Buchanan, 2015) suggested these problems are mainly rooted in political and social issues, it is generally accepted that most of the difficulties stem from the inherent features of cyberspace or in other saying architecture philosophy of internet. Understanding the philosophy behind this underlying architecture will guide us in discovering both the source of the problems and the solutions.

The philosophy behind internet can be understood from the hipster movements during the 1950s and 1960s since there is a significant connection between the Hipster Movements and open sources codes that form the internet (Bıçakçı, 2014, p. 113). The apparent articles in manifesto of hipster which are: 1) "Anything that helps us to learn about computers or how the world works should always be shared and accessible without control"; 2) "Promoting of free exchange information"; and 3) "There should be an open system without borders and obstacles" (Levy, 2001, p. 41) clearly demonstrate the fundamental design philosophy of the internet. As manifesto shows that, not the identity of the connector and security but a reliable, easy and fast connection and circulation of free information were aimed at the first design of the internet (Lindsay, 2013, pp. 375-6). All these main problems demonstrate that deterrence is a multi-dimensional concept and its application to cyberspace is quite complicated. Therefore, to better understand and to analyze these difficulties and to offer a solution, addressing the difficulties in implementing classical deterrence in cyberspace separately²⁶ can shed light on how deterrence can be successful.

²⁶ The difficulties in this chapter are mainly derived from nine questions of Martin Libicki which three critical and six ancillaries about distinctions of cyber deterrence from classical deterrence. Also, to classify separately the difficulties, it was appealed to master thesis of Yavuz Akdağ titled as "*Cyber Deterrence against Cyberwar between the United States and China: A Power Transition Theory Perspective*", because the difficulties are appropriately classified in his thesis.

4.1. THE DIFFICULTY OF ATTRIBUTING THE OFFENDERS

Even if attribution problem has become a more visible and controversial concept with the advent of cyberspace, it is an essential concept in every period of history. So, what makes attribution for cyber deterrence is so problematic? To find an answer to this question, it is necessary to look at the prevailing assumptions in the literature.

Attribution is the most challenging problem for cyber deterrence (Betz & Stevens, 2011, pp. 75-76) and this difficulty mainly stemmed from the technical dimension as Libicki (2009, p. 43) and Boebert (2011, pp. 51-2) underlined: Cyber-attacks do not leave distinct physical evidence behind as conventional attacks do. In the cyberspace, there are billions of nearly the same packages. Therefore, cyber-attacks could have been carried out by everyone. The attacker even can be a dog (Steiner, 1993, p. 61)! Even though the technical aspect of cyberspace is held responsible as the main culprit of this situation, it should be noted that attribution is actually not a problem in cyberspace, on the contrary, *“cyberspace has been constructed in a way that has made anonymity easier to attain”* (Lupovici, 2016, p. 330). While the main concept of the internet is anonymity, there is a possibility in which every move on the internet can stay without being attributed.

The attribution problem aggravates the possibility of deterring in many ways. Firstly, because of the attribution problem, the victim state does not even know to use deterrence strategies against whom at the very beginning. This situation is where the whole chain of events starts. When to trace the accurate identity of the attacker is challenging, it is very tedious to convey a threat message as well (Betz & Stevens, 2011, p. 32). That is to say, how does a retaliation by deterrence can be carried out while the victim state does not even know who did it? Thus, with the advantage of problem of attribution, the offender can hide its identity in many ways which necessities great effort by the victim to find out who did it (Kello, 2013, p. 33).

Moreover, the attribution problem not only allows for offenders to hide its identity but also put responsibility for the attack to another party through false flag operations.²⁷ An attacker can adopt the “misleading signatures that so-called false flag” via by using Virtual Private Network (VPN) to change its source to divert its source of the attack to hide its identity (Solomon, 2011,

²⁷ False flag is a deliberate misrepresentation, especially a covert military or political operation carried out to appear as if it was carried out by another party (Online Oxford Dictionary, 2019).

p. 5). As Libicki (2009, p. 44) points out that the false flag operations have greater risk for the success of deterrence by retaliation because in case of misattribution of an attacker and punishing innocent states, there are possibilities of new conflicts with new adversaries. Especially the state who are to be attacked by offender may experience crises with another actor. In that case, the offender state may have a chance to carry out cyber-attacks to put the responsibility on another actor's shoulders via false flag operation due to the attribution problem. On the other hand, some scholars suggested that even though there is a possibility of misattribution the offender throughout the interest (Libicki, 2009, p. 44), offender state can be found from the context (Lucas, 2013, pp. 17-8) since major cyber incidents have been employed by kinetic means by states during international crises (Sterner, 2011, p. 74). In other words, for cyber-attacks in which used as a tool of hybrid conflict and needs absolute retaliatory, attribution is not impossible (Goodman, 2010, pp. 110-2). However, there is always a possibility of false flag operation as indicated reasons above.

Even if the possibility of false flag operation in major cases is ignored, and source of the attack is traced, we confront new difficulties: Is the state a real offender or a third party? In other words, the attribution problem also creates the possibilities of engagement of third parties into crises. For example, even if there is a crisis between the two states, the party that believed as the offender may not have carried out the attack. Despite all evidence points the state actor, the state may not have supported, and the cyber-attack may have been initiated by third parties apart from the state. Although this case is within the possibilities, states generally use third parties to cover their roles with the cyber-attacks.

For instance, in the cases of 2007 Estonia, 2008 Georgia and lastly in the 2016 U.S. Presidential Election, Russia was blamed for these attacks. However, Russia claimed that these attacks were carried by “patriotically minded private Russian hackers” (Higgins, 2017) and Kremlin expressed it has not got any connection both with these hacker groups and attacks. However, due to the attribution problem, solid evidence could not be found to justify legal sanctions against Russia²⁸. Therefore, even if the major cyber incidents take place between major powers, attribution still plays a significant role.

²⁸ However, due to the unwillingness of the Russian government to cooperate with these victim states, Russia has been accepted as an offender.

If it proceeds from the Russian case, another problem of attribution stands out: Legal response to the offenders (Taddeo, 2018, p. 345). There must be enough evidence to carry out a legal process against the suspected actor. Moreover, even if the source of the attack is identified, it is a complicated process to find whether the state is behind the attack unless the legal investigation of within the suspected state is carried out. Attribution to be successfully concluded, the legal process necessitates a great time of efforts to collect evidence and analyze them and to reach a conclusion. Moreover, if the legal process lasts too long, the credibility and legitimacy of exercising retaliation threat will be considerably decreased (Lupovici, 2016, p. 325). As a result, the victim will not be deterred from launching unattributable cyber-attacks when there is no fast and effective retaliation as Lindsay (2013, p. 378) underlined.

Also, there is a discussion that attribution problem can be eased with collective cyber defense as NATO has been trying. In addition to classical meaning of collective defense which means that in case of an attack on members of NATO, the Article V would be triggered; in cyberspace, this method also underlines that the ally countries share information about the cyber-attacks to attribute the source of the cyber-attacks. However, on the contrary to conventional weapons, if a state's defensive system is not developed enough, it is hard to protect from the adversaries with developed states' capacities. For instance, while the nuclear weapons of the U.S. or the air defense systems such as Patriots could protect the allied countries from the threats of the adversaries during the Cold War; however, its defensive technology could not protect the other vulnerable ally states in cyberspace. In addition, every state within the NATO does not have the same capabilities to collect, understand, and analyze the cyber-attack to support the operation of NATO (Porter& Jordan, 2019). Therefore, members of NATO such as the U.S. might be reluctant to share classified information with relatively less developed states due to the risk of exposing or stealing the classified information by adversaries. Hence, the attribution problem appears as a challenging issue for cyber deterrence, especially extended deterrence by NATO.

So, how can the attribution problem be solved? The supporters of the idea that attribution is a technical problem due to the philosophy of architecture of the cyberspace put forward that there is a necessity of reengineering the internet to "make attribution, geolocation, intelligence analysis and impact assessment" (McConnell, 2010). Without the technical improvements, the attribution cannot be overcome. As technological developments and innovations continue, it is regarded that the attribution becomes complicated for the states and companies. However, on

the other faces of the Janus, the defensive technologies are developing as well. The private cybersecurity companies that have relations with the states have a growing capacity to attribute correct actors. (It is another discussion topic that this will bring the dependency of states to private companies for the security.) Thus, as Buchanan (2016, p. 145) points out with the growth of the cybersecurity industry and experts, the complicated attacks can also be uncovered and enough information to attribute can be found. In this direction, for instance, the Internet Protocol version (IPv6) enables improved attribution than IPv4 since IPv6 tracks the source of a package more unerringly. However, it is far from solving the attribution problem completely (Libicki, 2009, p. 43).

On the other hand, some scholars (Lupovici, 2016 ; Rid & Buchanan, 2015) suggested that the attribution is not only related to the technical dimension but also a political and social dimension. For instance, Thomas Rid considers McConnell's idea of reengineering as entirely unrealistic and will never lead to a solution because “the attribution problem has a territorial dimension which makes it a “political problem” (2013, p. 140). Therefore, he considers attribution is “what states make of it” (2015, p. 7). They pay attention not only to a technical dimension but also the human factor, the division of labor, the expertise, strategies and communication to overcome the attribution problem (2015, pp. 6-10). Also, Lupovici (2016, p. 331) asserted that social context is a barrier rather than the attribution problem for successful deterrence. To prove, he addresses Stuxnet case and asks: If a bomb had given the same damage to centrifuges caused by the Stuxnet attack, would Iran have waited for the attribution or would Iran have directly retaliated? In other words, if the attack did not create a severe result, would state ignore the attack or initiate a complicated and expensive process to find out who was attacking? In sum, the main problem for Lupovici about attribution is that social norms such as violence are in the construction process yet. In addition to these two sides, Iasiello (2014, p. 58) has the last word: Successful attribution can only be possible in cyberspace when technical, behavioral and cognitive analysis are merged.

4.2. THE DIFFICULTY OF DEMONSTRATING CYBER CAPACITY

Since deterrence is a psychological game between actors, capacity is one of the most necessary elements for successful deterrence. To discourage the opponent in this psychological game; either defender makes concessions to the offender, or the offender is convinced to have a significant cost in case of performing an undesired act. In other words, the defender needs a

capacity to signal the offender which convinces offender of the cost will be much more than benefit in case of undesired action. For instance, when the world military history is reviewed, it can be encountered that when the states feel anxious about the rival state, and if the opponent is neighbor, units of the army are positioned near the border with that state. Another example is military exercises. States aim to minimize the problems in case of a conflict or war through military exercises, on the other hand, states also appeal to military exercises to show capability and capacity of its army to the rival states. For instance, the joint military exercises by Russia and China in 2018 was a clear message to the United States who has tension with these two countries (Editorial Board of Economist, 2018).

However, in cyberspace, defender state confronts challenges to signal its capacity to the offender for many reasons: First of all, for the success of the signal, it is necessary to convince defender that weapon has the destructive capacity. For instance, it was not expected that cyber weapons could cause physical damage before the Stuxnet. Instead, cyber-attacks were seemed as only causing economic damage. Even a kinetic weapon rather than a cyber weapon should be convincing to the defender. For instance, if Hiroshima and Nagasaki had not been attacked with the atom bomb, it would not be convincing about nuclear weapons' catastrophic consequence on humankind even though its potential strength would be seen in tests (Elliot, 2011, p. 36). On the other hand, there is even no guarantee to use cyber-weapons in another time because cyber weapons are derived from the exploitation of vulnerabilities of the victim. Victim state can discover the vulnerabilities even before the materialization of cyber-attacks and fix them in the shortest time possible. Therefore, it is very challenging for a defender to signal its cyber capacity to the offender.

Secondly, in contrast to deterrence in the other four dimensions, in cyberspace states does not reveal their cyber-weapons so as to increase deterrence stance. For instance, Russia almost displays its nuclear weapon at national days in every possible opportunity in order to give a message to other major states. On the contrary, how can a state display its cyber weapons that only 10-megabyte size? Even state displays its cyber weapons, is it credible in the eyes of opponents? Besides, any state is unwilling to reveal its cyber capacity because it means both sharing the blueprint of cyber weapon and the cyber strategy of the state. Since cyber weapons are designed according to vulnerabilities of the targets, revealing of cyber-weapons means revealing of both vulnerabilities and targets. Also, while the vulnerabilities would be fixed and

the cyber weapon would become ineffective, other actors even can use that cyber-weapon against the creator of the cyber weapon by recoding it (Lindsay, 2015, p. 53).

Even though signaling of capacity is a vital factor for the successful deterrence, many states choose to hide real capacity. Thus, it creates a major negative impact on establishing effective deterrence posture due to minimizing effects on a credible signal on states. In case of no clear signal, deterrence by punishment is doomed to be ineffective, carrying endanger of misperception, misunderstanding and escalation of unintentional crises. For this reason, Uri Tor (2017, p. 100) claimed that the most sensible solution to displaying of cyber capacity is to claim responsibility for the previous cyber-attacks.

4.3. THE DIFFICULTY OF CALCULATING THE IMPACT OF THE CYBER ATTACKS AND REPEATABILITY

On August 6, 1945, when Hiroshima and Nagasaki were attacked by atom bomb which equaled to 15,000 tons of Trinitrotoluen (TNT) (Lockie, 2017), the possible physical damage more or less could be estimated by the United States. If the attack took place one year later, the damage probably would be the same with 1945. Since it is well known by everyone what likely results in the event of a new nuclear attack, the credibility of destructive retaliation threat by the nuclear-armed state is very high. Due to Mutual Assured Destruction (MAD), even it can be claimed that nuclear weapons enable the relatively peaceful environment after World War II. Thus, even it can be claimed that since states could no longer bear the losses of nuclear weapons, the war moves to proxies of great powers. Also, in the beginning, the location of the launching platform of nuclear weapons could be discovered. However, states advanced their launching platform and placed them within the submarines. So, nuclear missiles could be launched from anywhere. As a result, states have developed an anti-missile system to prevent possible nuclear attacks and to decrease the credibility of nuclear weapons.

In contrast, it is tedious to calculate the extent to which impact by a retaliatory cyber-attack because physics rules of cyberspace are different from the other four dimension's physics rules. Thus, firstly, in contrast to kinetic attacks, the attacker has no idea about what the sum of effects of cyberweapons will be after it is launched (Libicki, 2009, p. 52). This ambiguity can lead to two consequences: it will have a far less impact than expected, or it will likely turn into an attack that is much larger than intended. In the case of reprisal cyber-attack that causes less impact than intended, the offender does not deter from this retaliation. Instead, since offender

considers a similar response from the victim state in the forthcoming cyber-attacks, this ambiguity causes to more cyber-attacks. In short, if the response of the victim state is not credible in the eyes of the suspect, this significantly damages the posture of the deterrence. On the other hand, the cyber-attack causes a much more tremendous impact than intended, and this miscalculation could escalate the crises between parties. Even, it could turn into a conventional conflict between parties although there is no example so far.

Secondly, not only the attacker but also victim state cannot accurately calculate what the impact of cyber-weapon is. If the anomaly of cyber-weapon is very low, the victim state even may not discern the cyber-attacks. From the offender states' point of view, probably the worst outcome of retaliation would be that no one should notice the retaliation (Libicki, 2009, p. 52). If the victim state fails to get a response or get it too late, the deterrent message can be considered failure. Another point is that the retaliation message would successfully be signaled to offenders, but the response of the attacker would not have achieved. This ambiguity may create a circulation of uncertainty and can continue as long as one of the parties can reveal cyber-attacks.

Thirdly, there is no guarantee to use cyber-weapons in another time because cyber weapons are derived from the exploitation of vulnerabilities of the victim. Victim state even before the materialization of cyber-attacks can discover the vulnerabilities and fix them in the shortest time possible. Also, these vulnerabilities can be fixed throughout the routine patches without defender realizes there is a vulnerability (Bendiek & Metzger, 2015, p. 559). As a result, as Geist (2015, p. 51) underlined that the new cyber weapon with never-before-seen effects could appear overnight.

Moreover, how states will continue to carry out a retaliatory attack when there is a risk of fixing vulnerabilities immediately by opponents during the conflict. Therefore, the half-life of vulnerabilities that are continually being discovered and fixed leads to the dilemma of "use it or lose it" in the eyes of states (Libicki, 2009, p. 58) In this situation, state seesaws either to exploit the vulnerabilities before the fixed or to wait for a more appropriate time which carries the possibility of never usage of that vulnerability. Besides, it should be noted that; taking into consideration the difficulty of finding new vulnerabilities within the systems, codes, networks, and so forth on, since they do not want to miss the opportunity, states generally exploit the discovered vulnerabilities. As a result of this ambiguity, states cannot assess the effectiveness of a well-thought-through retaliation which is a necessity for a deterrence.

4.4. THE DIFFICULTY OF PROPORTIONATE RESPONSE AND RISK OF ESCALATION

In October 2016, the United State announced that Kremlin-directed both cyber-attacks regarding private emails of Hillary Clinton and the 2016 Presidential Election of the United States (U.S. Department of Homeland Security, 2016). After this official statement, it was highly anticipated how the United States would respond. Afterwards, Barack Obama, the former president of the United States explained that there were many options on the table and the United States would give the most proportional response (Davis & Harris, 2016). So, what is the proportionate response to cyber-attacks?

While there is a principle of proportional response in kinetic conflicts as Geneva Conventions indicated; there is also the so-called principle of proportionality in the cyberspace. As Tallinn Manual indicated that countermeasures of cyber-attack should not violate norms and rules and should be a proportional response (Schmitt, 2017, pp. 122-3). However, as mentioned above, the impact of cyber-attacks cannot be precisely measured. Even if it is measured, it is hard to mention about the legally binding agreement and enforcing international norms over cyber-attacks.²⁹ These underlying ambiguities bring into another difficulty to achieve successful deterrence: *Difficulty of Proportionate Response and Risk of Escalation*.

Proportionately responding in cyberspace confronts with difficulties as follow: First of all, as mentioned in the difficulty of measuring of impact of the cyber-attacks, the impact of cyber-weapons generally takes place in two ways: Either the damage is greater than intended or less than.³⁰ When the high connectivity of modern societies and dual-use technologies³¹ taken into consideration, a cyber-attack can paralyze the modern states. For instance, a bomber drone can distinguish the civilians and military vehicles and pilot of the drone to avoid hitting non-combatants vehicles. However, this discrepancy is not apparent in cyberspace where a computer, systems and networks can simultaneously be used by both military and civilians. (Singer & Friedman, 2014, p. 191)

²⁹ Although there are important initiatives such as Tallinn Manual 1.0 and 2.0 -which guide how international law can apply to cyberspace, led by NATO, NGO's and private companies (Ilves, 2016, p. xxiii)- it is hard to mention about the legally binding agreement and enforcing international norms over cyber-attacks.

³⁰ Although generally the impact of cyber-attacks create fewer impacts than expected, it is still a major issue since it damages the principle of proportional response (Sterner, 2011, p. 73).

³¹ It is a concept to illustrate an equipment suitable or designed for both military and civilian purposes. (Oxford Online Dictionary, 2019)

Secondly, the impacts of the attacks can be observed over months or even years as Stuxnet due to the low level of the anomaly. In the meantime, the systems may seem functioning, but they have already been manipulated by malicious computer worm without attracting any attention by authorities. In such a case, how the state will give a proportional response is quite problematic. On the contrary, the cyber-attacks such as DDoS attacks are easily discernible, these attacks create a public pressure for states “to do something” (Limnéll, 2017, p. 37). To ease the public pressure, states may unwillingly respond to the cyber-attacks which poses a risk of disproportionate response without the attacker being fully determined that may lead a crisis with third parties. This misattribution may extend the scope of crises and lead to an escalation of crises. Besides, since the effects of the attacks cannot be precisely determined, the initial hurry response can be very insufficient as well. Also, when investigation about cyber-attack is completed, very late response to the offender may perceive from the offender as a new attack rather than retaliation, and a new crisis may occur (Limnéll, 2016, p. 10).

Thirdly, cyber-attack can be a result of a mistake made by a user within the system, and a person may even attack himself/herself, which causes significant damage. What happens if a state unintentionally attacks to another state and that state perceives mistake as a deliberate attack and it counterattacks to state which makes mistakes, and that counterattack is perceived by the state that mistakenly attacks as an offensive attack by the state? In short, the intention of an attack in cyberspace is not entirely known, so it is difficult to give an appropriate answer.

Fourthly, which kind of response should be used against the cyber-attacks? Retaliating to cyber-attacks with kinetic tools could be regarded as a proportionate response? In other words, just because the attack came from the cyberspace, the response should be within the borders of cyberspace so as to say the response is proportional. Richard Harknett criticizes this disproportion response by saying that: “*At its core, deterrence theory rests on the principle of retaliation in kind. where the cost inflicted in retaliation will at least match the level of costs associated with the offensive attack. If an attack reduces no buildings to rubble and kills no one directly, but destroys information, what is the response? We tend to think about information as intangible, but the loss of information can have tangible personal, institutional, and societal costs.*” (Harknett, 1996).

As Sterner (2011, p. 72) underlined that this situation brings a dilemma of “bits for lives” that means either the “life of challenger” or “bits of the defender” is more valued. Therefore, the kinetic response is not a proportional response to cyber-attack. Although a kinetic response is

not on the table for many states, on 6 May 2019, Israel broke new ground by becoming the first state which responding to a cyber-attack with an air strike. This response was the first in world history (Doffman, 2019) in terms of responding with kinetic tools against cyber-attacks. Therefore, this attack marks a new period of cyber deterrence and international politics as Doffman (2019) underlined: *“No doubt the regime in Teheran will be taking note. Iran's offensive cyber capabilities are on the increase and could well now be seen as legitimate targets as the U.S. moves military forces into the region.”* However, responding to a cyber-attack with kinetic tools poses a severe risk because, in the case of misattribution, there is a risk of conflict with a third party in the worst-case scenario as it will be discussed in the following headline.

4.5. THE PROBLEM OF ASYMMETRY AND ENGAGEMENT OF THIRD PARTIES INTO POLITICAL CONFLICT

One of the essential difficulties encountered for the success of cyber deterrence is the asymmetric structure of cyberspace. When it is looked at the definition of the concept of asymmetry which is having parts or features which are not similar or equivalent, it points out that: Asymmetric relation between parties is not only a feature specific to cyberspace because it is impossible to acquire equality in terms of anything. In this perspective, it can be claimed that there has never been equality between all states. Moreover, even Libicki (2009, p. 70) asserted that it is hard to mention from perfect symmetric relation between states when there is a country alike the United States. Taking into consideration the capacity of the United States in terms of economic and military capacity, no one can compete with the US. However, such a state like the US was targeted by the terrorist organization through even hijacking a passenger plane and intentionally crashing the symbolic Towers of the World Trade Center. Especially in regard to terrorist attacks, to implement a deterrence policy against them is very complicated for states. Moreover, how a state can deter one who wants to explode himself.³² These issues show that difficulties of asymmetry are not only specific to cyberspace. However, the level of asymmetric relations in cyberspace cannot be comparable with other dimensions.

This distinction is firstly stemmed from the low cost of entering and standing in cyberspace that allows for non-state actors to get a more active role within the cyberspace. Also, in contrast to the other four dimensions, non-state actors have more opportunity to possess cyber tools more

³² For more detail, Uri Tor, ‘Cumulative Deterrence’ as a New Paradigm for Cyber Deterrence”, *Journal of Strategic Studies*, Vol.40, No. 1-2, 2017, pp. 92-117

easily. The non-state actors such as individuals, organizations and other many sub-state entities have cyber tools which can cause damage either physically or virtually, with fewer efforts and cost than kinetic weapons. For instance, a million-dollar budget is needed to launch a kinetic attack against the state, with a few hundred dollars, non-state actors can carry out cyber-attacks which cause a damage worth of billion dollars. However, as Geers (2010, p. 302) underlined that just because non-state actors possess cyber weapons, it does not mean they have "computer network or other "identifiable infrastructure" worth being attacked by retaliation. That is to say, if the victim state cannot retaliate to the non-state actor since there is no solid target to hit back at, deterrence fails due to given asymmetric relations (Bendiek & Metzger, 2015, p. 559)..

On the other hand, asymmetric relations do not only take place between state and non-state actors; but also, between states. While some states have much depended on information and communication technology to continue their daily life, some states have less. In another saying, the asymmetric relation between states stems from the dependency on cyberspace. Therefore, the less wired state has less vulnerable to retaliation by cyber means (Bendiek & Metzger, 2015, p. 559).

The relation between North Korea and the United States is an appropriate illustration of asymmetric relations of states in cyberspace. The society and economy of the United States are heavily depended on cyberspace. Moreover, it is undisputedly the first country in terms of cyber capacity in the world. On the other hands, it can be mentioned about neither North Korea is socially nor economically integrated into cyberspace. In fact, even access to the internet has gradually started (Kang, 2018), and that North Korean network only allows for the connection to the domestic websites. So, it is not possible to say that ICTs have become widespread across North Korea. On the contrary to this restricted wired environment, North Korea has significant cyber capability and capability. In this asymmetric relationship, while North Korea could cause significant damage through cyber-attacks, the US had to adopt other alternatives rather than hit back with cyber-attacks due to asymmetrical relations.³³ Therefore, as Geers (2010, p. 302)

³³ The Sony Hack case can be given as good example to demonstrate the asymmetrical relation between two parties. To see: Andrea Peterson, The Sony Pictures hack, explained, *The Washington Post*, available at https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?utm_term=.b97d99a00804

underlined that the asymmetric nature of cyberspace damages the credibility of deterrence by punishment.

As another example, the Estonian Cyber Attack in 2007 by Russia can be given. Estonia is the prominent well-wired state in the world, and it has a reputation as an “E-stonia” thanks to its great connection over the country. Even it was the first state that introduced online voting for elections (Mulligan, 2017). On the other hand, Russia has the considerable cyber capacity, but it is hard to say Russia is wired to cyberspace all over the country. In 2007, Estonian government decided to move the “Bronze Soldier Monument” (original name is “Monument to the Liberators of Tallinn”) was unveiled by Soviet Authorities in 1947, to the outskirts of the city (McGuinness, 2017). As a result of this decision, outrage among Russian speakers in Estonia led to spark of outrage, and they took to the streets. In the following of these incidents, Estonian government bodies, banks, important organizations and many media outlets were taken down by major DDoS cyber-attacks that cause unprecedented levels of internet traffic, and it lasted weeks (McGuinness, 2017). Even after this attack, it was claimed that “hackers take down the most wired country in Europe” (Davis, 2007). For DDoS attacks, Estonia had accused direct involvement of Kremlin and claimed that “Not only Estonia but the European Union was under the attack (Davis, 2007). However, Estonia had no chance to deter Russia with cyber-attacks considering the less wired environment of Russia. Therefore, in contrast to the other four dimensions, states have ironically turned into the most vulnerable actors in cyberspace when they have developed their ICTs because of asymmetrical structures of cyberspace. Thus, the metaphor of Singer and Friedman in which “*most powerful and heaviest biggest rock-throwing actors in cyberspace live in the most precise and largest glass houses*” quietly describes this environment (Singer & Friedman, 2014, p. 152).

Besides, the Estonia case brings another significant difficulty for successfully achieving cyber deterrence: *Engagement of Third Parties into Political Conflict*. For DDoS attacks that paralyzed the Estonian's government and economy, Estonian Foreign Minister “Urmas Paet” directly accused the Kremlin (Davis, 2007). However, Duma Deputy Sergei Markov offered Estonia think another perpetrator rather than the Kremlin by commenting that “*do not worry, that attack was carried out by my assistant. I will not tell you his name, because then he might not be able to get visas*” (Leyden, 2009). His assistant was a leader in “Ours” (Nashi) movement which consists of 120.000 Russian teenagers. “Ours movement” not officially part of the Kremlin but organized by Pro-government supporters to fight over the anti-fatherland forces

(Singer & Friedman, 2014, p. 111). During the Estonia attacks, even they try to find extra supporters for the attack by sharing how to make a computer a zombie computer in blogs. Even though Estonian officials believe that Kremlin heavily supported of these patriotic hackers, there is no firm evidence that these attacks were carried out by the Kremlin (McGuinness, 2017). In this environment, while Russia did not accept the direct relation with Estonia attack and put the responsibility to third parties, Estonia could not retaliate with cyber-tools against third parties.

From these underlying points, difficulties for cyber deterrence that caused by engagement of third parties can be listed as: Firstly, even though the non-state actors take an important role in the physical domain, however, since easy and low cost access to cyber weapons has led to both increase of non-state actors and their capacity in cyberspace, they have turned into direct combatant in the conflicts rather than indirect role. In this way, “third parties can play in the same league as states” (Libicki, 2009, p. 63). For this reason, they have acquired the right to act waywardly. Secondly, it is almost impossible for non-state actors to initiate and continue an attack in the other four dimensions without the knowledge of the state. For example, if the militias initiate an operation, it is unlikely that the state will be unaware of it. It either supports the operation or stops it immediately. Also, any non-state actor cannot be part of the attack without the government's permission during an operation in the physical world. However, in the event of a crisis between the two states in cyberspace, “patriotic hackers” of one side can attack the other parties without the permission of their states. In this case, even if the state that in the position of the offender wants to stop the participation of third parties into conflict may not successfully hinder them. On the other hand, the victim state put the responsibility to opponent government for the cyber-attacks and may escalate the crises by counter cyber-attacks.

Thirdly, in case of a crisis, states may have asked for help from non-state actors and non-state actors may have played an essential role in the crisis. Then, states may have desired to cease the conflict with other party and to meet on common ground diplomatic or other means. However, “patriotic hackers” may not be satisfied with the deal, so that they may carry out new cyber-attacks. This situation may lead to down the pan of all diplomatic initiatives and may even lead to new conflict between two sides. Thus, as Libicki (2009, p. 63) rightfully points out that the participation of third parties weakens an implied promise of deterrence “if you stop, we stop” and strengthens the promise of “if you stop-it stops”.

Fourthly, one of the essential requirements for deterrence is a rational cost-benefit calculation since it is not possible to establish a deterrence relationship with an irrational actor. When it is considered that non-state actor can hack just for fun and personal prestige or for their interests rather than a state; they can be classified as irrational actors within the international system. Thus, all the reasons demonstrate that third parties, especially patriotic hackers decrease the chance of cyber deterrence by retaliation.

Fifthly, the third parties do not have to be non-state actors. To limit the target of cyber-attack with one target is very difficult due to the vast proliferation of ICTs all over the world and international connection. Thus, in case of an attack, the other states also can be the target even though there is no relation with offender state. For instance, as mentioned above few times, Iran was the real target of the Stuxnet virus. However, when it is looked at the report, it is shown that almost %43 of the cyber-attacks target the other states (Zetter, 2011). So, the cyber-attack always carries a risk of engagement of the third parties into a conflict which may escalate the crises and decreases the chance of success of the cyber deterrence.

4.6. THE DIFFICULTY OF DRAWING RED LINES

In cyberspace, to deter all cyber-aggressions is technically and practically impossible since there are numerous cyber-attacks from penetrating a system to manipulating information to intentionally causing devastating failures of critical infrastructure; from defacement of the website to DDoS attacks that paralyze the whole country (Solomon, 2011, p. 11).. Besides, while which some cyber-attacks stem from the unintentional mistakes, some may be intended to cause great damage. Therefore, states need a classification of cyber-attacks according to their level of threat. However, this classification of cyber-attacks is not an easy task because there is a need for efficient communication between parties over what are acceptable and unacceptable behaviors (Iasiello, 2014, p. 56). In other saying, for successful deterrence strategy, there is a necessity to draw red lines or establish thresholds which both offender and defender should recognize. While in physical world, to draw redlines is relatively uncomplicated process because it is easy to measure “simple” and “recognizable” thresholds (Schelling, 1966, p. 137), on the other hand, in cyberspace to draw red lines in accordance with what state wishes to deter

is complicated due to idiosyncratic features of cyberspace. So, what are the reasons for difficulties to elucidate to redlines in cyberspace?

The first reason is that as Solomon (2011, p. 12) pointed out there are limited international norms defining cyber-attack and its impacts. Thus, it is generally applied to long-standing international law to describe in which cyber-attack will exceed the threshold. In this way, it is underlined that if a cyber-attack creates damage which equals to damage by kinetic weapon, then defender could respond to cyber-attack through kinetic tools” (Beidleman, 2009, p. 12). NATO also drew an analogy from international law and even agreed that a cyber-attack could trigger the famous Article 5³⁴ (Goździewicz, 2016, p. 56). However, Article 5 can only be invoked in case of a cyber-attack which creates a kinetic effect such as significant damage and loss of life (Healey & Jordan, 2014, p. 4). In addition, NATO also declared that there would be harsh respond to serious cyber-attacks even if they do not cross the threshold of Article 5 (NATO, 2018).³⁵ However, there is an ambiguity about which cyber-attacks cross the threshold. As can be seen from the above, to justify a cyber-attack as *jus ad bellum*, or to consider a cyber-attack that crosses the threshold, it is considered that the cyber-attack must cause severe results similar to kinetic attacks. On the contrary, the cyber-attacks such as DDoS, espionage and data privacy violations that could cause serious consequences would remain below the threshold just because they do not cause similar impact with conventional weapons. This ambiguity is an apparent indication of drawing similar red lines with the physical world is challenging because the inadequacy of international norms about the cyber-attacks is incompatible to cyberspace.

Secondly, as Libicki underlined that death of people is an advantageous situation for the physical world in terms of drawing red lines because it is unambiguous, however, in cyberspace, death is a secondary rather than primary consequence (2009, p. 67). Moreover, when taken into consideration that there is no-one who died due to the direct impact of cyber-attacks, it can be seen that drawing an analogy from the international law confronts significant challenges. Thirdly, most of the undesired impact of cyberattack has taken place in the forms of economic

³⁴ Article 5 is one of the famous articles of the North Atlantic Treaty which specifies that in case of an armed attack to one or more of the members of NATO, it is considered an attack against them all.

³⁵ For NATO, it is vague about implementing an extended deterrence strategy against severe cyber because so as to offer a collective defense, allies should integrate their cyber networks. In this case, technologically advanced members, especially the US, may become more vulnerable because with the integration of the system, the deficiencies of relatively less developing countries may make the system more fragile (Morgan, 2010, p. 73). Therefore, Although NATO encourages member states to develop their cybersecurity capacities and capabilities, it does not seem likely that they will use completely integrated system soon.

loses so far. Therefore, there is also a necessity to establish a threshold regarding economic criteria. However, determining the amount as a threshold is not an easy task: If \$ 500,000 is decided as a threshold, is not it going to be deterred below the threshold? To overcome this situation, Libicki (p. 68) proposed a method in which different response can be applied according to the level of damage from ten to one. However, this brings another issue into question: How to draw a red line for the elements that have no material value such as losses of secret, trust and privacy in cyberspace? This difficulty particularly prevails among espionage attacks. What should be the threshold for stealing information? After which stage of espionage justifies the response by victim state? As it will be analyzed in the third chapter, the United States which is the most exposed to espionage attacks, has attempted to establish a threshold for espionage attacks. Thus, as Clapper (2013) underlined that the US and its ally countries have initiated to change the preconceived norms of cyber espionage attacks as they are not all acceptable. In this context, they stated that only the espionage actions to ensure the national security of the state are acceptable and that it is unacceptable if it is to be motivated by economic motivations to take advantage commercially.

All of these difficulties to draw red lines in each case decrease the credibility of deterrence by both retaliation and denial. Most of these difficulties actually take place due to the lack of international law about the cyberspace. Therefore, in order to fill this international law norm deficiency and to draw a credible red line, important initiatives such as Tallinn Manual 1.0 and 2.0 -which guide how international law can apply to cyberspace, began to appear. In particular, Manual analyses the major events that are important for international law by comparing them with the cases in cyberspace so as to establish an applicable and practical threshold. In this respect, Tallinn Manual restated that if a cyber-attack causes severe consequences such as the death of civilians, it is considered a breach of laws as expressed 1949 Geneva Convention and it justifies the retaliation through either kinetic or cyber tools (Goldstein, 2013, p. 134). However, the distinct point of Tallinn Manual is that not only Manual justifies retaliation against cyber-attacks that cause an impact as kinetic tools do, but also it justifies the cyber-attacks that its impact can be visible in cyberspace. For instance, sabotage cyber-attacks that aim to cause economic damage or manipulation attacks which would constitute an attempt to weaken the integrity of the state are considered crossing the red line and justify the response by the victim state (Goldstein, 2013, p. 135). However, even though Tallinn Manual is a pioneering initiative regarding international cyber law and drawing thresholds about not only for cyber-attacks that cause physical damage but also cyber-attacks that stay below the

thresholds; it has still many challenges to overcome. The main reason for these challenges derives from the facts that "states desire to continue their activities in grey areas" and "states cannot find a middle ground about defining legal norms" as will be discussed below.

4.7. THE DIFFICULTY OF DISSUADING STATES FROM EXPLOITING GREY ZONES AND CREATE INTERNATIONAL NORMS IN AN ENVIRONMENT WHERE NOBODY TRUSTS EACH OTHER

As discussed above, the existing international norms and rules face difficulties to address the issues in cyberspace. A significant proportion of these challenges take place due to the unique elements of cyberspace which make complicated it to apply the international law established in accordance with physical logic. For instance, it is still unknown what justifies the kinetic response in cyberspace or how a foreign perpetrator would be tried and so forth on. However, to assert the failure of precisely deciding rules of international cyber law and to make it binding by states is an idiosyncrasy of cyberspace, led to failing to notice an important point: *States are the forefront actors of writing and implementing international rules*. For instance, almost one decade after the first usage of aircraft in war by Italy against the Ottoman Empire in 1911 (MacIsaac, 2016), the 1923 Hague Rules on Aerial Warfare was written to decide how the aircraft should be used either in peace and war. Although comparing aircraft with cyber tools does not seem to be an accurate comparison, the underlying point of this comparison is that there is no cyberspace version of international law such as Hague Rules on Cyberwarfare or Cyber Geneva Convention even though decades pass on the first usage of cyberspace.

Although it is an undeniable fact that the forefront barrier to such a legal arrangement is the inherent feature of cyberspace, also states cannot agree on international norms or do not want to meet at a common ground. The reason why states cannot agree on binding international legal rules is that rules consist of pitfalls for states. This means that state fears from a binding treaty because to accede to a treaty necessity giving up some advanced technologies (Menn, 2011). In this way, when asked to the UK and its allies want a treaty to as NATO adviser Rex Hughes, he said that: *"The official response is yes, we want there to be rules of the road and to apply the law of armed conflict. But unofficially the answer is no – countries that have advanced capabilities want to preserve that"* (Menn, 2011).

There are three reasons for states to dissemble: 1) States have the desire to exploit the cyberspace according to their interests; 2)The fear of tying their only own hands while others

continue to exploit the cyberspace through ignoring the new international laws (Singer & Friedman, 2014, p. 186); 3) States have different priorities which aggravating to meet at common ground.

Firstly, the grey zone is a concept that is used to define a situation where the borders are not accurately determined, the cyber actions do not bring legal consequences, but states did not welcome the actions. Therefore, it can be claimed that there are neither war nor peace in the grey areas which constitute a rather favorable zone of an abusing for the states. States also try to limit their activities to stay below the threshold to preclude the possible kinetic response by rivals. In this way, without the direct kinetic or severe response from the victim states, states can exploit the grey zones to pursue their strategic interests. In this respect, James Andrew Lewis claimed that states are unlikely to launch cyber-attacks that create a catastrophic consequence since it brings immediate severe retaliation. Instead, states seek to maximize their interests in grey areas without engaging in armed conflict (Lewis, 2018, p. 9). In short, Lewis also underlined that the most fundamental problem for states, especially the US, is the attacks that occur in grey areas rather than devastating attacks because states do not know how to retaliate to these attacks (Lewis, 2018, p. 12). For these reasons, states do not want to give up this beneficial area at least for now.

Secondly, states generally perceive keeping to the agreement as standing idle with hands tied in cyberspace because states have a lack of confidence about other states and forecasts other states as violating the rules of the agreement. It is relatively easy to check the other parties whether stick to an agreement on limiting of kinetic weapons especially in the modern times thanks to numerous surveillance tools and methods, on the other hand, it is rather problematic to check whether the parties comply with an agreement on limiting cyber weapons in cyberspace. In other saying, the difficulty of disarmament of cyberweapon, which creates a very undesirable condition for deterrence, also poses a severe problem for the implementation of international law. Also, in this insecure environment, states are also abstaining from other states' legislative proposals because to agree on the provisions for binding agreement may create a disadvantage for itself in the long run (Singer & Friedman, 2014, p. 186). So, this ambiguity of intention compels states to abstain from the binding treaties.

Thirdly, even though it is agreed that the cyberspace is an emerging battlefield and this environment necessities international norms and rules; the states who will have an essential role in the formation of norms in cyberspace such as the US, China and Russia, have different

priorities which aggravating to meet at common ground. For instance, given the consideration of leader role of the US in terms of “know-how” and “intellectual properties”, it can be straightforwardly predicted that the US will support the legal regulations about restricting the economically motivated cyber espionage attacks (Menn, 2011). On the contrary, it cannot be expected from Russia that has relatively fewer intellectual properties than the US, to show similar effort to limit espionage attack. In addition, the US is trying to promote international norms regarding limiting the governments' censorship right because it considers censorship is a tool of totalitarian regimes over their people (Markoff & Kramer, 2009). The states that are well known for their censorship such as China and Russia reject these international norms since these countries consider censorship is a domestic issue rather than the international. Therefore, they are embracing the uncompromising approach over censorship. Also, China even considers the distribution of cyber tools to activist to surpass internet monitoring as a cyber-attack (Menn, 2011). Moreover, China that attaches importance to “social stability” also objects the application of norms of humanitarian law into international cyber norms such as human rights and freedom because it sees these norms as a means of the United States to justify its intervention of other states' domestic affairs. Instead, according to a spokesman for the Foreign Ministry, China attaches great importance to concerns about the security of information through supporting internet safety and cracking down on criminal activities in cyberspace (Markoff & Kramer, 2009).

On the other hand, Russia tries to create an international norm on the cyber-attacks that targets critical infrastructure (Grigsby, 2018) and try to the disarmament of cyberweapons. For instance, Kremlin offers an agreement that is underlying the ban a state from secretly inserting malicious codes that could be activated anytime (Markoff & Kramer, 2009). While the United States attaches importance to establish the rules of international law related to espionage attacks because the US is the most attacked country through espionage attack as it will be seen in the third chapter, in the same way, Russia tries to prevent the development of weapons by the US such as the logic bomb that can stay without noticed and activated at crucial times (Markoff & Kramer, 2009). Also, it is also possible to interpret Russia's attempts to arms control in cyberspace as while it is very challenging to monitor whether state to increase its cyber weapon armory, given the cases of Estonia and Georgia; Russia also employs the non-state actors (or as Russia called them as “patriotic hackers”) (Singer & Friedman, 2014, p. 186). So, it would not be wrong to assume that Russia will benefit from disarmament treaty rather than to suffer from it.

In short, although it is an undeniable fact that the forefront barrier to such a legal arrangement is the inherent features of cyberspace; states cannot agree on international norms or do not want to meet at a common ground due to their different priorities from each other. Therefore, major states have been locked in a fundamental disagreement over how to prevent the increasing threat of cyber-attacks so far and this situation not only led to decrease the effect of deterrence strategies but also led to increasing of the number of the cyber-attacks.

4.8. THE DIFFICULTY OF PROVIDING ABSOLUTE SECURITY

Almost all the difficulties as mentioned above were related to the deterrence by punishment. However, apart from deterrence by punishment, there are also very severe difficulties for deterrence by denial which is one of the major classical deterrence strategies. Given the main hypothesis of deterrence by denial that it is defensive facet of deterrence (Goodman, 2010, p. 106) which aims to persuade attackers to change its mind by convincing defensive systems would prevent any attacks or even if the attack breaches the defensive system, the aggressor would not be able to reach its aim (Kugler, 2009, p. 327). In this way, offenders are convinced that launching a cyber-attack will not bring the benefit but the costs due to defensive capacities and measures (Goodman, 2010, p. 108). Moreover, it is claimed that deterrence by denial is more effective strategy than deterrence by punishment (Tolga, 2018, pp. 13-4) since it does not encounter severe problems such as attribution problem, the risk of escalation, disproportionate response and so forth on that deterrence by punishment does.

On the other hand, given the fact that deterrence by denial is defense facet of deterrence, firstly, it is almost impracticable to obtain absolute security in cyberspace similar to the medieval fortresses that were almost impossible to climb over. Just as the medieval fortresses began to collapse with the development of military technology - the usage of cannonball in the war - bring the curtain down on Medieval Age symbolically; cyber-weapons have the capability to put an end to an age every day due to its "*dynamic and fast-evolving nature*" (Geers, 2010, p. 300). Also, the system or computer may be running without any problems, but a low-anomaly logic bomb may have already been injected into the system. In other words, a trojan horse that sneaks into the castle can suddenly destroy the whole castle if it is activated. Great cyber firewalls can be constructed each day more robust than the previous one, but it cannot guarantee that it will not be overpassed the next day because it is unclear what new cyber-weapon is capable of tomorrow.

Secondly, the development of conventional weapons takes a long time compared to cyber weapons. For instance, while the development of cannonballs to destroy castles has lasted for centuries or the fundamental philosophy of the atomic bomb is almost the same since 1950; on the contrary, Kaspersky Lab detected “360,000” new malicious suspicious programs a day in 2017 (Kaspersky Lab, 2017). As this comparison demonstrates, while the defensive technologies against conventional weapons can be developed relatively more efficiently; the fast and dynamic development of offensive cyber tools hampers the efficiency of deterrence by denial. Thirdly, a state not only must protect its fortress against the state but also against numerous different the non-state actors because as Mudrinich (2012, p. 170) pointed out that not only states but also non-state actor can possess these weapons in cyberspace due to possessing a cyber-weapon is easy and cheap.

Therefore, with these various actors, complex and sophisticated threats, to provide absolute security by preventing all threats has become troublesome in the eyes of states. Although the cyber deterrence by denial strategy is held the upper hand against deterrence by punishment strategy at the beginning because it does not encounter the major problems such as attribution problem; this strategy has been criticized since the defense cannot be fully implemented in cyberspace. Instead, states have started to think about new strategies to ease the possible damage at a minimal level, to provide continuation of operation process without losing function of affected computers and networks or information systems when an attack takes place (Ridout, 2016, p. 78). This new strategy is called “deterrence by resilience”.

5. WHAT CYBER ATTACKS TELL ABOUT CYBER DETERRENCE AND STATES' STRATEGIES ABOUT NEW DIMENSION?

Cyber deterrence studies are generally concerned with how deterrence can be acquired in the literature. In these studies, mostly the necessary elements, reason of failures, possible scenarios of cyber-attacks and so forth are analyzed with theoretical assumption rather than case studies of cyber-attacks. This situation mostly stems from; failure to identify the offender which is also called the problem of attribution, secondly; inability to know/decide how to respond against the cyber-attacks that are below the threshold, thirdly; inability to realize when cyber-attack is started and lastly; the difficulty of analyzing cyber-attacks since there are thousands of cyber-attacks that take place per second. However, as Goodman points out, examining deterrence only from a theoretical point of view and ignoring political elements will lead to exaggerating the extent of the attacks in cyber space and even to perceive deterrence as a concept that will never be realized (Goodman, 2010, p. 1).

In parallel to Goodman's argument, in this chapter, it will be tried to analyze cyber-attacks with cases to interpret whether the theory of deterrence can be applicable for cyberspace. For the meaningful interpretation, a great number of cyber-attacks will be used even though it is a fact that each cyber-attack has its distinct structure and contain different elements. On the other hand, it is very likely that all cyber-attacks are distinctive from each other. Thus, by analyzing large number of cyber-attacks, the classification will be created from the common points of cyber-attacks in the light of data that has been obtained from open sources. Even in case not having constructive interpretation end of the analysis, at least large number of cyber-attacks can guide us about cases in which cyber deterrence is failed.

For this reason, in this chapter, 260 cyber-attacks are analyzed within six categories as suspected state actors, the victim state, the time of the cyber-attack, the type of attack, the target sector of the attack, the response of the victim state.³⁶With these categorizing, hypotheses about the main problem of cyber deterrence and the necessity of cyber deterrence will be produced to guide us about practicality of cyber deterrence. In addition, the testability of the meaningful relationship between the variables within the 260 cyber-attacks will be examined by statistical analysis for the requirements of the scientific study.

³⁶ Details about analyses can be found at the chapter of 1.5 Methodology of Analyze.

5.1. FINDINGS OF ANALYSIS AND HYPOTHESES

When qualitative data is converted into statistical data, the attention is first drawn to the relations of suspected and victim states.³⁷

Table 5.1: Suspected State-Victim State Cross Tubulation

		Suspected					Total
		China	Russia	Iran	North Korea	US	
Victims US	Count	56	18	13	7	0	94
	% within Victims	59,6%	19,1%	13,8%	7,4%	0,0%	100,0%
	% within Suspected	48,7%	27,3%	37,1%	35,0%	0,0%	37,2%
Asian Allies	Count	35	3	1	12	0	51
	% within Victims	68,6%	5,9%	2,0%	23,5%	0,0%	100,0%
	% within Suspected	30,4%	4,5%	2,9%	60,0%	0,0%	20,2%
EU	Count	14	23	3	1	0	41
	% within Victims	34,1%	56,1%	7,3%	2,4%	0,0%	100,0%
	% within Suspected	12,2%	34,8%	8,6%	5,0%	0,0%	16,2%
Russian Sphere	Count	0	18	0	0	0	18
	% within Victims	0,0%	100,0%	0,0%	0,0%	0,0%	100,0%
	% within Suspected	0,0%	27,3%	0,0%	0,0%	0,0%	7,1%
Middle East Allies of US	Count	0	3	12	0	0	15
	% within Victims	0,0%	20,0%	80,0%	0,0%	0,0%	100,0%
	% within Suspected	0,0%	4,5%	34,3%	0,0%	0,0%	5,9%
Iran	Count	0	0	0	0	6	6
	% within Victims	0,0%	0,0%	0,0%	0,0%	100,0%	100,0%
	% within Suspected	0,0%	0,0%	0,0%	0,0%	35,3%	2,4%
Russia	Count	2	0	0	0	4	6
	% within Victims	33,3%	0,0%	0,0%	0,0%	66,7%	100,0%
	% within Suspected	1,7%	0,0%	0,0%	0,0%	23,5%	2,4%
India	Count	7	0	0	0	0	7
	% within Victims	100,0%	0,0%	0,0%	0,0%	0,0%	100,0%
	% within Suspected	6,1%	0,0%	0,0%	0,0%	0,0%	2,8%
Turkey	Count	0	1	5	0	0	6

³⁷ However, even if the Israel was included the analyse as both suspected and victim, Israel is excluded from the Statistical Chi-Square Model. Since, cyber-attacks numbers of other suspected state's cyber-attacks quite higher than Israel which decrease the frequency of relations between suspected and victims and to decrease the significance statistical data. Also, the joint attacks and one denial response is excluded from the statistical analyses.

	% within Victims	0,0%	16,7%	83,3%	0,0%	0,0%	100,0%
	% within Suspected	0,0%	1,5%	14,3%	0,0%	0,0%	2,4%
China	Count	0	0	1	0	4	5
	% within Victims	0,0%	0,0%	20,0%	0,0%	80,0%	100,0%
	% within Suspected	0,0%	0,0%	2,9%	0,0%	23,5%	2,0%
North Korea	Count	1	0	0	0	3	4
	% within Victims	25,0%	0,0%	0,0%	0,0%	75,0%	100,0%
	% within Suspected	0,9%	0,0%	0,0%	0,0%	17,6%	1,6%
Total	Count	115	66	35	20	17	253
	% within Victims	45,5%	26,1%	13,8%	7,9%	6,7%	100,0%
	% within Suspected	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%

When the analysis is revived, it is seen that most attacked first three countries/country group are most developed countries in terms of economic and technologically which are the US, The Asian Allies of the United States and the European Union in order. On the other hand, China appears as the most suspected actors that carry out cyber-attacks to these three countries/country groups. Also, the United States is the country that most cyber attacked with 94 attacks that carried out by China (56), Russia (18), Iran (13) and North Korea (7). For the Asian allies of United States, it appears as that the group is suffered from 51 cyber-attacks that are carried out by China (35), North Korea (12), Russia (3) and Iran (1). For the European Union, the 41 cyberattacks carried out by Russia (23), China (14), Iran (3) and North Korea (1). In the light of these information:

Firstly, it is observed that there are rather troublesome relations between the countries where cyber-attacks are taking place. The mentioned countries either have politically problematic relations or are competitive with each other. For instance, when the countries that attack the United States (China, Russia, Iran, North Korea) are classified at a common point, the headline can be called as "*countries that challenge the hegemony of the United States either globally or regionally*". This example reveals that the states bring political issues, political rivalries in four dimensions into cyberspace as well. As Yves Lacoste asserts that geography is for fighting (Lacoste, 1998), a similar hypothesis that *states maintain their similar political motivations in land, sea, air and space in cyberspace as well*, can be put forward. Even one who does not follow political developments, can easily notice the tension between the two countries only

when they look at these cyber-attacks. In other words, even the numbers of cyber-attacks can reveal the relationship between the two countries.

From this hypothesis, it can be asserted that *cyber deterrence becomes more challenging task to achieve because of the increased risk of cyber-attacks in the event of political tension or competition between parties*. In order to test this hypothesis, the relations between China and the United States is applicative. As showed up in "Suspected -Victim" relations table, for 115 of 253 cyber-attacks³⁸ that equal to 45,5 percent of all cyber-attacks, China appears as the most suspected state for cyber-attacks. 56 of the 115 cyber-attacks of China target the US which means that while 48,7 per cent of China's cyberattacks targets the US, on the other hand, it forms 59,6 of cyber-attacks that target the United States. Thus, it should be asserted that given the global economic and political hegemony rivalry between China and the United States; and 56 cyber-attacks that carried out by China to the US, support the hypothesis that the economic and political rivalry continues in the cyberspace along with other four dimensions and to aggravate a possibility of achieving cyber deterrence between two parties.

When looked at the China, also it appears that while China carry out 56 cyber-attacks to United States, 35 of the remaining 59 cyber-attacks (30,4 percent of China's attack, 68,6 percent of all attacks that target the Asian Allies of United States) targets the countries who have political problem in Eastern Asia with China such as Taiwan and Japan. With this information, another hypothesis can be put forward: *If there is a political conflict between the states in the same region, the frequency of cyber-attack increases and the likelihood of achieving cyber deterrence decreases*. When it is looked at the other examples in the analysis to test this hypothesis, firstly the relations of Ukraine and Russia draw attention since all 11 cyber-attacks that targets Ukraine were carried by Russia. When other examples in the analysis are reviewed, it is ensued that Iran has carried out 17 of its 35 attacks directly to the countries in its region (Israel, Saudi Arabia and Turkey that are considered as regional rivalry states in the eye of Iran), and of 20 cyber-attacks that target to South Korea, 11 are carried out by North Korea and 6 by China. These examples are crucial for understanding how regional political tension is effective in the materialization of cyber-attacks. When 94 cyber-attacks on the US were excluded from 260 cyber-attacks, 106 cyber-attacks of the remaining 166 attacks took place among regionally rival states. Thus, it can be claimed that *if the political tension is higher among the countries in the*

³⁸ 260 is the total number, due to exclusion of Israel as a suspected actor and denial response in statistical analysis, total cyber-attack number is taken as 253.

same region rather than different region, the cyber-attack rate is higher, and this situation makes the deterrence against the state in the same region considerably challenging.

In addition, the map of the cyber-attacks shows that the proxy warfare of major powers is continuing with the new forms. As Andrew Mumford points out that cyberspace offers a platform on which to participate to indirect conflicts (2013, p.44). When looked at the development within the international system; China appears as the first country that needs an indirect conflict. The main reason is that while China is a rising a new global power which necessities projection of power and interest maximization, on the other hand, China needs to contain its influence to prevent direct conflict so as not to endanger the existing economic interdependence. Indeed, even it could be asserted that a form of proxy war has been simmering between US and China over Taiwan since while the United States sees Taiwan as place to block Chinese expansion and weaponing the Taiwan (Mumford, 2013, p. 44), on the other hand, China perceive Taiwan as area of enlargement and ally of the US. Thus, cyber proxy warfare is a rather useful tool for China to maximize interest and to projecting power without direct conflict. By cyber-attacks, China both can test the defense system of US military weapons and steal the blueprint of the weapons. In this way, it can be argued that cyber-attacks from China to Asian allies of the United States can be the rehearsal of possible attacks on the United States. Therefore, this circumstance also points out the fact that *conflicts are getting more hybrid between states through the increase of usage of cyber tools. Hence, it is very unlikely to achieve successful deterrence in cyberspace without considering political elements and conventional tools as well.*

Another point is that cyber-attacks in the analysis are often carried out from relatively more powerful parties to weaker parties or between similar conventional forces. As an exception, North Korea and Iran's cyber-attacks against the United States can be mentioned. Given that North Korea possesses nuclear weapons and Iran's significant conventional power and capability, it appears that countries which apply the most cyber-attacks have a significant conventional capacity. For Iran, even it is possible to claim that it is one of the foremost conventional powers in Middle East since as Amir Lupovici points out, the main reason why the United States and Israel attacked with Stuxnet on Iran instead of a physical/conventional assault as did to Iraq or Syria, is the conventional deterrent posture of Iran. (2016, p. 334).

The main reason of relation between cyber-attacks and conventional capacity is because states with have relatively significant capacities do not believe the credibility of deterrence of weaker

states. Since, in case of an attempt of punishment by weaker victim state, conveniently stronger state can carry out conventional attacks through the right of escalating the crises. On the other hand, in case of the attacks between similar forces, the states cannot take the chance of starting a conflict with a similar force for cyber-attacks. Thus, in contrast to a widespread assumption in which even weaker states have the ability to intimidate powerful states due to asymmetric relations, as analysis shows that the characteristic features of cyberspace have become more useful for the conventionally powerful forces rather than weaker states. In conclusion, these facts reveal that *“not only effective defensive and offensive cyber capacity, but also conventional capacity is necessary to employ cyber deterrence.”*

When we continue the analysis through the type of attacks after the relationship of numbers of attacks, victim and suspected states, the following table has emerged:³⁹

Table 5.2: Types of Cyber-Attacks by Number

Confidentiality (222)		Integrity (16)		Availability (21)	
Espionage	Doxing	DDoS	Defacement	Sabotage	Data Destruction
220	2	16	2	14	5

Table 5.3: Suspected Actor, Type of Cyber Attacks Cross Tabulation

			Type of Cyber Attacks			Total
			Confidentiality	Integrity	Availability	
Suspected	China	Count	111	0	2	113
		% within Suspected	98,2%	0,0%	1,8%	100,0%
		% within Type	52,1%	0,0%	13,3%	45,4%
	Russia	Count	52	11	3	66
		% within Suspected	78,8%	16,7%	4,5%	100,0%
		% within Type	24,4%	52,4%	20,0%	26,5%
	Iran	Count	27	4	3	34
		% within Suspected	79,4%	11,8%	8,8%	100,0%
		% within Type	12,7%	19,0%	20,0%	13,7%
North Korea	Count	12	2	5	19	

³⁹ Table 9 consists of Israel and Denial response; however, in the Table 10; they are excluded in the analyses due to increase the frequency.

	% within Suspected	63,2%	10,5%	26,3%	100,0%
	% within Type	5,6%	9,5%	33,3%	7,6%
US	Count	11	4	2	17
	% within Suspected	64,7%	23,5%	11,8%	100,0%
	% within Type	5,2%	19,0%	13,3%	6,8%
Total	Count	213	21	15	249
	% within Suspected	85,5%	8,4%	6,0%	100,0%
	% within Type	100,0%	100,0%	100,0%	100,0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	42,571a	8	,000

When we examine the types of attacks, the attention is immediately drawn to the number of confidentiality (espionage + doxing) attacks. 222 of the 260 cyber-attacks (%85) targets the confidentiality of victim state. Within the confidentiality cyber-attacks, %99 are the espionage attacks. This ratio is the highest among the data obtained so far. Therefore, reviewing espionage attacks, which account for 84% of all cyber-attacks, can provide valuable clues about the reasons for the failure of cyber deterrence and the factors necessary for its success.

States mostly apply espionage attacks because espionage attacks are usually taking place in the grey areas where the boundaries are not clear, the actions are not legally criminalized but not welcomed. Also, to realize espionage attack is a very challenging task. Even if the attack is detected, it is a tough task to find who is the actor behind it. Even if actor is known, how should victim respond to the act of espionage? If the victim country responds with counterespionage, it may not be able to obtain same valued information in response. If the victim state decides to carry criminal charges, there is also a difficulty of judging the offenders, it is very challenging especially if it is carried out by foreigners. Secondly, the historically adopted perception by states in which espionage action is not a crime, but a political act of the state, makes it difficult to prevent espionage attacks. As stated by Martin Libicki, attacks that damage physically are treated as unacceptable by the states and response is given forcefully; vice versa, as acts of espionage, are perceived to be relatively acceptable because they do not directly damage the states (2017, pp. 1-2). For such reasons, espionage attack, which does not harm physically, but can cause severe damage in economic, political, military and so forth, has become the apple of the state's eye. In this context, it would not be wrong to claim that *“the espionage attacks are the most problematic type of attack for cyber deterrence.”*

Besides, 182 of the 222 confidentiality attacks, victim states did not respond to the suspected state or reveals any information if a response is ever given. This figure underlines two points which firstly, states have difficulty in responding to espionage attacks; secondly, they respond with different tools. Also, it is also evident that technologically and economically developed states could be disturbed by espionage attacks, given that 181 of the confidentiality cyberattacks carried out to US, EU and US allies, and they did or could not respond 150 of cyber-attacks.

For this reason, in recent years, the US and its ally countries have initiated to change the preconceived norms of cyber espionage attacks as they are not all acceptable. In this context, they stated that only the espionage actions to ensure the national security of the state were acceptable and that it was unacceptable if it was to be motivated by economic motivations to take advantage commercially (Clapper, 2013). This initiative is a good indicator of the fact that technologically and economically developed states such as the US and the EU are beginning to feel discomfort from espionage attacks. The US's attempt to prohibit espionage attacks- especially carried out with economic motivation- can also be evaluated by looking at the analysis.

Table 5.4: Most Suspected States and Their First Three Targets

	Their Target 1	Their Target 2	Their Target 3
China (114)	United States (55)	Asian Allies of US (36)	European Union (14)
Russia (54)	European Union (20)	United States (17)	West Sphere of Russia (9)
Iran (28)	Middle Eastern Allies of US (10)	United States (10)	Turkey (5)

Table 5.5: Suspected State- Sector Cross Tabulation

		Sector										Total
		Private Sector	Government	Military	Civil Society	P+G	P+M	P+C	G+M	G+C	G+P+C	
Suspected China	Count	33	23	8	5	23	5	4	9	2	3	115
	% within Suspected	28,7%	20,0%	7,0%	4,3%	20,0%	4,3%	3,5%	7,8%	1,7%	2,6%	100,0%
	% within Sector	46,5%	46,9%	53,3%	38,5%	47,9%	71,4%	100,0%	27,3%	100,0%	30,0%	45,6%

Russia	Count	20	20	2	7	10	1	0	5	0	1	66
	% within Suspected	30,3%	30,3%	3,0%	10,6%	15,2%	1,5%	0,0%	7,6%	0,0%	1,5%	100,0%
	% within Sector	28,2%	40,8%	13,3%	53,8%	20,8%	14,3%	0,0%	15,2%	0,0%	10,0%	26,2%
Iran	Count	11	3	1	0	7	0	0	7	0	6	35
	% within Suspected	31,4%	8,6%	2,9%	0,0%	20,0%	0,0%	0,0%	20,0%	0,0%	17,1%	100,0%
	% within Sector	15,5%	6,1%	6,7%	0,0%	14,6%	0,0%	0,0%	21,2%	0,0%	60,0%	13,9%
North Korea	Count	7	2	1	1	6	0	0	2	0	0	19
	% within Suspected	36,8%	10,5%	5,3%	5,3%	31,6%	0,0%	0,0%	10,5%	0,0%	0,0%	100,0%
	% within Sector	9,9%	4,1%	6,7%	7,7%	12,5%	0,0%	0,0%	6,1%	0,0%	0,0%	7,5%
US	Count	0	1	3	0	2	1	0	10	0	0	17
	% within Suspected	0,0%	5,9%	17,6%	0,0%	11,8%	5,9%	0,0%	58,8%	0,0%	0,0%	100,0%
	% within Sector	0,0%	2,0%	20,0%	0,0%	4,2%	14,3%	0,0%	30,3%	0,0%	0,0%	6,7%
Total	Count	71	49	15	13	48	7	4	33	2	10	252
	% within Suspected	28,2%	19,4%	6,0%	5,2%	19,0%	2,8%	1,6%	13,1%	0,8%	4,0%	100,0%
	% within Sector	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	90,368 ^a	36	,000

As shown above in the table, China is the most suspected in terms of carrying out cyber-attacks (44% of all) as well as espionage attacks. It is seen that 55 (or 48%) of the espionage attacks suspected by China are targeting the United States. In addition, it is observed that, 33 (60%) of these 55 attacks are targeting the private sector. This information is vital in terms of showing why the United States is concerned about economic motivation, particularly cyber espionage attacks by China. Furthermore, the claim that China is trying to close the gap in the fields where

fall behind, in particular, know-how, by cyber espionage attacks against leading companies of the US, can be confirmed with this data as well.⁴⁰

Also, when the time of economic espionage attacks between the two is examined, it can be easily predicted that the economic competition between the USA and China escalated especially in the 2010s. The number of espionage attacks increased dramatically particularly from 2010 to until 2015 when the agreement in which not to engage in cyber theft and cyber-attacks that target commercial institutions between the two countries, was signed. (Kopan, et al., 2015). While 9% of cyber-attacks occurred between 2005 and 2010, 63.6% of espionage attacks occurred between 2010 and 2015. Only in 2014, 30% of the espionage attacks occurred. Therefore, it is quite clear why the US strived to get such an agreement with China in 2015. Besides, there is a fact that the United States has few options instead of making such a deal. For instance, taken into consideration bringing legal proceedings against China under the current international law and China's permanent memberships of United Nations (UN) and its right to veto any UN's decisions, to deter China from espionage attacks is highly challenging for the US. However, if the US chooses to punish China by counter espionage attacks, there is a disadvantaged point: Although there is no obstacle for the US in terms of technical or capacity to carry out similar attacks, that attacks will not able to deter China. Since, as Libicki stated, China has the upper hand due to the fact that the US has more incomparably intellectual property than China has (2017, p.3). Unless this equilibrium change, the US is confined to lose cyber espionage war. In other words, the development gap creates an asymmetrical relationship between China and the US. For the very reason, while the United States aims to sit the diplomacy table with China to limit the activities of cyber espionages; on the other hand, China aims to reduce the reaction of developed countries against it and, to improve its image as a production hub in the international trade. Nevertheless, it is difficult to say that this agreement, which is the pioneer of the diplomatic initiatives about cyber-attacks that significantly reduce cyber-attacks between the two sides, has been working in absolute terms. Since 21% of the 33 attacks against the US private companies by China took place after the agreement. One of the main reasons for this result is that the agreement does not have any legal binding between two sides. Secondly, it is the fact that the state who has a gap with a rival in terms of economically, politically and technologically, does not give up the cyber-attacks so as to close that gap unless

⁴⁰ To see how China copied the blueprint of technological devices, the comparison between the new iPhone models and Chinese phone producers'(in particular Xiaomi and Huawei) products can be enough. For more major example, one can compare the similarities between F35 fighter jet and Shenyang J-31 fighter jet.

this situation creates a disadvantaged result for China. For these reasons, it is not wrong to assume that *in addition to political competition, if the economic competitiveness exists between the two states, the frequency and number of cyber-attacks increases which decreases the possibility of cyber deterrence.*

What about the other types of attacks? Is a cyber-attack that targets the integrity and availability is unacceptable in cyberspace as in four dimensions while confidentiality is not in the eyes of state in cyberspace as Libicki (p.2) stated? When looked for the cyber-attacks that targets the availability in order to find an answer, the following table shows up:

Table 5.6: Top Four Countries that Carry Out DDoS Cyber Attacks

	Their Target 1	Their Target 2	Their Target 3
North Korea (5)	South Korea (3)	United States 2	
Iran (3)	United States (2)	European Union (1)	
Russia (3)	Estonia (1)	Georgia (1)	European Union (1)
United States (3)	North Korea (2)	China (1)	
16 DDoS Cyber Attack by Sector			
Private Sector 6 + 2(Government)	Government 3+ 4(Military) +2 (Private Sector)	Military 1 + 4(Government)	

(The number after the + symbol indicates how many cyber-attacks are taken places together with the sector in parenthesis. For example, nine attacks are targeting the government, but four of these attacks target both government and military, and two of them target both government and private sector. This regulation aims to prevent overestimation of cyber-attacks.)

When the data are analyzed, it is seen that the within the 260 cyber-attacks, 16 of them targets the availability of the victim states. Also, all of 16 availability cyber-attacks are the Distributed Denial of Service (DDoS) which is generally taken into consideration as the least complicated forms of cyber-attacks (Brantly, 2018, p. 42). This is stemmed from the fact that the DDoS attacks can be conducted with relatively less technical knowledge⁴¹ and capacity than other types of cyber-attacks. However, even though it is a least complicated type of cyber-attack, it has a distinguished feature: As it was discussed in the second chapter, it is not known whether the cyber weapon will work in other situations and cases because cyber weapons are generally created according to founded vulnerabilities. Therefore, there is no guarantee that vulnerability

⁴¹ Even necessary programs to carry out DDoS attacks are easily findable on the Internet.

exists when it is decided to apply that cyber weapon. In contrast, DDoS attacks function as causing traffic on servers which results with stop or slow the servers rather than the vulnerabilities. Hence, *in the case of state or state-sponsored actors need to act and react quickly, they resort to DDoS attacks because its effects on the target can be visible, and the message can be given more directly.* For this reason, *in times of crisis or conflict, states often attempt to respond quickly and effectively to the opponents through making systems and computers inoperable by targeting availability with DDoS attacks.*

As an example, both patriotic Russian hackers' DDoS attacks to Estonia in 2007, and Georgia in 2008 can be mentioned. In both of these attacks, there was a political crisis between the two parties (even Georgia and Russia joined battle), and at least one of the parties aimed to give damage or message to the other party. For the cyber-attacks that target integrity and confidentiality, there is a necessity of previously detected vulnerability to employ cyber-attacks, but in case of crises, there is no time for the preliminary discovery. Hence, DDoS attacks that do not require the discovery of vulnerability but can slow or stop the systems and servers by creating lots of traffic were employed by Russia. Therefore, it can be alleged that *"the states conduct DDoS attacks in order to obtain easy, fast and effective results in a crisis."*

When we look at the other attacks in the data to strengthen this hypothesis, DDoS attack to US software company-GitHub- by Chinese government supported actors in 2015 is a striking example. When the relationship between time, suspected state, victim state and the case is analyzed; it is highly explicit that that attack was not a random attack. On 16 March 2015, the articles about the two pages of GitHub in which GreatFire (is an anti-censorship group who was providing alternative access to websites banned by the Chinese government) and Chinese language edition of New York Times, was published on Wall Street Journal (Bicchierai, 2015). Only one day after the publication of that article, (Dou & Barr , 2015) GitHub that hosts these two projects, faced massive DDoS attacks for five days (Smith, 2015) from Chinese servers. China was held responsible for this attack for two reasons which are: firstly, Chinese government were directly targeted by two projects; secondly, it is the fact that that kind of DDoS attack in which create massive traffic on servers of GitHub could not take place without being noticed by famous Great Firewall of China. So, without the permission of Chinese authorities, it was not possible to carry out that kind of massive attack.

After the confidentiality and availability attacks, the third type of cyber-attacks that target one of the essential elements of the cybersecurity; integrity, constitutes %8 (21/260) of all cyber-

attacks. The majority of the integrity attacks appears as sabotage attacks with the %66,66 (14/21) in data. In the eyes of states, sabotage attacks are perceived as cyber-attacks in which may have the most severe consequences. Since they have the capacity to break the integrity of the systems and computers, even in some cases, they can indirectly cause physical results by triggering the relation between virtual and real dimensions. Another reason is that, as Thomas Rid states, malicious software is ideal for the sabotage of industrial control systems, especially in critical infrastructures. (2013, p. 56). Therefore, cyber-attacks that damage the integrity are given more importance compared to confidentiality and availability attacks and they are considered as a national security problem. In addition, frequency of cyber-attacks is highly decreasing when the attacks target integrity because it requires relatively more technical knowledge and experience. This situation can be verified by data which shows that only %8 of all cyber-attack targets integrity.

When the 14 sabotage attacks in the 21 integrity attack were examined, Russia appears as the most suspected state in terms of conduction sabotage attacks by nine attacks that equal 64% of all sabotage attacks. Four of the nine (% 44, 4) suspected attack targeted western neighbor, Ukraine, who was politically engaged in a deep crisis and even on the brink of war with Russia. Actually, when considering the hypotheses that the cyberspace has become the place where the states continue their politics interest and activities and, war is getting hybrid pattern, it is not surprising that this kind of relationship emerged between the two neighboring countries since the ongoing crisis since 2014. It is also seen in the data that these five of nine attacks target the private sector, three governments and one civil society. Furthermore, Russia's sabotage attacks on private sectors are targeting private companies that are operating critical infrastructure, particularly in Ukraine's power grid.

The remaining three of the five sabotage attacks were carried out by the US and the remaining two by North Korea. While North Korea carried out one of the two attacks to South Korea and other against Taiwan; on the other hand, the United States targeted North Korea with two attacks and Iran with one. When the sector of targets of the US are analyzed, the striking point appears as that all the three sabotage attacks directed to the military of the victim states by the US. This rate of 100% is significant in terms of showing that the US has carried out sabotage attacks only with military motivation. Another remarkable point is that the two countries where a sabotage attack have been carried by the US, have had a military security problem by and against the United States. Given the fact that North Korea is in a position to challenge the United

States through advancing the range of its intercontinental ballistic missiles, and Iran is in a position to undermine the interests of the United States in Middle East through nuclear enrichment program and conventional capacity; it can be understandable why the main motivation of the US to carry out sabotage attacks is to prevent or interfere with the military development of the states which consider as a threat for its regional and international security.

If the attacks of Integrity are severe attacks for national security in the eyes of the states, how states respond to such acts?

Table 5.7: Response for Total 21 Integrity Cyber-Attacks that Targets Integrity

Unknown (11)	Denouncement (8)	Criminal Charges (0)	Sanction (2)
--------------	------------------	----------------------	--------------

Table 5.8: Response for Total 14 Sabotage Cyber-Attacks

Unknown (7)	Denouncement (5)	Criminal Charges (0)	Sanction (2)
-------------	------------------	----------------------	--------------

Table 5.9: Response for 219 Cyber-Attacks That Targets Confidentiality

Unknown (180)	Denouncement (31)	Criminal Charges (5)	Sanction (2)	Denial (1)
---------------	-------------------	----------------------	--------------	------------

According to the tables above, as the numbers of cyber-attacks that targeting the integrity increase, the possibility of states to respond increases as well. For instance, in general states responded to 17.8% of espionage attacks, 47.6 % of integrity attacks and 50 % of sabotage attacks. This situation confirms the assumption of Martin Libicki in which states can neglect espionage attacks because they do not contain physical violence while attacks that can cause physical violence are not tolerable, is concern of cyberspace as well (2017, pp. 1-2). In other words, *the violence in cyberspace is still not fully comprehended by states because the norm of violence in cyberspace is perceived same as in the other four dimensions and the uniqueness of the norm of violence in cyberspace has been ignored.* Thus, *to achieve cyber deterrence is difficult task not only because of technical elements but also with normative uncertainties about cyberspace.*

When we continue to examine all the 260 cyber-attacks included in the analysis through the responses of the states, the following table appears:

Table 5.10: Response for Total 260 Cyber-Attacks

Unknown (204)	Denouncement (42)	Criminal Charges (8)	Sanction (5)	Denial (1)
---------------	-------------------	----------------------	--------------	------------

As the table demonstrates, states have a problem in responding to cyber-attacks, or they respond with hidden paths. When we look at the cyber-attacks in which response is unknown against then, 179 of 204 cyber-attacks are espionage attacks. This situation demonstrates that the states have difficulty in identifying/confronting and have problems in responding to the espionage attack. As long as they do not give an appropriate response, it is not wrong to predict that the suspected states will continue to explore the boundaries of cyberspace. Hence, it can be argued that *the most challenging type of attack to deterrence for the states is espionage attacks as statistically indicated.*

On the other hand, states gave a response explicitly against victim states 55 times within 260 cyber-attacks. These 55 attacks are vital in regard with demonstrating in which conditions are necessary to ensure deterrence; how the attacker is identified in these attacks; and in which cyber-attacks are unacceptable for states. With 42 attacks in 55 attacks (81.81%, in general 16%), suspected states were denounced by the victim state.⁴² There are two main reasons why states choose denouncement: 1) States may have opted for denouncement because they do not know/can decide how to respond in cyberspace legally, but at least do not want to remain silent. 2) Even if the victim state can predict which state supports the attacking actor, however, victim state cannot have sufficient evidence to respond legally. In this kind of situation, the state can content itself with denouncement. Considering 30 of the 42 condemnation took place against espionage attacks, it is very likely that the two allegations mentioned above were possible.

Another important point is the relationship between denouncement decision and the target of the suspected state. According to data, the government and government institutions are targeted in the 66% of the responded attacks as seen in Suspected -Sector Cross Tabulation. This shows that as the rate of attack on the government increased, the reaction of the state increased with the same rate. In other words, in case of a cyber-attacks on the government in which state cannot respond in a legal, economic and political ways but also do not want to stay in silence as well,

⁴² Denouncement decision of state is obtained from the many different sources such as press releases of states and media. However, it is not known precisely whether the states respond secretly with a counter cyber-attack.

the states try to increase deterrence posture by demonstrating that state will not knuckle under to cyber-attacks.

When we look at another type of response against suspected states, criminal charges; there are only eight criminal charges as a response within 260 cyber-attacks (3%). Although it is quite difficult to put forward a general hypothesis with limited data, there are some remarkable factors are rising when analyzing the eight attacks. First of all, in all the cases of eight cyber-attacks, the victim state was the only the US. In other words, only the US has/can impose criminal sanctions after the cyber-attack. Due to all the eight criminal charges response are applied by the US, it is not wrong to ask that question specific to the US: What distinguish these eight attacks from the others in the eyes of the US? How the United States able to apply or impose penalties for these eight attacks while unable to others? The answers to these can be found by looking at the target sector of the attacks: Because seven of eight took aim at the major private companies of the US such as Boeing, Lockheed Martin, AMC Theatres, Bank of America, JP Morgan Chase, and one target the US Anti- Doping Agency.

This fact basically illustrates that when the cyber-attack damage the private companies that played a major role in the economy of the US, that attacks exceeds the threshold. An attack on such companies affects not only the customers of this company but the US state itself in the first place. Also, while an attack on the government or the military could be easily hidden by the state and these attacks could be responded to by other means in hidden ways; it is very difficult to hide cyber-attacks against companies that have a very important place in the international arena. For this reason, so as to prevent possible attacks against other institutions and companies in future, it is tried to assure the deterrence through increasing credibility of punishment threat via legal acts. Moreover, instead of directly blaming a state for an attack on private companies, it is always easier to regard non-state actors as responsible for the cyber-attacks even though there are limitations for the foreign actors. In this way, while legal actions against offenders are being taken, in the same way, the clear message is given to the country of the offenders. In short, when there is a violation by other states in the area which is secured by the states, the state responds with criminal or other means and tries to provide deterrence posture. On the contrary, if an attack took place within the unsecured area, states remain in silent according to data.

6. CONCLUSION

In the light of the first four chapters, firstly, it will be emphasized that how the perception of threat has changed throughout the recent past and why the cyber-attacks in the gray areas, especially cyber-espionage attacks, has become the greatest obstacles for the deterrence in cyberspace. Secondly, it will be addressed how the appropriate cyber deterrence strategy against exploiting gray areas of cyberspace, based on the strategies of the US against the Chinese economically motivated cyber espionage attacks in recent years. Lastly, this thesis is going to be concluded by underlying that although establishment of international cyber law is not possible soon; the implementation of the limited deterrence strategy and the increasing knowledge of each other as a result of increasing diplomatic initiatives, it is possible to construct widely accepted cyber norms and establishment of limited international cyber law.

At the beginning of the new millennium, the cyber-attacks that target the critical infrastructure were the most-feared cyber-attacks in the eyes of the states. In this way, states were developing policies to take precautions against the possible so-called cyber “Pearl Harbor” attacks. However, the recent years have demonstrated that although states have encountered complex and severe cyber-attacks that could cause unforeseen consequences both virtual and physical, and enough to prove the danger of cyber-attacks; the destructive cyber-attacks expected have not been materialized by states so far. Instead, states opt for limiting their cyber capacities and mostly tested their cyber-tools (Lewis, 2018, pp. 7-11). As an example of this situation, Ukraine- Russia relations can be mentioned since Ukraine has become a test lab of Russia for cyberwar since two countries get drawn into the conflict in 2014 (Greenberg, 2017). Moreover, Zengerle & Chiacu (2018) imply that the tested tactics and cyber weapons on Ukraine could be used against Western States in the future.

So, instead of devastating cyber-attacks; most of the cyber-attacks have taken place within the so-called grey area of cyberspace where the borders are not accurately determined, and cyber actions do not bring legal consequences for the offender. By not destructing but exploiting the grey areas, states try to pursue their more substantial interests by considering that opponents unable to respond with military options. With the increasing frequency of cyber-attacks and their negative impacts for the states in which widely wired to cyberspace and have intellectual properties to lose, those face the negative impacts of the grey areas rather than positive due to the asymmetrical structure of the cyberspace. In particular, economically motivated cyber

espionage has become troublesome for major industrial states. Thus, the primary efforts regarding cyber-attacks are made by those states to deter the espionage attacks more than ever.

So, even though espionage activities have employed by states over the centuries, why cyber espionage has become an unbearable activity by developed states today? This question is worthy of elaborately answering since the answer can guide us to find the most appropriate cyber deterrence strategy for cyber-attacks below the threshold. For this, we should first comprehend the historical transformation of espionage activities. In this respect, before the advent of computers, the most vital information would be securely guarded in locked storage of locked doors room of locked building behind the great high walls. However, with the advent of computers, the critical secrets have begun to be stored in the hard disk in the computers that generally have an internet connection because it allows working more efficiently and effectively than ever before due to quickly sending and receiving classified information across authorized persons (Singer & Friedman, 2014, p. 92). However, the networks of information are not as secure as imagined by the authorities. While storing in a hard disk is making it easier for analyzing the information across agents, on the other hand, it makes easier stealing of secret information by adversaries as well. Moreover, not only the states that have a high level of espionage satellites or airplanes but the states that have an internet connected computer can steal the secret of states. Thus, this situation has considerably reduced the cost of spying that traditionally a labor-intensive pursuit that carries the risk of arrest or worse and made further institutions viable targets (Timberg & Nakashima, 2013).

In addition, while states employing politically motivated espionage activities throughout the history in particular during the Cold War Era, with the advent of cyberspace, not an only scale of espionage increased, but also the form of espionage has been evolving from political motivations to economic motivations.⁴³ Therefore, all states who wish to support their industry may employ cyberespionage attacks to steal intellectual properties (IP) of major industrial states in order to boost their industries shortly. In this respect, Dmitri Alperovitch who was vice president of McAfee that antivirus and computer security software company, underlined that:

“I am convinced that every company in every conceivable industry with significant size and valuable intellectual property and trade secrets has been compromised (or will be shortly), with the great

⁴³ Even the political and economic motivations were emphasized as independent concepts, the reality is two concepts generally interlinked with each other. For instance, a economically motivated cyber attack can also be realized as a political motivation if it aims an strategic asset.

majority of the victims rarely discovering the intrusion or its impact. In fact, I divide the entire set of Fortune Global 2,000 firms into two categories: those that know they have been compromised and those that do not yet know” (Alperovitch, 2011, p. 2).

Since due to primary three reasons which are 1) there are state-run and state-affiliated corporations, 2) the fast and long-lasting economic development is necessary to the stability of its regime and 3) its poor record about cyber-activities; many parties have directly blamed China for the abusing cyber espionage attacks. In addition, it is believed that to sustain its economic growth, China needs a new industrial model in which focusing on increasing the value of products rather than assembling the products of foreign companies via cheap labor. Thus, it is feared that to make up the difference of intellectual properties (IP), China will apply heavily to cyber espionage to steal foreign companies’ intellectual properties (McBride & Chatzky, 2019). While the major industrial states have anxious about this situation, the “*Made in China 2025*” doctrine of China that is a state-led industrial policy which endeavors to make China predominant in global high-tech manufacturing by pursuing intellectual property acquisition to catch up and then surpass western technological developments in advanced industries through state subsidies (McBride & Chatzky, 2019), set off alarm bells for those states.

With this development, while espionage activities have been carried out mostly with economic motivation rather than political with the advent of cyberspace; ironically, cyber theft of intellectual properties through espionage activities has started to create global tensions and make espionage activities more political problem ever than before. Indeed, this tension has become visible in recent years between the Western States and China because although each cyber espionage case is not significant, with its accumulation, the impact of cyber espionage by China have begun to create an unbearable circumstance for major industrial states particularly for the United States. Hence, even an analogy between the oldest Chinese torture method “*Ling-chi*” known as “slow slicing” or “death by a thousand cuts” (Eldridge, 2019) was drawn Fallows, (2010) to imply that while one cyber espionage attack cannot create a fatal impact for state; however, continuous exploiting through cyber espionage attacks as Alperovitch (2011, p. 2) implies that could result in the “*historically unprecedented transfer of wealth*”. That is to say that when Western states have realized that China adapted the cyber version of *Ling-chi*, they try to find alternative strategies to dissuade China before to die from “the loss of blood”.

In this respect, as shown in the report entitled “*Summary of Cyber Strategy 2018*” published by the United States Department of Defense, exploitation of grey areas by states pose severe

problems that cannot be neglected anymore. In particular, the following statement in the report is noteworthy to illustrate that the United States is gravely disturbed by attacks which arise from grey areas and it no longer will tolerate these attacks: “*We will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict*” (U.S Department of Defense, 2018b, p. 1). Moreover, after the disinformation campaigns of Russia during the election process in both the US and Europe, the European Union stated that “*the EU will directly punish computer hackers after member countries agreed on a new mechanism to target individuals anywhere in the world, freezing their assets in the European Union and banning them from entry*” (Reuters, 2019). As these developments show that both the EU and the US try to deter future cyber-attacks below the threshold.

So, how the United States try to tackle the difficulties of cyber-attacks below the threshold? This question is noteworthy because the answer might give us some vital clues about one of the problematics of this thesis: How a classical deterrence theory can apply to cyberspace? In this context, the two strategies have come to the forefront: 1) Applying a restricting deterrence strategy instead of absolute deterrence strategy; 2) Applying hybrid deterrence strategy that consists of conventional political and economic tools.

Firstly, the United States has begun to consider cyber deterrence and nuclear deterrence as a different strategy because to consider cyberspace, and other four dimensions as a similar undermine the successful application of conventional deterrence to cyberspace. Since, as Uri Tor underlined that the classical deterrence theory was developed by the concept of the Cold War and as a natural result, the main issue was the threat of the existence of states via nuclear weapons. Therefore, any failure would lead to catastrophic results for both sides. However, while nuclear weapons compelled states to embrace the absolute deterrence approach, it does not embrace the absolute cyber deterrence because it is impossible to deter all cyber-attack (Tor, 2017, p. 93). Ben Buchanan also supports the restrictive deterrence strategy by underlying that no one type of deterrence meets the requirements to prevent all threats and actors but according to the source, seriousness and time of threats; different strategies of cyber deterrence should be employed (Buchanan, 2014, pp. 131-132). For instance, Chinese and Russian threats of attacks to the US's strategic computer networks are different in the eyes of the United States. While China is generally considered as a country that is overspecializing in terms of economically motivated cyber espionage to steal trade secrets and intellectual properties; on the other hand, Russia is considered as a launcher of attacks that cause political chaos in the Western World or

to target to financial organizations since their trade is relatively lesser than China. Thus, Buchanan is right when asserting that “*from an American Perspective, what deters China might not deter the Russians, and vice versa (2014, p. 133)*. In this respect, given efforts of the US against cyber-attacks below the threshold, particularly for Chinese espionage attacks, indeed, the United States has adopted a restrictive cyber deterrence strategy.

Secondly, the US not only use the cyber tools to respond to cyber espionage but political and economic tools due to the asymmetrical structure of the cyberspace. This mainly stems from the fact that China has the upper hand since the US has more incomparably intellectual property than others have (Tor, 2017, p.3). Therefore, the US is aware of the fact that unless this equilibrium change, the US is confined to lose cyber espionage war. This also points to a significant point about cyber deterrence: to limit the means of cyber-deterrence with a tool of cyberspace, even if it might be successful against some states, in general, it is doomed to fail. *Therefore, the cyber deterrence should adopt hybrid strategies in which consist of the tools in accordance with the sore point of the adversaries.* For instance, if the perpetrator of cyber-attack has limited physical tools capacity, the cyber deterrence should employ physical tools; if the aggressor is in a hard situation economically, cyber deterrence should consist of economic tools. That is the main logic behind the decisions of United States for instance while imposing a tariff on Chinese imports, on the other hand, tightening sanctions on Iran in terms of buying oil by ending exemptions from oil sanctions (Borger, 2019). This implies that the *state’s conventional and current strategies have come into existence in cyberspace as well. As our analysis in the fourth chapter proves that states maintain their similar political motivations in land, sea, air, and space in cyberspace as well.*

On the other hand, this situation also shows that *to mentioned about the cyber deterrence relations, there should be symmetrical relation between states.* For instance, If China and Russia would not have enough capacity to deter the US from applying kinetic tools, the US would apply different strategies. In addition, Estonia could not have deterred Russia through cyber deterrence strategies because, in case of a harsh retaliation by Estonia against Russia, Russia would have lowered the threshold and could escalate the crises or even turn crises into conflict. Thus, the relatively small and middle-sized states might have to carry balancing policies against great power as in the case of intervention of NATO such as the crises between Estonia and Russia. Under these circumstances, it can easily be seen why major powers do not lean towards international initiatives aiming to create international norms and rules unless they

find the exact boundaries maximizing their interests in cyberspace. Even though as shown by the report of the Center for Strategic and International Studies (CSIS), the grey areas of cyberspace are not only exploited by the great powers, but also small and middle-sized powers since grey areas apply to every state to the degree their interest; there is an imbalance between states since while one side is heavily exploiting, on the other hand, the other side is generally abused by and his trend is getting more visible in the international system.

However, there is the fact that no one immune from the disadvantageous situation because in the long run, advantages of exploiting can turn into a disadvantage by the increase of mutual damage. For instance, while the United States has biggest stones and living in the house that has the greatest plate-glass house; China also has big stones in its hands and living a plate-glass window (Menn, 2011). Therefore, even though China has got an advantageous position right now and applying cyber Ling-chi method, as a difference from the past, its every action not only slice the victim but the hands that but the hand that is holding a knife as well. Hence, how the United Kingdom abandoned the privateering in 1865 even though it heavily used in 17th and early 18th centuries since the other states France and the United States has also heavily used against Britain; in the same way, the states that exploit the cyberspace face a similar situation due to increasing mutual damage.

Therefore, since the cyber-attacks mostly carried out by political motivations, this situation may compel states to make concessions and to open road to diplomacy between states. In this sense, there seems to have been a significant increase in the number of diplomatic initiatives jointly carried out by states, organizations, and the private sector. For instance, the Group of Governmental Experts on Information Security (GGE) is a group of experts which had five summits between 2004 and 2017 under the auspice of the UN. This group sheds light on the applicability of international law and the Charter of the United Nations on cyberspace in order to develop some “*responsible norms of conduct*” in that domain. Accordingly, GGE aimed to facilitate cyber cooperation, develop more transparency, and lower the risk of incomprehension (SGDSN, 2018, p. 35). Secondly, while this failure of GGE seems to represent a missing consensus between states, it is not an end for states to build a cybersecurity framework in an international realm. Cyberspace related issues continue to be debated in many different inter-governmental structures such as UN, G20, G7, and Organization for Security and Co-operation in Europe (OSCE). Also, a very significant initiative was promoted by launching “*Appel de Paris*” (Paris Call for Trust and Security in Cyberspace). “*Appel de Paris*” tends to especially

emphasize a *high-level declaration on developing common principles for securing cyberspace* (France Diplomatie, 2018). By bringing together over 370 private, non-governmental, civil society organizations and states, the Paris Call constitutes a broad initiative based on the very idea of peace and cooperation between states and non-state actors in cyberspace. In this way, “Appel de Paris” can be regarded as a major step vis-à-vis “*cyber stability*” by its primary focus on the support of international norms such as responsible behaviors in cyberspace and the relevance of the probable applicability of international law into cyberspace. Last but not the least, Tallinn Manual 1.0 and 2.0 can also be named as one of the most successful initiatives for the international law regulation on cyberspace, led by NATO, private companies, and NGOs.

Besides, even though the number of initiatives and the participant states has been gradually increasing, it is not expected to establish the cyber international law norm widely accepted and binding every state soon due to three reasons which are:

1) States have the desire to exploit the cyberspace according to their interests; 2) The fear of tying their only own hands while others continue to exploit the cyberspace through ignoring the new international laws (Singer & Friedman, 2014, p. 186); 3) States have different priorities which aggravating to meet at common ground.

However, as the strategy of cumulative deterrence by Tor (2017, p. 93) underlines that just because one-time deterrence fails, it does not mean the next time will. In parallel to this idea, just because a diplomatic initiative fails, it does not mean the next one will fail also. Indeed, with the increasing dialogue between the parties in each meeting in the international arenas, the state can realize what the other state’s concern and interests. Even though for now states cannot agree on international norms or do not want to meet at a common ground due to their different priorities such as- US supports the legal regulations about restricting the economically motivated cyber espionage attacks (Menn, 2011); Russia tries to create an international norm on the cyber-attacks that targets critical infrastructure (Grigsby, 2018) and try to the disarmament of cyberweapons- however, with these dialogues, each state can calculate what the red lines of other states about the cyberspace in each meeting more clearly.

In this context, as the former director of the CIA, Michael Hayden asserted that “Norms could be established with accepted practices, not treaties” (Menn, 2011). In cyberspace, even though it is the low possibility to reach on a treaty, however, states might reach to a consensus on

general norms what acceptable and what is not even though it might take years. At the first agreements, the aim should be to create fundamental values and rules that all responsible states can agree. As *Deibert* (2011, p. 7) implies that:

“With those agreements, the aim is less about controlling certain classes of weapons, than it is about controlling expectations and developing a set of principles, rules, and procedures, and norms about how states behave with respect to an entire domain”.

Moreover, the possible treaty is not going to bring peace automatically in cyberspace. As *Singer & Friedman* (2014, pp. 191-192) point out that:

“Treaty will not mean every state will automatically adhere to it. Indeed, there has never been a law written that someone did not break. Rather, the strategy is to begin to set common definitions and understandings that can then be used to create norms to shape behavior. Until you establish the baseline of what everyone is supposed to follow, you cannot create incentives and rewards for following them and, in turn, identify and punish those who violate them.”

Besides, not only the disagreements would take place in this meeting, but also, they can find a mutual interest to agree on. Not every time interest of states clashes each other's, but sometimes states can have a common interest to protect. For instance, even though Great Britain, The Austro-Hungarian Empire, Russia, and Prussia had different interests and motivations, the results of Congress of Vienna were signed by four states.

In conclusion, cyber deterrence is a multi-dimensional concept that necessities are employing different tools rather than only cyber-tools because almost all the major cyber-attacks carried out through political motivations by states. Since all states act in different motivation and interest in cyberspace, to apply one common deterrence strategy regarded as unlikely. Instead, each state should develop restricted deterrence strategy against what mostly to deter as America focuses on cyber espionage rather than embracing absolute deterrence strategy against nuclear weapons during the Cold War. The restricted cyber deterrence also allows for states to understand what the red lines are of both itself and other parties. In this way, for what the reason the states are abstaining from the agreement or what their real interest in their proposals, might be understood in a better way with the restricted cyber deterrence strategy. Thus, a limited set of international cyber law rules that bindings to all those who are agreed might be established. For the states who are failing to cooperate might be isolated in the international systems and excluded from all process. Even sanctions can be imposed on those states. Besides, as the US promoted the states by declaring that all states that were waging war on Germany and Japan

would be a founding member of the United Nations, it is tried to convince those discordant states with reward. The long and short of it, *it is not possible to provide a deterrence strategy that completely halted all cyber-attacks; cyber deterrence is possible through international rules and norms that will reduce the excesses of cyber-attacks. That is to say that, only a hybrid model which not only consists of cyber tools, but also conventional and diplomatic channels should be applicable to achieve deterrence in cyberspace.*



BIBLIOGRAPHY

- Ablon, L., 2018 “Data Thieves the Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data. Santa Monica”, CA: RAND Corporation.
- Adams, J., 2001. “Virtual Defense”, *Foreign Affairs*, 80(3), pp.98-112
- Ahmad, R. & Yunus, Z., 2012 “The Application of Mixed Method in Developing a Cyber Terrorism Framework”. *Journal of Information Security*, 3(3), pp. 209-214.
- Alperovitch, D., 2011 “*Deterrence in Cyberspace: Debating the Right Strategy with Ralph Langer and Dimitry Alperovitch*” [Interview] (20 09 2011).
- Alperovitch, D., 2011 “*Revealed: Operation Shady RAT (White Paper)*”, Santa Clara, California: McAfee.
- Andersen, D. et al., 2004 “*Preliminary System Dynamics Maps of the Insider Cyber-Threat Problem*”
- Arquilla, J & Ronfeldt, D., 1996 “The Advent of Net War”, Santa Monica: California, RAND Corporation.
- Editorial Board of Economist ,2010 “A Worm in The Centrifuge”, *The Economist* [Online] Available at: <http://www.economist.com/node/17147818> [Accessed 12 January 2018].
- Arntz, P., 2018 “*Bank Robbers 2.0: Digital Thievery and Stolen Cryptocoins, Malwarebytes*”, [Online] Available at: <https://blog.malwarebytes.com/cybercrime/2018/02/bank-robbers-2-0-digital-thievery-stolen-cryptocoins/> [Accessed 24 10 2018].
- Arquilla, J. & Ronfeldt, . D., 1996 “*The Advent of Net War*”, Santa Monica, CA: RAND Corporation.
- Bajema, N. E., 2016 “Dr. Strangelove and Deterrence”, *Nuclear Spin Cycle*, August.1(1).
- Barrett, B., 2018 “*How China’s Elite APT10 Hackers Stole the World’s Secrets*”, [Online] Available at: https://www.wired.com/story/doj-indictment-chinese-hackers-apt10/?mbid=social_twitter&utm_brand=wired&utm_campaign=wired&utm_medium=socia [Accessed 21 12 2018].
- Baylis, J., 2008 “Uluslararası İlişkilerde Güvenlik Kuramı (The Concept of Security in International Relations)”, *Uluslararası İlişkiler*, Summer, 5(18), pp. 69-85.
- BBC News, 2014“*Edward Snowden: Leaks that exposed US spy programme*” [Online] Available at: <http://www.bbc.com/news/world-us-canada-23123964> [Accessed 09 January 2018].

- BBC News, 2018 “*US charges 'China government hackers'*”, [Online] Available at: <https://www.bbc.com/news/world-us-canada-46638323> [Accessed 04 03 2019].
- Behr, I. v., Reding, A., Edwards, C. & Gribbon, L., 2013 “*Radicalisation in the Digital Era: The Use of The Internet in 15 Cases of Terrorism and Extremism*”, Santa Monica, CA: RAND Corporation.
- Beidleman, L. S. W., 2009, “*Defining and Deterring Cyberwar*”, Carlisle, PA: Army War College.
- Bendiek, A. & Metzger, T., 2015, “Deterrence Theory in the Cyber- Century Lessons From a State of the Art Literature Review”, *German Institute of International and Security Affairs*, pp. 553-570.
- Betz, D. & Stevens, T., 2011, “*Cyberspace and the State Towards a Strategy for Cyber-Power*”, 1 ed. London: IISS/Routledge.
- Bıçakcı, S., 2014 “NATO’nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik. *Uluslararası İlişkiler*”, (Winter), 10(40), pp. 101-130.
- Bıçakcı, S., 2014 “*Protecting National Cyber Space and Recent Internet Regulations in Turkey*” [Interview] (14 04 2014).
- Bıçakcı, S., 2018, “*Kavram Avcıları: Siber Saldırı Nedir?*”, [Interview] (04 07 2018).
- Bicchierai, L. F., 2015, “*Did China Just Launch a Cyber Attack on GitHub?*”, [Online] Available at: https://motherboard.vice.com/en_us/article/pgawjn/did-china-just-launch-a-cyber-attack-on-github [Accessed 08 04 2019].
- Blackwell, J., 2011 “Deterrence at the Operational Level of War”, *Strategic Studies Quarterly*, pp. 30-51.
- Boebert, W. E., 2011 “*Proceedings of a Workshop on Deterring Cyberattacks*”, Washington DC: National Academies Press.
- Borger, J. & Beaumont, P., 2018 “*Syria: US, UK and France Launch Strikes in Response to Chemical Attack*”, [Online] Available at: <https://www.theguardian.com/world/2018/apr/14/syria-air-strikes-us-uk-and-france-launch-attack-on-assad-r> [Accessed 27 12 2018].
- Borger, J., 2019 “*US Toughens Stance on Iran, Ending Exemptions from Oil Sanctions*”, [Online] Available at: <https://www.theguardian.com/world/2019/apr/23/us-toughens-stance-on-iran-ending-exemptions-from-oil-sanctions> [Accessed 18 05 2019].

- Brantly, A. F., 2018 “The Cyber Deterrence Problem”, *10th International Conference on Cyber Conflict*, Tallinn, NATO CCD COE Publications, pp. 31-54.
- Breeden, A. & Rubin, A. J., 2015 “French Broadcaster TV5 Monde Recovers After Hacking”, [Online] Available at: <https://www.nytimes.com/2015/04/10/world/europe/french-broadcaster-tv5-monde-recovers-after-hacking.html> [Accessed 23 02 2019].
- Brodie, B., 1958 “*The Anatomy of Deterrence*”, Santa Monica, California: RAND Corporation.
- Brodie, B. et al., 1946 “*The Absolute Weapon*”, New York: Harcourt and Brace.
- Bruijne, M. d., Eeten, M. v. & Gañán, C. H., 2017 “Towards a New Cyber Threat Actor Typology A Hybrid Method for the NCSC Cyber Security Assessment”, Delft: Faculty of Technology, Policy and Management Delft University of Technology.
- Buchanan, B., 2014 “Cyber Deterrence Isn’t MAD; It’s Mosaic”, *Georgetown Journal of International Affairs International Engagement on Cyber IV*, pp. 130-140.
- Buchanan, B., 2016 “*The Cybersecurity Dilemma Hacking, Trust, and Fear Between Nations*”, New York: Oxford University Press.
- Buchanan, B. & Williams, R. D., 2018 “A Deepening U.S.-China Cybersecurity Dilemma”, *Lawfare*, 24 October, [Online] Available at: <https://www.lawfareblog.com/deepening-us-china-cybersecurity-dilemma>. [Accessed 18 01 2019].
- Campbell, J., 2015 “French TV Network TV5Monde 'Hacked by Cyber Caliphate in Unprecedented Attack' That Revealed Personal Details of French soldiers”, [Online] Available at: <https://www.independent.co.uk/news/world/europe/french-tv-network-tv5monde-hijacked-by-isis-hackers-in-unprecedented-attack-that-revealed-personal-10164285.html> [Accessed 15 03 2019].
- Cavelty, M. D., 2008 “*Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*”, New York, NY: Routledge.
- Cerulus, L., 2019 “How Ukraine Became a Test Bed for Cyberweaponry”, *Politico*, 14 February, [Online] Available at: <https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/> [Accessed 21 02 2019].
- Choucri, N., 2012 “*Cyberpolitics in International Relations*”, London: The MIT Press.
- Chrisafis, A. & Gibbs, S., 2015 “French Media Groups to Hold Emergency Meeting After Isis Cyber-Attack”, [Online] Available at: <https://www.theguardian.com/world/2015/apr/09/french-tv-network-tv5monde-hijacked-by-pro-isis-hackers> [Accessed 27 10 2018].

- Çiftçi, H., 2017 “Her yönüyle Siber Savaş (Cyber Warfare in All Aspects)”, 2 ed.: Türkiye Bilim ve Araştırma Kurumu (TUBİTAK) Popüler Bilim Kitapları.
- Çılan, Ç. A., 2013 “Sosyolojik Bilimlerde Kategorik Verilerle İlişki Analizi Kontenjans Tabloları Analizi (Analysis of Relationship Analysis with Categorical Data in Sociological Sciences)”, 2 ed. Ankara: Pagem Akademi.
- Clapper, J. R., 2013, “Statement by Director of National Intelligence James R. Clapper on Allegations of Economic”, Office of the Director of National Intelligence, [Online] Available at: <https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2013/item/926-statement-by-director-of-national-intelligence-james-r-clapper-on-allegations-of-economic-espionage> [Accessed 29 10 2018]
- Clark, D. D. & Landau, S., 2011, “Untangling Attribution”, *Harvard National Security Journal*, Volume 2, pp. 25-40.
- Critical Art Ensemble, 1994 “*The Electronic Disturbance*”, New York: Autonomedia,.
- Danilovic, V., 2001 “The Sources of Threat Credibility in Extended Deterrence”, *The Journal of Conflict Resolution*, 45(3), pp. 341-369.
- Davis, J., 2007 “Hackers Take Down the Most Wired Country in Europe”, *Wired*, 21 August [Online] Available at: <https://www.wired.com/2007/08/ff-estonia/> [Accessed 10 04 2019].
- Davis, J. H. & Harris, G., 2016 “Obama Considers ‘Proportional’ Response to Russian Hacking in U.S. Election”, [Online] Available at: <https://www.nytimes.com/2016/10/12/us/politics/obama-russia-hack-election.html> [Accessed 10 04 2019].
- Davis, J. H. & Sanger, D. E., 2015 “Obama and Xi Jinping of China Agree to Steps on Cybertheft”, [Online] Available at: <https://www.nytimes.com/2015/09/26/world/asia/xi-jinping-white-house.html> [Accessed 26 01 2019].
- Deibert, R., 2011 “Tracking the Emerging Arms Race in Cyberspace”, *Bulletin of the Atomic Scientists*, 67(1), pp. 1-8.
- Demchak, C. C. & Dombrowski, P., 2011 “Rise of a Cybered Westphalian Age”, *Strategic Studies Quarterly*, Spring, 5(1), pp. 32-61.
- Denning, D. E., 2001, “Activism, Hactivism, and Cyberterrorism: the Internet As a Tool for Influencing Foreign Policy”, in: J. Arquilla & D. Ronfeldt, eds. *Networks and Netwars: The Future of Terror, Crime, and Militancy*, Santa Monica, CA: RAND Corporation, pp. 239-288.

- Denning, D. E., 2015 “Rethinking the Cyber Domain and Deterrence”, *Joint Force Quarterly*, 77(2), pp. 8-15.
- Denning, D. E. & Strawser, B. J., 2017 “Active Cyber Defense: Applying Air Defense to the Cyber Domain”, in: G. Perkovich & A. E. Levite, eds. *Understanding Cyber Conflict: 14 Analogies*. Georgetown University Press, pp. 193-209.
- Denning, D. & Lee, R. M., 2018 “A *Primer Active Defense and "Hacking Back: A Primer"*, [Interview] (22 05 2018).
- Doffman, Z., 2019 “Israel Responds to Cyber Attack with Air Strike on Cyber Attackers in World First”, *Forbes*, 06 May, [Online] Available at: <https://www.forbes.com/sites/zakdoffman/2019/05/06/israeli-military-strikes-and-destroys-hamas-cyber-hq-in-world-first/#37564d1aafb5> [Accessed 06 05 2019].
- Dou, E. & Barr, A., 2015 “U.S. Cloud Providers Face Backlash from China’s Censors, The *Wall Street Journal*, 16 March, [Online] Available at: <https://www.wsj.com/articles/u-s-cloud-providers-face-backlash-from-chinas-censors-1426541126> [Accessed 08 04 2019].
- Downs, G. W., 1989 “The Rational Deterrence Debate”, *World Politics*, January, Volume 41, pp. 225-237.
- Dr. Strangelove*. 1964, [Film] Directed by Stanley Kubrick, Hawk Films.
- Dreyfus, S. & Assange, J., 1997 “*Underground: Tales of Hacking, Madness, and Obsession on the Electronic Frontier*”, Cotham Road, Kew: Mandarin.
- Editorial Board of CHIP, 2018 “*10 Security Tips to Know by Heart*. *CHIP*, October- December 22(05).
- Editorial Board of Economist, 2018 “Russia and China Hold the Biggest Military Exercises for Decades America Should Beware”, *The Economist*, 06 September [Online] Available at: <https://www.economist.com/europe/2018/09/06/russia-and-china-hold-the-biggest-military-exercises-for-decades> [Accessed 10 03 2019].
- Editorial Board of Encyclopedia Britannica, 2018 “*Privateer*”, [Online] Available at: <https://www.britannica.com/technology/privateer> [Accessed 12 05 2019].
- Egloff, F., 2017 “Cybersecurity and the Age of Privateering”, in: G. P. and & A. E. Levite, eds. *From Understanding Cyber Conflict: Fourteen Analogies*, Georgetown University Press, pp. 231-247.
- Eldridge, A., 2019 “*Cruel and Unusual Punishments: 15 Types of Torture*”, *Encyclopedia Britannica*, [Online] Available at: <https://www.britannica.com/list/cruel-and-unusual-punishments-15-types-of-torture> [Accessed 18 05 2019].

- Elliot, D., 2011 “Detering Strategic Cyberattack”, *IEEE Security & Privacy*, 9(5), pp. 36-40.
- Evans, M., 2015 “*Hackers Steal £650 Million In World's Biggest Bank Raid*”, [Online] Available at: <https://www.telegraph.co.uk/news/uknews/crime/11414191/Hackers-steal-650-million-in-worlds-biggest-bank-raid.html> [Accessed 21 10 2018].
- Falliere, N., 2010 “*Exploring Stuxnet’s PLC Infection Process*”, [Online] Available at: <https://www.symantec.com/connect/blogs/exploring-stuxnet-s-plc-infection-process>
- Falliere, N., Murchu, L. O. & Chien, E., 2011 “*W32.Stuxnet Dossier Version 1.4*, Symantec.
- Fallows, J., 2010 “Cyber Warriors” *The Atlantic*, March, [Online] Available at: <https://www.theatlantic.com/magazine/archive/2010/03/cyber-warriors/307917/> [Accessed 16 05 2019].
- Fenrich, K., 2008 “Securing Your Control Systems”, *Power Engineering*, February 112(2), pp. 44-51.
- Flake, H., 2013 “*Analogies, Piracy, Attribution, and the Law of Unintended Consequences*”, [Online] Available at: <http://addxorrol.blogspot.com/2013/06/analogies-piracy-attribution-and-law-of.html> [Accessed 15 02 2019].
- France Diplomatie, 2018 “*Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace*” [Online] Available at: <https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in> [Accessed 05 01 2009]
- Fred, S., 2015 “On Cyberwarfare”, *DCAF Horizon 2015 Working Papers*, pp. 12-16.
- Freedman, L., 2004 “*Deterrence*”, Cambridge: Polity Press.
- Freedom House, 2017, “*Manipulating Social Media to Undermine Democracy*”, [Online] Available at: <https://freedomhouse.org/report/freedom-net/freedom-net-2017> [Accessed 09 January 2018].
- Fruhlinger, J., 2017 “*What is Stuxnet, Who Created It and How Does It Work?*”, *Csoonline*, 22 August, [Online] Available at: <https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html> [Accessed 04 03 2019].
- Garthoff, R. L., 2003 “Estimating Soviet Military Intentions and Capabilities” in: G. K. Haines & R. E. Leggett, eds. *Watching the Bear: Essays on CIA's Analysis of the Soviet Union*. Langley, Va: Center for the Study of Intelligence, Central Intelligence Agency.

- Geers, K., 2010 “The Challenge of Cyber Attack Deterrence”, *Computer Law & Security Review*, May, 26(3), pp. 298-303.
- Geers, K., 2011 “Strategic Cyber Security” Tallinn: CCD COE Publication.
- Geist, E., 2015 “Deterrence Stability in the Cyber Age”, *Strategic Studies Quarterly*, Winter, 9(4), pp. 44-61.
- Gibbs, J. P., 1968, “Crime, Punishment, and Deterrence”, *The Southwestern Social Science Quarterly*, 48(4), pp. 515-530.
- Gibson, W., 1984 “*Neuromancer*”, New York: Ace Book.
- Gökçe, Y., 2017 “Active Cyber Defense as a Preemptive Self-Defense Measure” in: Y. Gokce, Ü. Tatar & A. V. Gheorghe, eds. *Strategic Cyber Defense : A Multidisciplinary Perspective (NATO Science for Peace and Security Series - D: Information and Communication Security)*, IOS Press, pp. 120 - 128.
- Goldstein, G.-P., 2013 “Cyber Defense from Reduction in Asymmetrical Information Strategies”, *Military and Strategic Affairs*, 12, 5(3), pp. 129-155.
- Golumbia, D., 2013 “*Cyberlibertarianism: The Extremist Foundations of Digital Freedom*”, Virginia Commonwealth University.
- Goode, L., 2015 “Anonymous and the Political Ethos of Hacktivism”, *Popular Communication*, January, 13(1), pp. 74-86.
- Goodman, W., 2010 “Cyber Deterrence Tougher in Theory than Practice?”, *Strategic Studies Quarterly*, 4(3). pp. 102-135
- Goździewicz, W., 2016 “*NATO Road to Cybersecurity*”, Kraków: The Kosciuszko Institute.
- Greenberg, A., 2017 “How an Entire Nation Became Russia's Test Lab for Cyberwar”, *Wired*, 20 June, [Online] Available at: <https://www.wired.com/story/russian-hackers-attack-ukraine/> [Accessed 17 05 2019].
- Grenoble, R., 2017 “Welcome to The Surveillance State: China’s AI Cameras See All. [Online] Available at: https://www.huffingtonpost.com/entry/china-surveillance-camera-big-brother_us_5a2ff4dfe4b01598ac484acc [Accessed 25 04 2019].
- Grigsby, A., 2018 “Russia Wants a Deal with the United States on Cyber Issues Why Does Washington Keep Saying No?” *Council on Foreign Relations*, 27 August [Online] Available at: <https://www.cfr.org/blog/russia-wants-deal-united-states-cyber-issues-why-does-washington-keep-saying-no> [Accessed 10 02 2019].

- Grossman, D., 2014 “Cyber Extortionists Pose Growing Threat to Tech Firms. [Online] Available at: <https://www.bbc.com/news/technology-28605975> [Accessed 10 03 2019].
- Han, A. K. & Çelikpala, M., 2016. Cybersecurity and Nuclear Powerplants” in Ülgen, S.& Kim, G. eds, *A Primer on Cyber Security in Turkey and the Case of Nuclear Power*, Centre for Economics and Foreign Policy Studies, pp. 52-68.
- Harknett, R. J., 1996 “Information Warfare and Deterrence”, *Parameters*, Autumn, 26(4), pp. 93-107.
- Harris, S., 2013 “*CISSP Certification Exam Guide*”, 6 ed., The McGraw-Hill Companies.
- Healey, J. & Jordan, . K. T., 2014 “NATO’s Cyber Capabilities: Yesterday, Today, and Tomorrow”, *The Atlantic Council*, September, [Online] Available at: http://www.atlanticcouncil.org/images/publications/NATOs_Cyber_Capabilities.pdf [Accessed 15 03 2019].
- Higgins, A., 2017 “Maybe Private Russian Hackers Meddled in Election, Putin Says” , *The New York Times*, 1 June, [Online] Available at: <https://www.nytimes.com/2017/06/01/world/europe/vladimir-putin-donald-trump-hacking.html> [Accessed 10 04 2019].
- Hobbes, T., & Macpherson, C. B. 1968 “*Leviathan*”, Harmondsworth, Penguin Books.
- Hobsbawm, E., 1995, “*The Age of Extremes: A History of the World 1914-1991*”, London: Abacus.
- Holling, C. S., 1973 “Resilience and Stability of Ecological Systems”, *Annual Review of Ecology and Systematics*, 11(4), pp. 1-23.
- Hollings, A., 2018 “*Hacking the F-35: Turning the Fighter’s Biggest Strength Into Its Biggest Weakness*”, [Online] Available at: <https://fightersweep.com/10783/hacking-the-f-35-turning-the-fighters-biggest-strength-into-its-biggest-weakness/> [Accessed 04 03 2019].
- Huth, P. K., 1999 “Deterrence and International Conflict: Empirical Findings and Theoretical Debate”, *Annual Review of Political Science*, (2), pp. 25-48.
- Hymas, C., 2018 “*China is Ahead of Russia as 'Biggest State Sponsor of Cyber-Attacks on the West*”, [Online] Available at: <https://www.telegraph.co.uk/technology/2018/10/09/china-ahead-russia-biggest-state-sponsor-cyber-attacks-west/> [Accessed 26 02 2019].
- Iasiello, E., 2014 “Is Cyber Deterrence an Illusory Course of Action?”, *Journal of Strategic Security*, Spring, 7(1), pp. 64-67.

- Internet World Stats, 2019, “World Internet Users and 2019 Population Stats”, [Online] Available at: <https://www.internetworldstats.com/stats.htm> [Accessed 03 04 2019]
- Ismail, N., 2017. “*All the World Wide Web’s a stage: Understanding the Actor in the Cyber Threat Landscape*”. [Online] Available at: <https://www.information-age.com/actor-cyber-threat-landscape-123465686/> [Accessed 21 02 2019].
- Jervis, R., 1979 “Deterrence Theory Revisited”, *World Politics*, January, 31(2), pp. 289-324.
- Jinghua, L., 2018 “A Chinese Perspective on the Pentagon’s Cyber Strategy: From Active Cyber Defense to Defending Forward”, *Lawfare*, 19 October, [Online] Available at: <https://www.lawfareblog.com/chinese-perspective-pentagons-cyber-strategy-active-cyber-defense-defending-forward> [Accessed 18 01 2019].
- Johnson, L., 2018 “*Automated Cyber Attacks Are the Next Big Threat: Ever Hear of ‘Review Bombing’?*”, [Online] Available at: <https://www.entrepreneur.com/article/325142> [Accessed 10 01 2019]
- Jordan, T. & Paul, T., 2004 “*Hactivism and Cyberwars: Rebels with a Cause?*”, London: Routledge.
- Jouinia, M., Rabaia, L. B. A., Aissab & Ben, A., 2014 “Classification of Security Threats in Information Systems”, *Procedia Computer Science*, Volume 32, pp. 489-496.
- Kang, T.-j., 2018 “What’s Behind North Korea’s New Internet Opening?”, *The Diplomat*, [Online] Available at: <https://thediplomat.com/2018/08/whats-behind-north-koreas-new-internet-opening/> [Accessed 10 04 2019].
- Kasapoğlu, C., 2017 “Cyber Security: Understanding the Fifth Domain”, *EDAM Cyber Policy Paper Series 2017/1* [Online] Available at: <http://edam.org.tr/wp-content/uploads/2017/10/besinciboyuten.pdf> [accessed 04 08 2018]
- Kaspersky Lab, 2017 “*Kaspersky Lab detects 360,000 new malicious files daily – up 11.5% from 2016*”, [Online] Available at: https://www.kaspersky.com/about/press-releases/2017_kaspersky-lab-detects-360000-new-malicious-files-daily [Accessed 05 05 2019].
- Kaspersky, E., 2017, “*The Man Who Found Stuxnet – Sergey Ulasen in the Spotlight*”, [Online] Available at: <https://eugene.kaspersky.com/2011/11/02/the-man-who-found-stuxnet-sergey-ulasen-in-the-spotlight/> [Accessed 10 January 2018].
- Kaufmann, W. W., 1956 “The Requirements of Deterrence”, in: W. W. Kaufmann, ed. *Military Policy and National Security*. Princeton, New Jersey: Princeton University Press, pp. 12-38.

- Kello, L., 2013. The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security*, Fall, 38(2), pp. 7-40.
- Kennedy, P. M., 2004, “*The Rise and Fall of British Naval Mastery*”, London: Penguin.
- Khazan, O., 2013 “Actually, Most Countries Are Increasingly Spying on Their Citizens, the UN Says”, *The Atlantic*, 6 June [Online] Available at: <https://www.theatlantic.com/international/archive/2013/06/actually-most-countries-are-increasingly-spying-on-their-citizens-the-un-says/276614/> [Accessed 2018 January 09].
- Klimburg, A., 2012, “*National Cyber Security Framework Manual*”, Tallinn: NATO CCD COE Publication.
- Knopf, J. W., 201, “The Fourth Wave in Deterrence Research”, *Contemporary Security Policy*, 31(1), pp. 1-33.
- Knopf, W. J., 2013, “*Rationality, Culture and Deterrence*”, Monterey, CA: Monterey Institute of International Studies.
- Kopan, T., Holmes, K. & Collinson, S., 2015 “*U.S., China say they won't engage in cybertheft*” [Online] Available at: <https://edition.cnn.com/2015/09/25/politics/us-china-cyber-theft-hack/index.html> [Accessed 10 04 2019].
- Kramer, F. D., Binnendijk, H. & Hamilton, D. . S., 2015 “*NATO's New Strategy: Stability Generation*”. Washington D.C: The Atlantic Council & Center for Transatlantic Relations.
- Kugler, R. L., 2009. Deterrence of Cyber Attacks. In: F. Kramer, S. H. Starr & L. Wentz, eds. *Cyberpower and National Security*. Washington, DC: Potomac Books, pp. 309-340.
- Lacoste, Y., 1998 “Coğrafya Savaşmak İçindir (La géographie, ça sert, d'abord, à faire la guerre), trans. Arayıcı, A., İstanbul: Özne Yayınları.
- Lasconjarias, G., 2017. Deterrence through Resilience: NATO, the Nations and the Challenges of Being Prepared; *Eisenhower Paper*, May, No 7, pp. 1-6.
- Lebow, R. N. & Gross, J., 1989 “Rational Deterrence Theory: I Think, Therefore I Deter”, *World Politics*, January 41(2), pp. 208-224.
- Lee, T. B., 2017 “*The WannaCry Ransomware Attack Was Temporarily Halted. But it's Not Over Yet*” [Online] Available at: <https://www.vox.com/new-money/2017/5/15/15641196/wannacry-ransomware-windows-xp> [Accessed 10 05 2019].
- Lemnitzer, J. M., 2014 “*Power, Law and the End of Privateering*”, Palgrave Macmillan UK.

- Levy, S., 2001 *“Hackers Heroes of the Computer Revolution”*, New York: Penguin.
- Lewis, J. A., 2018 *“Rethinking Cyber Security: Strategy, Mass Effect, and States”*. Lanham, Boulder, New York, London: Center for Strategy & International Studies; Rowman & Littlefield.
- Leyden, J., 2009, *“Russian politician: My assistant started Estonian cyberwar”*. [Online] Available at: https://www.theregister.co.uk/2009/03/10/estonia_cyberwarfare_twist/ [Accessed 10 03 2019].
- Libicki, M. C., 2009 *“Cyberdeterrence and Cyberwar”*, Santa Monica, CA: RAND Corporation.
- Lieberman, E., 2013 *“Reconceptualizing Deterrence: Nudging Toward Rationality in Middle Eastern Rivalries”*, New York: Routledge.
- Linnéll, J., 2016 *“Developing a Proportionate Responses to a Cyber-Attack”*, *Aalto University Publication Series Science + Technology*, No 3, Aalto University.
- Linnéll, J., 2017 *“Proportional Response to Cyberattacks”*, *Cyber, Intelligence, and Security*, June, 1(2), pp. 37-52.
- Lindsay, R., 2015 *“Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence Against Cyberattack”*, *Journal of Cybersecurity*, 1(1), pp. 53–67.
- Lindsay, R. J., 2013 *“Stuxnet and the Limits of Cyber Warfare”*, *Security Studies*, 22(3), pp. 365-404.
- Li, X., 2015 *“Regulation of Cyber Space: An Analysis of Chinese Law on Cyber Crime”*, *International Journal of Cyber Criminology*, 9(2), pp. 185-204.
- Lockie, A., 2017 *“The US just Dropped the 'Mother of All Bombs' on ISIS in Afghanistan — Here's What That Means”*, [Online] Available at: <https://www.businessinsider.com/what-is-moab-mother-of-all-bombs-2017-4> [Accessed 10 03 2019].
- Long, A., 2008 *“Deterrence. From Cold War to Long War: Lessons from Six Decades of RAND Research”*, Santa Monica: RAND Corporation.
- Lucas, R. G. J., 2013 *“Can There Be an Ethical Cyber War?”* in A. Lowther & P. A. Yannakogeorgos, eds., *Conflict and Cooperation in Cyberspace: The Challenge to National Security*. Boca Raton, Florida: Taylor & Francis.
- Lupovici, A., 2010, *“The Emerging Fourth Wave of Deterrence Theory—Toward a New Research Agenda”*, *International Studies Quarterly*, 54(3), pp. 705-732.

- Lupovici, A., 2016 “The “Attribution Problem” and the Social Construction of “Violence”: Taking Cyber Deterrence Literature a Step Forward”, *International Studies Perspectives*, 17(3), pp. 322-342.
- MacIsaac, D., 2016. Air Warfare, *Encyclopedia Britannica*, 18 July, [Online] Available at: <https://www.britannica.com/topic/air-warfare> [Accessed 17 04 2019].
- Maoz, Z., 2003 “The Mixed Blessing of Israel’s Nuclear Policy”, *International Security*, 28(2), pp. 44-77.
- Markoff, J. & Kramer, A. E., 2009 “U.S. and Russia Differ on a Treaty for Cyberspace”, *The New York Times*, 27 June, [Online] Available at: <https://www.nytimes.com/2009/06/28/world/28cyber.html> [Accessed 15 03 2019].
- Marmon, W., 2018, “Main Cyber Threats Now Coming From Governments as “State Actors”, *European Institute*, 12 December, [Online] Available at: <https://www.europeaninstitute.org/index.php/136-european-affairs/ea-november-2011/1464-main-cyber-threats-now-coming-from-governments-as-state-actors> [Accessed 12 02 2019].
- Mazarr, M. J., 2018 “*Understanding Deterrence. Santa Monica*”, CA: RAND Corporation.
- McBride, J. & Chatzky, A., 2019 “Is ‘Made in China 2025’ a Threat to Global Trade?”, *Council on Foreign Relations*, 13 May, [Online] Available at: <https://www.cfr.org/background/made-china-2025-threat-global-trade> [Accessed 15 05 2019].
- McCanles, M., 1984, “Machiavelli and the Paradoxes of Deterrence”. *Diacritics*, 14(2), pp. 11-19.
- McConnell, M., 2010 “Mike McConnell on How to Win the Cyberwar We’re Losing”, *The Washington Post*, 28 February, [Online] Available at: <http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html> [Accessed 10 02 2019].
- McCue, A., 2008 “*Beware the insider security threat*”, [Online] Available at: <https://www.techrepublic.com/blog/cio-insights/beware-the-insider-security-threat/> [Accessed 10 12 2018].
- McGuinness, D., 2017 “How a Cyber-Attack transformed Estonia” *BBC*, 27 April, [Online] Available at: <https://www.bbc.com/news/39655415> [Accessed 10 03 2019].
- Mearsheimer, J. J., 2017 “*Conventional Deterrence, Cornell Studies in Security Affairs*”, Ithaca, New York : Cornell University Press.

- Mearsheimer, J. J. & Walt, S. M., 2003 “Keeping Saddam Hussein in a Box”, *The New York Times*, 02 February, [Online] Available at: <https://www.nytimes.com/2003/02/02/opinion/keeping-saddam-hussein-in-a-box.html> [Accessed 2019 02 14].
- Meer, S. et al., 2017, “Deterrence of Cyber-Attacks in International Relations: Denial, Retaliation and Signaling”, *International Affairs Forum*, pp. 85-135.
- Menn, J., 2011 “Agreement on Cybersecurity Badly Needed”, *Financial Times*, 12 October, [Online] Available at: <https://www.ft.com/content/e595e568-f4dc-11e0-ba2d-00144feab49a> [Accessed 09 05 2019].
- Menn, J. & Thomas, L., 2015 “France Probes Russian Lead in TV5Monde Hacking: Sources”, [Online] Available at: <https://www.reuters.com/article/us-france-russia-cybercrime/france-probes-russian-lead-in-tv5monde-hacking-sources-idUSKBN0OQ2GG20150610> [Accessed 03 04 2019].
- Merriam Webster Online Dictionary, 2018 “Deter” [Online] Available at: <https://www.merriam-webster.com/dictionary/deter> [Accessed 10 11 2018].
- Merriam Webster Online Dictionary, 2019 “Cyberspace” [Online] Available at: <https://www.merriam-webster.com/dictionary/cyberspace> [Accessed 04 02 2019].
- Merriam-Webster Online Dictionary, 2019, “Extortionist”, [Online] Available at: <https://www.merriam-webster.com/dictionary/extortionist> [Accessed 12 05 2019].
- Miller, Z. J., 2015 “U.S. Sanctions North Korea Over Sony Hack”, *Time*, 02 January, [Online] Available at: <http://time.com/3652479/sony-hack-north-korea-the-interview-obama-sanctions/> [Accessed 10 04 2019].
- Mills, E., 2012 “Old-time Hacktivists: Anonymous, You've Crossed the Line”, *Cnet*, 30 March, [Online] Available at: <https://www.cnet.com/news/old-time-hacktivists-anonymous-youve-crossed-the-line/> [Accessed 24 02 2019].
- Morgan, P. M., 2003 “*Deterrence Now*”, Cambridge: Cambridge University Press.
- Morgan, P. M., 1977 “*Deterrence: A Conceptual Analysis*”, Beverly Hills, CA: Sage Publications.
- Morgenthau, H. J., 1960 “*Politics Among Nations: The Struggle for Power and Peace*”, New York: Alfred A. Knopf.
- Mudrinich, E. M., 2012 “Cyber 3.0: The Department of Defense Strategy for Operating Incyberspace and the Attribution Problem”, *Air Force Law Review*, Volume 68, pp. 167-206.

- Mulligan, G., 2017 “Has the Time Now Come For Internet Voting?”, [Online] Available at: <https://www.bbc.com/news/business-39955468> [Accessed 1 05 2019].
- Mumford, A., 2013 “Proxy Warfare and the Future of Conflict” *The RUSI Journal*, 158(2), pp. 40-46.
- National Coordinator for Security and Counterterrorism, 2018, “*Cyber Security Assessment Netherlands 2018*”, [Online] Available at: <https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-018.html> [Accessed 14 04 2019].
- NATO, 2017 “*Yeni Tehditler: Siber Boyut (New Threats: Cyber Dimension)*” [Online] Available at: <https://www.nato.int/docu/review/2011/11-september/Cyber-Threats/TR/index.htm> [Accessed 8 12 2018].
- NATO, 2018 “*Speech by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference*” [Online] Available at: https://www.nato.int/cps/en/natohq/opinions_154462.htm [Accessed 08 05 2019].
- Niekerk, B. v. & Maharaj, M. S., 2011 “Relevance of Information Warfare Models to Critical Infrastructure Protection”, *Scientia Militaria, South African Journal of Military Studies*, 39(2), pp. 99-122.
- Nye, J., 2010 “*Cyber Power*”, Cambridge: Belfer Center for Science and International Affairs.
- Nye, J. S., 2017 “Deterrence and Dissuasion in Cyberspace”, *International Security*, 41(3), pp. 44-71.
- Oxford Online Dictionary, 2019, “*Attribution*”. [Online] Available at: <https://en.oxforddictionaries.com/definition/attribution> [Accessed 10 02 2019].
- Oxford Online Dictionary, 2019, “*Credibility*” [Online] Available at: <https://en.oxforddictionaries.com/definition/credibility> [Accessed 01 02 2019].
- Oxford Online Dictionary, 2019 “*Cyberspace*” [Online] Available at: <https://en.oxforddictionaries.com/definition/cyberspace> [Accessed 04 02 2019].
- Payne, K., 2003 “The Fallacies of Cold War Deterrence and a New Direction”, *Comparative Strategy*, 22(5), pp. 411-428.
- Porter, C. & Jordan K., 2019 “Don’t Let Cyber Attribution Debates Tear Apart the NATO Alliance”, *Lawfare*, 24 February, [Online] Available at: <https://www.lawfareblog.com/dont-let-cyber-attribution-debates-tear-apart-nato-alliance> [Accessed 7 05 2019].

- Posey, B., 2017 “*Cyber-Extortion: Why It Works and How to Fight Back*”, [Online] Available at: <http://techgenix.com/why-cyber-extortion-works/> [Accessed 8 04 2019].
- Press, D. G., 2005 “*Calculating Credibility: How Leaders Assess Military Threats*”, New York: Cornell University Press.
- Prior, T., 2018 “Resilience: The ‘Fifth Wave’ in the Evolution of Deterrence”, in: O. Thränert & M. Zapf, eds. *Strategic Trends 2018: Key Developments in Global Affairs*. Zurich: Center for Security Studies (CSS), ETH Zurich, pp. 63-80.
- Quackenbush, S. L., 2011 “Deterrence Theory: Where Do We Stand?”, *Review of International Studies*, 37(2), pp. 741-762.
- Rasor, E. L., 2004 “*English/British Naval History to 1815: A Guide to The Literature*”, London: Praeger Publisher.
- Reuters, 2019 “*Days Before Elections, EU Approves New Cyber Sanctions Regime*”, [Online] Available at: <https://www.reuters.com/article/us-eu-cyber-idUSKCN1SN1FQ> [Accessed 17 05 2019].
- Reveron, D. S., 2012 “*Cyberspace and National Security*”, Georgetown University Press.
- Ridout, T., 2016 “Building a Comprehensive Strategy of Cyber Defense, Deterrence, and Resilience”, *The Fletcher Forum of World Affairs*, Summer, 40(2), pp. 63-84.
- Rid, T., 2012 “Deterrence Beyond the State: The Israeli Experience”, *Contemporary Security Policy*, 33(1), pp. 124-147.
- Rid, T., 2013 “*Cyber War Will Not Take Place*”, London: Hurst.
- Rid, T. & Buchanan, B., 2015 “Attributing Cyber Attacks”, *The Journal of Strategic Studies*, 38(1-2), pp. 4-37.
- Roberts, D., 2015 “Obama Imposes New Sanctions Against North Korea in Response to Sony Hack”, *The Guardian*, 02 January [Online] Available at: <https://www.theguardian.com/us-news/2015/jan/02/obama-imposes-sanctions-north-korea-sony-hack-the-interview> [Accessed 10 04 2019].
- Rogers, M., 2015 “The Importance of Partnership in Cyberspace”, *CYCON: International Conference on Cyber Conflict*, Tallinn.
- Rue, F. L., 2013 “*Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, United Nations General Assembly Human Rights Council, [Online] Available at:

- https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf [Accessed 04 05 2019]
- Rühle, M., 2015. Deterrence: What It Can (And Cannot) Do, *NATO Review*, [Online] Available at: <https://www.nato.int/docu/review/2015/Also-in-2015/deterrence-russia-military/EN/index.htm> [Accessed 20 12 2018].
- Ryan, N. J., 2018 “Five Kinds of Cyber Deterrence”, *Philosophy and Technology*, 31(3), p. 331–338.
- Schelling, T. C., 1960 “*The Strategy of Conflict*”, New York: Oxford University Press.
- Schelling, T. C., 1966 “*Arms and Influence with a New Preface and Afterword*”, New Haven: Yale University Press.
- Schmitt, M. N., 2017 “*Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*”, New York: NY: Cambridge University Press.
- Schreier, F., 201 “On Cyberwarfare”, *Dcaf Horizon 2015 Working Paper*, (7).
- Serhan, Y., 2018 “Macron’s War on ‘Fake News’”, *The Atlantic Council*, 06 January, [Online] Available at: <https://www.theatlantic.com/international/archive/2018/01/macrons-war-on-fake-news/549788/> [Accessed 09 January 2019].
- Secretary General for Defence and National Security of France (SGDSN), 2018, *Revue Stratégique de cyberdéfense (Strategic Review of Cyber Defence)*, [Online] Available at: <http://www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf> [Accessed 17 04 2019]
- Shakespeare, W., 2005 “*As You Like It Webster’s Thesaurus Edition for PSAT®, SAT®, GRE®, LSAT®, GMAT®, and AP® English Test Preparation*”. San Diego, CA: ICON Group International.
- Shaw, S. J. & Shaw, E. K., 1976 “*History of the Ottoman Empire and Modern Turkey: Volume I, Empire of the Gazis: The Rise and Decline of the Ottoman Empire 1280-1808*”, Cambridge: Cambridge University Press.
- Shea, J., 2016 “Resilience: A Core Element of Collective Defence”, *NATO Review*, [Online] Available at: <https://www.nato.int/docu/review/2016/also-in-2016/nato-defence-cyber-resilience/en/index.htm> [Accessed 10 05 2019].
- Simanjuntak, D. A., Ipung, H. P., Lim, C. & Nugroho, A. S., 2010. Text Classification Techniques Used to Facilitate Cyber Terrorism Investigation, *2010 Second International Conference on Advances in Computing, Control, and Telecommunication Technologies*. Jakarta, pp. 98-200.

- Singer, P. W. & Friedman, A., 2014 “*Cybersecurity and Cyberwar What Everyone Needs To Know*”, New York/Oxford: Oxford University Press.
- Smith, C., 2015 “*We Are Under Attack*”, [Online] Available at: <https://en.greatfire.org/blog/2015/mar/we-are-under-attack> [Accessed 09 04 2019].
- Snyder, G. H., 1961 “*Deterrence and Defense: Toward a Theory of National Security*” Princeton, New Jersey: Princeton University Press.
- Solomon, J., 2011. Cyber Deterrence Between Nation-States: Plausible Strategy or a Pipe Dream? *Strategic Studies Quarterly*, 5(1).
- Statista, 2018 “Internet of Things (IoT) Connected Devices Installed Base Worldwide From 2015 to 2025 (in billions)”, [Online] Available at: <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/> [Accessed 02 12 2018]
- Steiner, P., 1993 “*Cartoon*”. *The New Yorker*, 05 July, 69(21).
- Stern, E., 2011 “Retaliatory Deterrence in Cyberspace”, *Strategic Studies Quarterly*, 5(1), pp. 62-80.
- Sulmeyer, M., 2018 “How the U.S. Can Play Cyber-Offense Deterrence Isn't Enough”, *Foreign Affairs*, 22 April [Online] Available at: https://www.foreignaffairs.com/articles/world/2018-03-22/how-us-can-play-cyber-offense?cid=nlc-fa_fatoday-20180322 [Accessed 10 01 2019]
- Symantec, 2015 “*White Paper: The Cyber Resilience Blueprint: A New Perspective on Security*”, [Online] Available at: https://www.symantec.com/content/en/us/enterprise/white_papers/b-cyber-resilience-blueprint-wp-0814.pdf [Accessed 02 02 2019].
- Taddeo, M., 2018 “The Limits of Deterrence Theory in Cyberspace”, *Philosophy & Technology*, 31(3), p. 339–355.
- Taipale, K. A., 2009 “*Cyber-Deterrence: Law, Policy and Technology: Cyberterrorism, information, Warfare, Digital and Internet Immobilization*”, Center for Advanced Studies in Science and Technology Policy.
- Taylor, P. A., 2005 “From Hackers to Hacktivists: Speed Bumps on the Global Superhighway?”, *New Media & Society*, 7(5), p. 625–646.
- Tfoft, I. A., 2001. How the Weak Win Wars: A Theory of Asymmetric Conflict. *International Security*, 26(1). pp. 93-128

- The State Council Information Office of the People's Republic of China, 2015 "China's Military Strategy", [Online] Available at: http://english.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm [Accessed 10 03 2019].
- Thompson, H. & Trilling, S., 2018 "Cyber Security Predictions: 2019 and Beyond", *Symantec*, 28 November [Online] Available at: <https://www.symantec.com/blogs/feature-stories/cyber-security-predictions-2019-and-beyond> [Accessed 15 01 2019].
- Thucydides, 1998. *History of the Peloponnesian War*, trans. Jowett, Benjamin, Amherst, N.Y: Prometheus Books.
- Timberg, C. & Nakashima, E., 2013 "Chinese Cyberspies Have Hacked Most Washington Institutions, Experts say", *The Washington Post*, 20 February [Online] Available at: https://www.washingtonpost.com/business/technology/chinese-cyberspies-have-hacked-most-washington-institutions-experts-say/2013/02/20/ae4d5120-7615-11e2-95e4-6148e45d7adb_story.html?utm_term=.9f7e951acef2 [Accessed 10 05 2019].
- Tolga, İ. B., 2018 "*Principles of Cyber Deterrence and the Challenges in Developing a Credible Cyber Deterrence Posture*", Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.
- Tor, U., 2017 "Cumulative Deterrence' as a New Paradigm for Cyber Deterrence", *Journal of Strategic Studies*, 40(1-2), pp. 92-117.
- Townsend, K., 2018 "HoneyPot Shows the Power of Automation in the Hands of Hackers", *Security Week*, 18 April. [Online] Available at: <https://www.securityweek.com/honeypot-shows-power-automation-hands-hackers> [Accessed 26 01 2019].
- Tzu, S., 1963. "*The Art of War*", trans. Griffith, Samuel B., New York and Oxford: Oxford University Press.
- U.S. Department of Defense, 2011 "*2011 Department of Defense Strategy for Operating in Cyberspace*" [Online] Available at: <https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf> [Accessed 30 12 2018]
- U.S. Department of Defense, 2018 "*DOD Dictionary of Military and Associated Terms (June 2018)*", United States Joint Chiefs of Staff. [Online] Available at: <https://www.hsdl.org/?abstract&did=813130> [Accessed 10 02 2019].
- U.S. Department of Defense, 2018b "*Summary Department of Defense Cyber Strategy 2018*", [Online] Available at: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF [Accessed 30 12 2018]

- U.S. Department of Homeland Security, 2016, “Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security”, [Online] Available at: <https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national> [Accessed 10 04 2019].
- Ünver, A., 2018 “*Kavram Avçıları: Siber Saldırı Nedir?*”, [Interview] (13 08 2018).
- Vidalis, S. & Jones, . A., 2005 “Analyzing Threat Agents and Their Attributes”, *4th European Conference on Information Warfare and Security*, University of Glamorgan, pp. 369-380.
- Walt, S. M., 1991 “The Renaissance of Security Studies”, *International Studies Quarterly*, 35(2), pp. 211-239.
- Weber, M., 2008. Max Weber’s Complete Writings on Academic and Political Vocations, Dreijmanis, J., eds., Algora Publishing.
- Weimann, G., 2005 “Cyberterrorism: The Sum of All Fears?”, *Studies in Conflict & Terrorism*, 28(2), pp. 129-149.
- Wenger, A. & Wilner, A., 2012 “Deterring Terrorism: Moving Forward”, in: A. Wenger & A. Wilner, eds. *Deterring Terrorism: Theory and Practice*, Stanford, CA: Stanford Security Studies, pp. 301-324.
- Whitman, M. E. & Mattord, H. J., 2004 “*Management of Information Security*”, Course Technology.
- Winner, L., 1977 “*Autonomous Technology Technics out of Control as a Theme in Political Thought*”, Cambridge: MIT Press.
- Woods, E., 2019 “*The Role of Human Error in Successful Cyber Security Breaches*”, [Online] Available at: <https://blog.getusecure.com/post/the-role-of-human-error-in-successful-cyber-security-breaches> [Accessed 10 04 2019].
- Zengerle, P. & Chiacu, D., 2018 “*U.S. 2018 elections under attack by Russia: U.S. intelligence chief*”, [Online] Available at: <https://www.reuters.com/article/us-usa-security-russia-elections/u-s-2018-elections-under-attack-by-russia-u-s-intelligence-chief-idUSKCN1FX1Z8> [Accessed 17 05 2019].
- Zetter, K., 2011 “How Digital Detectives Deciphered Stuxnet the Most Menacing Malware in History” *Wired*, 07 November [Online] Available at: <https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/> [Accessed 10 04 2019].
- Zettter, K., 2014 “Hacker Lexicon: What Is An Air Gap?”, *Wired*, 12 August [Online] Available at: <https://www.wired.com/2014/12/hacker-lexicon-air-gap/> [Accessed 10 03 2019].

CURRICULUM VITAE

Personal Information

Name Surname : Atakan YILMAZ
Place and Date of Birth : Sinop/Merkez-12.02.1994

Education

Undergraduate Education : İstanbul University
Political Science and International Relations / 2012-2017

Anglo American University
International Relations and Diplomacy / 2015-2016

Graduate Education : Kadir Has University
International Relations / 2017-2019

Foreign Language Skills : English (Advanced)

Work Experience

2017- : Research Assistant
İstanbul Esenyurt University (Department of Political Science and
International Relations)

2015 : Internship at Administrative Affairs and Health Department
(July-August) North Cypriot Consulate General in İstanbul

2015 : Internship at Administrative Affairs
(April-May) Governorship of İstanbul

2014 : Internship at Teknosa Academy
September-October) TeknoSA Domestic and Foreign Trading Inc.

Contact:

Telephone : +90 539 858 07 80
E-mail Address : atknylmzz@gmail.com

APPENDIX A

A.1 260 CYBER ATTACKS WITH DETAILS

	Title of the Cyber Attack	Time	Response of Victim	Victims State	Suspected State	Type of Cyber Attack	Target Sector
1	Shamoon 2.0	1.12.2016	Unknown	MA ally of US- Saudi Arabia	Iran	Data destruction	Government
2	Compromise of Ukrainian banks	13.12.2016	Unknown	West Sphere of Russia - Ukraine	Russia	Data destruction	Private sector
3	Compromise of the Sands Casino	12.12.2014	Denouncement	United States	Iran	Data destruction	Private sector
4	Compromise of Saudi Aramco and RasGas	16.08.2012	Denouncement	MA ally of US- Saudi Arabia	Iran	Data destruction	Private sector
5	Flame	28.05.2012	Unknown	Iran	United States, Israel	Data destruction	Military, Private sector
6	Targeting North Korea's Reconnaissance General Bureau	30.09.2017	Unknown	North Korea	United States	DDoS	Government
7	Compromise of TV5 Monde	9.04.2015	Denouncement	EU 1-France	Russia	Defacement	Private sector
8	Defacement of Baidu	12.01.2010	Unknown	China	Iran	Defacement	Private sector
9	Fourth of July incident	8.07.2009	Denouncement	United States	North Korea	Denial of service	Government, Private sector
10	Targeting North Korea's Reconnaissance General Bureau	2017-09	Unknown	North Korea	United States	Denial of service	Government

11	Denial of service incident against media websites in Sweden	19.03.2016	Unknown	EU 1-Sweden	Russia	Denial service of	Private sector
12	Disruption of GitHub	27.03.2015	Unknown	United States	China	Denial service of	Private sector
13	Unresponsive computer networks in South Korea	20.05.2013	Unknown	Asian ally of US-South Korea	North Korea	Denial service of	Private sector
14	Attempted compromise of the BBC Persian TV service	14.03.2012	Unknown	EU 1-UK	Iran	Denial service of	Private sector
15	ITSecTeam	18.09.2012	Criminal charges	United States	Iran	Denial service of	Private sector
16	Denial of service attacks against U.S. banks in 2012–2013	18.09.2012	Criminal charges	United States	Iran	Denial service of	Private sector
17	Denial of service incident against South Korean and U.S. targets	9.04.2011	Unknown	United States	North Korea	Denial service of	Government, Military
18	Denial of service incident against South Korean and U.S. targets	9.04.2011	Unknown	Asian ally of US-South Korea	North Korea	Denial service of	Government, Military
19	Fourth of July incident	8.07.2009	Denouncement	Asian ally of US-South Korea	North Korea	Denial service of	Government, Private sector
20	Offensive cyber campaign against Georgia	13.08.2008	Denouncement	East Sphere of Russia-Georgia	Russia	Denial service of	Government
21	Estonian denial of service incident	16.05.2007	Denouncement	West Sphere of Russia-Estonia	Russia	Denial service of	Military, Government
22	Compromise of Chinese government computers	23.10.2007	Unknown	China	United States	Denial service of	Government, Military
23	Attack on the Syrian Air Force	4.10.2007	Unknown	The Russian ally in Middle East -Syria	Israel	Denial service of	Military
24	Compromise of the U.S. Anti-Doping Agency	4.10.2018	Criminal charges	United States	Russia	Doxing	Civil society
25	Compromise of Sony Pictures Entertainment	3.12.2014	Sanctions	United States	North Korea	Doxing	Private sector

26	Targeting of Westinghouse Electric Corporation	12.04.2018	Criminal charges	United States	Russia	Espionage	Private sector
27	Targeting of North Korean defectors and journalists	15.05.2018	Unknown	Asian ally of US-South Korea	North Korea	Espionage	Civil society
28	Targeting of German critical infrastructure sectors	7.06.2018	Denouncement	EU 1- Germany	Russia	Espionage	Private sector
29	Project Sauron	2016	Unknown	China	United States	Espionage	Government, Military
30	Compromise of an air-gapped German government network	28.02.2018	Denouncement	EU 1- Germany	Russia	Espionage	Government
31	RedAlpha	26.06.2018	Unknown	India	China	Espionage	Civil society
32	Targeting of congressional campaigns for the 2018 U.S. midterm elections	19.07.2018	Unknown	United States	Russia	Espionage	Government
33	Rocket Kitten	9.11.2015	Unknown	Eu 1-UK	Iran	Espionage	Government, Military
34	Rancor	26.06.2018	Unknown	Asian Ally of US-Singapore	China	Espionage	Government, Civil society
35	GhostNet	28.03.2009	Unknown	EU 1	China	Espionage	Government, Private sector
36	Targeting of organizations associated with trade activity with China	16.08.2018	Unknown	United States	China	Espionage	Government, Private sector
37	Targeting of foreign ministries	28.02.2018	Unknown	EU	Russia	Espionage	Government
38	Compromise of the German Foreign Office	16.03.2018	Unknown	EU 1- Germany	Russia	Espionage	Government
39	Targeting of a European defense agency	15.03.2018	Unknown	EU	Russia	Espionage	Government
40	Targeting of Japanese companies	22.04.2018	Unknown	Asian ally of US- Japan	China	Espionage	Private sector

41	Allanite			Unknown	United States	Russia	Espionage	Private sector
42	Nitro attacks	31.10.2011		Unknown	EU 1	China	Espionage	Government, Private sector
43	SabPub	16.04.2012		Unknown	United States	China	Espionage	Government
44	Winnti Umbrella	3.05.2018		Unknown	United States	China	Espionage	Private sector
45	Targeting of international sports federations	12.01.2018		Unknown	EU 1-UK	Russia	Espionage	Civil society
46	Compromise of a U.S. Navy contractor	8.06.2018		Unknown	United States	China	Espionage	Private sector
47	Targeting of AMC Theatres	6.09.2018		Criminal charges	United States	North Korea	Espionage	Private sector
48	Targeting of U.S. energy and other critical infrastructure sectors	15.03.2018		Sanctions	United States	Russia	Espionage	Private sector, Government
49	Targeting of Mammoth Screen	6.09.2018		Unknown	EU 1 -UK	North Korea	Espionage	Private sector
50	Targeting of U.S. defense contractors	6.09.2018		Criminal charges	United States	North Korea	Espionage	Private sector
51	Mustang Panda	15.06.2018		Unknown	United States	China	Espionage	Civil society
52	Targeting of financial and chemical organizations in Europe	19.06.2018		Unknown	West Sphere of Russia - Ukraine	Russia	Espionage	Private sector
53	Targeting of financial and chemical organizations in Europe	19.06.2018		Unknown	EU 1	Russia	Espionage	Private sector
54	Compromise of Australian National University	6.07.2018		Unknown	Asian ally of US-Australia	China	Espionage	Civil society
55	Targeting of chemical research and media organizations in Germany	12.07.2018		Unknown	EU 1- Germany	Russia	Espionage	Private sector

56	Targeting of the office of U.S. Senator Claire McCaskill	26.07.2018	Unknown	United States	Russia	Espionage	Government
57	Targeting of a Swiss federal agency	15.09.2017	Denouncement	EU 1	Russia	Espionage	Government
58	Lucky Cat	30.03.2012	Unknown	India	China	Espionage	Civil society, Private sector
59	Sneaky Panda	14.09.2012	Unknown	Asian allies of the US	China	Espionage	Private sector, Civil society
60	Sykipot	4.09.2013	Unknown	United States	China	Espionage	Private sector, Military
61	Leviathan	16.10.2017	Denouncement	Asian ally of US-The Philippines	China	Espionage	Government, Private sector
62	Bronze Butler	12.10.2017	Unknown	Asian ally of US- Japan	China	Espionage	Private sector
63	Operation Cleaver	2.12.2014	Unknown	Turkey	Iran	Espionage	Private sector, Government
64	Black Energy	3.11.2014	Unknown	East Sphere of Russia-Kazakistan, Kirgizistan	Russia	Espionage	Private sector, Government
65	DragonOK	10.09.2014	Unknown	Asian ally of US-Taiwan	China	Espionage	Private sector
66	APT 10	4.04.2017	Denouncement	United States	China	Espionage	Private sector, Government
67	Compromise of Kaspersky Labs	10.10.2017	Unknown	Russian Federation	Israel	Espionage	Private sector
68	Targeting of Chinese-language news websites	5.07.2017	Unknown	United States	China	Espionage	Civil society
69	Attempted compromise of email accounts associated with the UK Parliament	25.06.2017	Unknown	EU 1-UK	Iran	Espionage	Government
70	CopyKittens	25.07.2017	Unknown	MA allies of US- Saudi Arabia, Israel, Jordan	Iran	Espionage	Government, Private sector, Civil society

71	Hellsing	15.04.2015	Unknown	India	China	Espionage	Government
72	Targeting of U.S. electric companies	10.10.2017	Unknown	United States	North Korea	Espionage	
73	APT 33	20.09.2017	Denouncement	MA ally of US- Saudi Arabia	Iran	Espionage	Private sector
74	Targeting of Marco Rubio's presidential campaign	30.03.2017	Unknown	United States	Russia	Espionage	Civil society
75	Compromise of a Danish Ministry of Defense e-mail service	23.04.2017	Denouncement	EU 1-Denmark	Russia	Espionage	Military, Government
76	Compromise of the Czech foreign minister's computer	31.01.2017	Denouncement	West Sphere of Russia - Czech Rep.	Russia	Espionage	Government
77	Targeting of French presidential candidate Emmanuel Macron's campaign	26.04.2017	Unknown	EU 1-France	Russia	Espionage	Civil society
78	Magic Hound	15.02.2017	Unknown	MA ally of US- Saudi Arabia	Iran	Espionage	Government, Private sector
79	Hellsing	15.04.2015	Unknown	Asian ally of US-The Philippines	China	Espionage	Government
80	Winniti Umbrella	3.05.2018	Unknown	EU 1-UK	China	Espionage	Private sector
81	SabPub	16.04.2012	Unknown	India	China	Espionage	Government
82	WhiteBear	30.08.2017	Unknown	East Sphere of Russia-Uzbekistan	Russia	Espionage	Government, Private sector
83	Compromise of the Italian Ministry of Foreign Affairs	10.02.2017	Unknown	EU 1-Italy	Russia	Espionage	Government
84	Operation BugDrop	17.02.2017	Unknown	West Sphere of Russia - Ukraine	Russia	Espionage	Private sector
85	Axiom	24.09.2014	Unknown	EU 1	China	Espionage	Government, Private sector

86	Targeting of employees of companies that operate U.S. nuclear power plants	30.06.2017	Unknown	United States	Russia	Espionage	Private sector
87	Attempted compromise of Norwegian government networks	4.02.2017	Denouncement	EU 1- Norway	Russia	Espionage	Government, Military
88	Compromise of South Korean government computers (2016)	6.12.2016	Denouncement	Asian ally of US-South Korea	North Korea	Espionage	Military
89	Compromise of the Democratic National Committee	14.06.2016	Sanctions	United States	Russia	Espionage	Civil society
90	APT 12	3.09.2014	Unknown	Asian ally of US-Taiwan	China	Espionage	Private sector, Government
91	Black Energy	3.11.2014	Unknown	MA Ally of US-Israel	Russia	Espionage	Private sector, Government
92	OilRig	5.01.2016	Unknown	MA Allies of US- Israel, Saudi Arabia	Iran	Espionage	Government, Private sector, Civil society
93	Nitro attacks	31.10.2011	Unknown	United States	China	Espionage	Government, Private sector
94	Icefog	25.09.2013	Unknown	Asian ally of US- Japan	China	Espionage	Government, Military
95	Sykipot	4.09.2013	Unknown	United States	China	Espionage	Private sector, Military
96	Compromise of gaming companies	18.10.2016	Unknown	United States	China	Espionage	Private sector
97	Spear-phishing campaign against Google accounts in 2015	26.06.2016	Unknown	United States	Russia	Espionage	Government, Private sector, Civil society
98	Cloud Atlas	10.12.2014	Unknown	East Sphere of Russia-Kazakistan	Russia	Espionage	Government
99	Lazarus Group	1.02.2016	Unknown	United States	North Korea	Espionage	Government, Private sector
100	Mofang	15.06.2016	Unknown	United States	China	Espionage	Government, Private sector

101	RUAG espionage	23.05.2016	Unknown	EU 1-Switzerland	Russia	Espionage	Private sector
102	Operation Cleaver	2.12.2014	Unknown	United States	Iran	Espionage	Private sector, Government
103	DragonOK	10.09.2014	Unknown	Asian ally of US- Japan	China	Espionage	Private sector
104	Project Sauron	8.07.2016	Unknown	China	United States	Espionage	Government, Military
105	Compromise of entities involved in the China-Philippines territorial dispute	12.07.2016	Unknown	Asian ally of US-The Philippines	China	Espionage	Government, Private sector
106	Compromise of computer networks associated with diplomats, journalists, and others in South Korea	1.08.2016	Denouncement	Asian ally of US-South Korea	North Korea	Espionage	Government
107	Compromise of a mobile app used by Ukrainian artillery units	22.12.2016	Denial	West Sphere of Russia - Ukraine	Russia	Espionage	Military
108	APT 16	16.12.2016	Unknown	Asian ally of US- Japan	China	Espionage	Private sector
109	Attempted compromise of U.S. think tanks	9.11.2016	Unknown	United States	Russia	Espionage	Civil society
110	Unnamed Actor	13.04.2016	Unknown	Asian ally of US-Taiwan	China	Espionage	Civil society, Government
111	Duqu 2.0	10.06.2015	Unknown	Iran	Israel	Espionage	Government, Private sector
112	Chafer	7.12.2015	Unknown	Turkey	Iran	Espionage	Private sector
113	APT 3	23.06.2015	Unknown	United States	China	Espionage	Private sector
114	Emissary Panda	5.08.2015	Unknown	EU 1	China	Espionage	Government, Private sector
115	Targeting of the government of Thailand	24.11.2015	Denouncement	Asian ally of US- Thailand	China	Espionage	Government

116	APT 17	14.05.2015	Unknown	United States	China	Espionage	Government, Private sector, Civil society
117	Rocket Kitten	9.11.2015	Unknown	Turkey	Iran	Espionage	Government, Military
118	Equation Group	16.02.2015	Unknown	Russian Federation	United States	Espionage	Government, Military
119	Compromise of a Pentagon legacy system	4.06.2015	Denouncement	United States	Russia	Espionage	Military
120	Hellsing	15.04.2015	Unknown	United States	China	Espionage	Government
121	Targeting of South Korean actors prior to meeting of Donald J. Trump and Kim Jong-un	5.06.2018	Unknown	Asian ally of US-South Korea	China, Russia	Espionage	Government
122	Compromise of an unclassified network associated with the U.S. Joint Chiefs of Staff	28.07.2015	Unknown	United States	Russia	Espionage	Military
123	Compromise of Anthem	6.02.2015	Unknown	United States	China	Espionage	Private sector
124	Compromise of United Airlines	29.07.2015	Unknown	United States	China	Espionage	Private sector
125	Targeting of Ukrainian law enforcement and government officials	13.03.2015	Denouncement	West Sphere of Russia - Ukraine	Russia	Espionage	Military, Government
126	Compromise of the Seoul subway system	5.10.2015	Denouncement	Asian ally of US-South Korea	North Korea	Espionage	Government
127	Compromise of the Permanent Court of Arbitration's website	16.10.2015	Unknown	EU 1- Holland	China	Espionage	Government
128	Compromise of unclassified White House networks	7.04.2015	Unknown	United States	Russia	Espionage	Government
129	Attempted compromise of the Dutch organization investigating the crash of flight MH17	22.10.2015	Unknown	EU 1- Holland	Russia	Espionage	Government
130	Compromise of networks in the Saudi government ministries	21.05.2015	Unknown	United States	Iran	Espionage	Government, Military

131	Compromise of social media accounts of State Department officials	24.11.2015	Unknown	United States	Iran	Espionage	Government
132	Compromise of the networks at the German parliament (Bundestag)	29.05.2015	Denouncement	EU 1- Germany	Russia	Espionage	Government
133	Network compromise at the Australian Bureau of Meteorology	1.12.2015	Unknown	Asian ally of US-Australia	China	Espionage	Government
134	Project Sauron	2016	Unknown	Russia	United States	Espionage	Government, Military
135	DragonOK	10.09.2014	Unknown	Russian Federation	China	Espionage	Private sector
136	Compromise of U.S. Transportation Command Contractors	17.09.2014	Denouncement	United States	China	Espionage	Military, Private sector
137	Moafee	10.09.2014	Unknown	United States	China	Espionage	Private sector
138	Axiom	24.09.2014	Unknown	United States	China	Espionage	Government, Private sector
139	Operation BugDrop	17.02.2017	Unknown	EU 1- Austria	Russia	Espionage	Private sector
140	WhiteBear	30.08.2017	Unknown	EU 1-UK	Russia	Espionage	Government, Private sector
141	Black Energy	3.11.2014	Unknown	MA Ally of US-Israel	Russia	Espionage	Private sector, Government
142	Newscaster	28.05.2014	Unknown	MA Allies of US- Saudi Arabia, Israel	Iran	Espionage	Government, Military
143	APT 18	2.09.2014	Unknown	United States	China	Espionage	Government, Private sector, Civil society
144	Compromise of Community Health Systems	8.09.2014	Unknown	United States	China	Espionage	Private sector
145	Indictment of PLA officers	19.05.2014	Criminal charges	United States	China	Espionage	Private sector

146	Compromise of Boeing	12.07.2014	Criminal charges	United States	China	Espionage	Private sector
147	APT 12	3.09.2014	Unknown	Asian ally of US- Japan	China	Espionage	Private sector, Government
148	Equation Group	16.02.2015	Unknown	China	United States	Espionage	Government, Military
149	Compromise of U.S. Investigations Services	6.08.2014	Unknown	United States	China	Espionage	Private sector
150	Compromise of iCloud in China	21.10.2014	Unknown	United States	China	Espionage	Private sector
151	Saffron Rose	12.05.2014	Unknown	United States	Iran	Espionage	Military, Civil society
152	Compromise of the U.S. State Department	28.10.2014	Unknown	United States	Russia	Espionage	Government
153	Compromise of the U.S. Postal Service	9.11.2014	Unknown	United States	China	Espionage	Government
154	Regin	24.11.2014	Unknown	Iran	United States	Espionage	Government, Private sector
155	Regin	24.11.2014	Unknown	Russia	United States	Espionage	Government, Private sector
156	Putter Panda	10.06.2014	Unknown	United States	China	Espionage	Private sector, Government
157	APT 33	20.09.2017	Denouncement	Asian ally of US-South Korea	Iran	Espionage	Private sector
158	WhiteBear	30.08.2017	Unknown	Asian ally of US-South Korea	Russia	Espionage	Government, Private sector
159	Operation Cleaver	2.12.2014	Unknown	MA Allies of US- Saudi Arabia, Israel, Egypt	Iran	Espionage	Private sector, Government
160	Lotus Blossom	28.07.2014	Unknown	Asian allies of the US- Taiwan, Japan, The Philippines	China	Espionage	Military, Government

161	Attempted compromise of Ukrainian email accounts	9.12.2014	Denouncement	West Sphere of Russia - Ukraine	Russia	Espionage	Government, Military
162	Cloud Atlas	10.12.2014	Unknown	West Sphere of Russia-Czech- Belarus	Russia	Espionage	Government
163	OilRig	5.01.2016	Unknown	United States	Iran	Espionage	Government, Private sector, Civil society
164	Kimsuky	11.09.2013	Denouncement	Asian ally of US-South Korea	North Korea	Espionage	Government, Private sector
165	admin@338	31.10.2013	Unknown	United States	China	Espionage	Government, Private sector, Civil society
166	Mirage	11.12.2013	Unknown	Eu 1	China	Espionage	Government
167	Compromise of the Finnish Ministry of Foreign Affairs	1.11.2013	Unknown	EU 1	Russia	Espionage	Government
168	Rocket Kitten	9.11.2015	Unknown	MA Allies of US- Saudi Arabia, Israel, Egypt	Iran	Espionage	Government, Military
169	Project Sauron	8.07.2016	Unknown	Russian Federation	United States	Espionage	Government, Military
170	Sykipot	4.09.2013	Unknown	EU 1-UK	China	Espionage	Private sector, Military
171	Winnti Umbrella	3.05.2018	Unknown	Asian ally of US-South Korea	China	Espionage	Private sector
172	Icefog	25.09.2013	Unknown	Asian ally of US-South Korea	China	Espionage	Government, Military
173	Deep Panda	1.01.2013	Unknown	United States	China	Espionage	Private sector, Military
174	Compromise of EADS and ThyssenKrupp	25.02.2013	Unknown	EU 1- Germany	China	Espionage	Private sector
175	Compromise of the Indian Defense Research and Development Organization	13.03.2013	Denouncement	India	China	Espionage	Military

176	Team Spy Crew	20.03.2013	Unknown	West Sphere of Russia- Hungary- Belarus	Russia	Espionage	Government, Private sector
177	Anchor Panda	22.03.2013	Unknown	EU 1	China	Espionage	Government, Military
178	Compromise of Australian government agencies	27.05.2013	Unknown	Asian ally of US- Australia	China	Espionage	Government, Military
179	Compromise of unclassified U.S. Navy network	27.09.2013	Unknown	United States	Iran	Espionage	Military
180	Sneaky Panda	14.09.2012	Unknown	United States	China	Espionage	Private sector, Civil society
181	APT 10	4.04.2017	Denouncement	EU 1	China	Espionage	Private sector, Government
182	SabPub	16.04.2012	Unknown	EU 1	China	Espionage	Government
183	Compromise of Coca-Cola	4.11.2012	Unknown	United States	China	Espionage	Private sector
184	Lucky Cat	30.03.2012	Unknown	Asian ally of US- Japan	China	Espionage	Civil society, Private sector
185	Compromise of gaming companies	18.10.2016	Unknown	Russian Federation	China	Espionage	Private sector
186	Madi	17.07.2012	Unknown	MA Ally of US-Israel	Iran	Espionage	Government, Private sector
187	Lazarus Group	1.02.2016	Unknown	Asian ally of US-South Korea	North Korea	Espionage	Government, Private sector
188	Compromise of Oak Ridge National Laboratory	19.04.2011	Unknown	United States	China	Espionage	Government, Private sector
189	Shady RAT	3.08.2011	Unknown	United States	China	Espionage	Government, Military
190	Compromise of a Taiwanese political party	9.08.2011	Denouncement	Asian ally of US-Taiwan	China	Espionage	Government

191	Operation BugDrop	17.02.2017	Unknown	MA ally of US- Saudi Arabia	Russia	Espionage	Private sector
192	CopyKittens	25.07.2017	Unknown	United States	Iran	Espionage	Government, Private sector, Civil society
193	Nitro attacks	31.10.2011	Unknown	Asian allies of the US	China	Espionage	Government, Private sector
194	Duqu	26.10.2011	Unknown	Iran	Israel	Espionage	Military
195	Interference with NASA satellite Landsat 7	9.11.2011	Unknown	United States	China	Espionage	Government
196	Interference with NASA satellite Terra (EOS AM-1)	9.11.2011	Unknown	United States	China	Espionage	Government
197	Compromise of RSA SecureID tokens	19.03.2011	Unknown	United States	China	Espionage	Private sector
198	Compromise of the U.S. Chamber of Commerce	21.12.2011	Denouncement	United States	China	Espionage	Government
199	Operation Aurora	14.01.2010	Denouncement	United States	China	Espionage	Private sector
200	Compromise of the Indian Prime Minister's Office	14.01.2010	Denouncement	India	China	Espionage	Government
201	Night Dragon	25.01.2010	Unknown	United States	China	Espionage	Private sector
202	Compromise of three Australian mining companies	19.04.2010	Unknown	Asian ally of US- Australia	China	Espionage	Private sector
203	Shadow Network	6.04.2010	Unknown	United States	China	Espionage	Military, Government
204	WhiteBear	30.08.2017	Unknown	United States	Russia	Espionage	Government, Private sector
205	GhostNet	28.03.2009	Unknown	Asian allies of the US	China	Espionage	Government, Private sector

206	APT 33	20.09.2017	Denouncement	United States	Iran	Espionage	Private sector
207	Compromise of the office of Senator Ben Nelson	20.03.2009	Unknown	United States	China	Espionage	Government
208	Compromise of computers associated with the Joint Strike Fighter program	21.04.2009	Unknown	United States	China	Espionage	Military
209	Compromise of Indian military computers	5.05.2008	Unknown	India	China	Espionage	Military, Government
210	Compromise of U.S. presidential campaigns in 2008	4.11.2008	Unknown	United States	China	Espionage	Civil society
211	Compromise at NASA Kennedy Space Center	19.11.2008	Unknown	United States	China	Espionage	Government
212	Compromise of NASA network in Washington, DC	19.11.2008	Unknown	United States	China	Espionage	Government
213	Agent.btz	28.11.2008	Unknown	United States	Russia	Espionage	Military, Private sector
214	Targeting of U.S. National Laboratories	7.12.2007	Unknown	United States	China	Espionage	Government, Private sector
215	Compromise of National Defense University	12.01.2007	Unknown	United States	China	Espionage	Military
216	Secretary of defense email incident	22.06.2007	Unknown	United States	China	Espionage	Military
217	Compromise of German government networks	27.08.2007	Denouncement	EU 1-Germany	China	Espionage	Government
218	Compromise of French Defense Ministry website	9.09.2007	Unknown	EU 1-France	China	Espionage	Military
219	Attempted compromise of Australian and New Zealand government computers	12.09.2007	Unknown	Asian ally of US-Australia	China	Espionage	Government
220	Compromise at the Department of Homeland Security	24.09.2007	Unknown	United States	China	Espionage	Military

221	Compromise at the State Department	11.07.2006	Unknown	United States	China	Espionage	Government
222	Compromise of the Pentagon's NIPRNet	17.08.2006	Unknown	United States	China	Espionage	Military
223	Compromise at U.S. Naval War College	4.12.2006	Unknown	United States	China	Espionage	Military
224	Titan Rain	25.08.2005	Unknown	United States	China	Espionage	Military, Government
225	APT 10	4.04.2017	Denouncement	Asian allies of the US	China	Espionage	Private sector, Government
226	Allanite		Unknown	EU 1-UK	Russia	Espionage	Private sector
227	Leviathan	16.10.2017	Denouncement	United States	China	Espionage	Government, Private sector
228	Project Sauron	2016	Unknown	Iran	United States	Espionage	Government, Military
229	Duqu	26.10.2011	Unknown	Iran	Israel	Espionage	Military
230	APT 16	16.12.2016	Unknown	Asian ally of US-Taiwan	China	Espionage	Private sector
231	Chafer	7.12.2015	Unknown	MA Allies of US-Saudi Arabia, United Arab Emirates, Israel, Jordan, Iran	Iran	Espionage	Private sector
232	Compromise of gaming companies	18.10.2016	Unknown	Asian ally of US-South Korea	China	Espionage	Private sector
233	Bronze Butler	12.10.2017	Unknown	Asian ally of US-South Korea	China	Espionage	Private sector
234	Project Sauron	8.07.2016	Unknown	Iran	United States	Espionage	Government, Military
235	Rocket Kitten	9.11.2015	Unknown	Turkey	Iran	Espionage	Government, Military

236	Equation Group	16.02.2015	Unknown	Iran	United States	Espionage	Government, Military
237	OIRig	5.01.2016	Unknown	Turkey	Iran	Espionage	Government, Private sector, Civil society
238	Winnti Umbrella	3.05.2018	Unknown	Asian ally of US- Japan	China	Espionage	Private sector
239	Compromise of gaming companies	18.10.2016	Unknown	Asian ally of US-Taiwan	China	Espionage	Private sector
240	Black Energy	3.11.2014	Unknown	West Sphere of Russia - Ukraine-Belarus- Litvania	Russia	Espionage	Private sector, Government
241	Newscaster	28.05.2014	Unknown	United States	Iran	Espionage	Government, Military
242	Madi	17.07.2012	Unknown	United States	Iran	Espionage	Government, Private sector
243	Alleged Russian compromise of networking equipment	16.04.2018	Sanctions	EU 1 - UK	Russia	Sabotage	Private sector
244	Targeting of a chemical plant in Ukraine	11.07.2018	Unknown	West Sphere of Russia - Ukraine	Russia	Sabotage	Private sector
245	Compromise of computer networks associated with the 2018 Pyeongchang Winter Olympics	12.02.2018	Unknown	Asian ally of US-South Korea	Russia	Sabotage	Civil society
246	Bad Rabbit	24.10.2017	Denouncement	Turkey	Russia	Sabotage	Government
247	Compromise of Far Eastern International Bank	7.10.2017	Unknown	Asian ally of US-Taiwan	North Korea	Sabotage	Private sector
248	Alleged Russian compromise of networking equipment	16.04.2018	Sanctions	United States	Russia	Sabotage	Private sector
249	Compromise of cryptocurrency exchanges in South Korea	11.09.2017	Unknown	Asian ally of US-South Korea	North Korea	Sabotage	Private sector
250	Compromise the North Korean nuclear program	4.03.2017	Unknown	North Korea	United States	Sabotage	Military

251	A compromise causes a power outage in Kiev, Ukraine	20.12.2016	Unknown	West Sphere of Russia - Ukraine	Russia	Sabotage	Private sector
252	Compromise of a power grid in eastern Ukraine	23.12.2015	Denouncement	West Sphere of Russia - Ukraine	Russia	Sabotage	Private sector
253	Bad Rabbit	24.10.2017	Denouncement	Asian ally of US- Japan	Russia	Sabotage	Government
254	Stuxnet	22.07.2010	Denouncement	Iran	United States	Sabotage	Military
255	Compromise the North Korean nuclear program	March 2017	Unknown	North Korea	United States	Sabotage	Military
256	Bad Rabbit	24.10.2017	Denouncement	West Sphere of Russia - Ukraine	Russia	Sabotage	Government
257	APT 37	20.02.2018	Unknown	Asian ally of US-South Korea	North Korea		Government, Private sector
258	TempTick	5.06.2018	Unknown	Asian ally of US-South Korea	China		Government, Private sector
259	TempTick	5.06.2018	Unknown	Asian ally of US- Japan	China		Government, Private sector
260	Leafminer		Unknown	MA Allies of US- Saudi Arabia, Israel, Egypt	Iran		Private sector, Government