EFE DÜVEROĞLU

A COMPARATIVE ANALYSIS OF CRITICAL INFRASTRUCTURE CYBER SECURITY POLICIES:
BEST PRACTICES FROM THE US, EU AND TURKEY

Bilkent University 2020

A COMPARATIVE ANALYSIS OF CRITICAL INFRASTRUCTURE CYBER SECURITY POLICIES: BEST PRACTICES FROM THE US, EU AND TURKEY

A Master's Thesis

by
EFE DÜVEROĞLU

Graduate Program in
Energy Economics, Policy, and Security
İhsan Doğramacı Bilkent University
Ankara
June 2020

A COMPARATIVE ANALYSIS OF CRITICAL INFRASTRUCTURE CYBER SECURITY POLICIES: BEST PRACTICES FROM THE US, EU AND TURKEY

The Graduate School of Economics and Social Sciences
of
İhsan Doğramacı Bilkent University

by

EFE DÜVEROĞLU

In partial fulfillments of the Requirements for the Degree of
MASTER OF ARTS IN ENERGY ECONOMICS, POLICY & SECURITY

GRADUATE PROGRAM IN
ENERGY ECONOMICS, POLICY AND SECURITY
İHSAN DOĞRAMACI BİLKENT UNIVERSITY
ANKARA

June 2020

I certify that I have read this thesis and have found that it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Energy Economics, Policy, and Security.

Assoc. Prof. Dr. Özgür Özdamar
Supervisor

I certify that I have read this thesis and have found that it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Energy Economics, Policy, and Security.

Assoc. Prof. Dr. Serdar Güner
Examining Committee Member

I certify that I have read this thesis and have found that it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Energy Economics, Policy, and Security.

Assoc. Prof. Dr. Pınar İpek
Examining Committee Member

Approval of the Graduate School of Economics and Social Sciences

Prof. Dr. Halime Demirkan
Director

ABSTRACT

A COMPARATIVE ANALYSIS OF CRITICAL INFRASTRUCTURE CYBER SECURITY POLICIES: BEST PRACTICES FROM THE US, EU AND TURKEY

Düveroğlu, Efe

M.A., Program in Energy Economics, Policy and Security
Supervisor: Assoc. Prof. Dr. Özgür Özdamar

June 2020

Critical infrastructures are the physical and virtual systems forming the basis of modern societies and they are essential in ensuring national prosperity. Even though the importance of such infrastructures could not be grasped by states and international organizations in the beginning, an increasing number of cyber threats targeting critical infrastructure systems is becoming the reason behind the acceleration of the engagement of critical infrastructure protection as an agenda item as seen in the United States and the European Union. In Turkey, the field of critical infrastructure policy is still in its infancy. This thesis compares the developments of critical infrastructure security in the United States, the European Union and Turkey through an investigation of definitional, legal, institutional and economic practices relating to critical infrastructure. While doing so, this thesis aims to reveal Turkey's current status in the field of critical infrastructure protection. In this regard, this thesis also analyzes how successful critical infrastructure security policies have been in Turkey. According to the findings of this thesis, Turkey is far behind the United States and the European Union in the field as a result of institutional and legal gaps that prevent the development of infrastructure protection. The policy initiatives which Turkey has to pursue are also discussed in the thesis.

Keywords: Comparative Analysis, Critical Infrastructure Protection, Cyber Security, Policy Success Analysis

ÖZET

KRİTİK ALTYAPI SİBER GÜVENLİK POLİTİKALARININ KARŞILAŞTIRMALI ANALİZİ: ABD, AB VE TÜRKİYE'DEN EN İYİ UYGULAMALAR

Düveroğlu, Efe

Yüksek Lisans, Enerji Ekonomisi ve Enerji Güvenliği Politikaları Programı
Tez Danışmanı: Doç. Dr. Özgür Özdamar

Haziran 2020

Kritik altyapılar, modern toplumların temelini oluşturan fiziksel ve sanal sistemlerdir ve ulusal refahı sağlamak için gereklilerdir. Bu tür altyapıların önemi önceleri devletler ve uluslararası organizasyonlar tarafından anlaşılamamasına rağmen kritik altyapı sistemlerini hedef alan siber tehditlerin artması, Amerika ve Avrupa Birliği'nde olduğu gibi kritik altyapıların korunmasının bir gündem maddesi olarak ele alınmasının hızlanmasına neden olmaktadır. Türkiye'de ise bu alanın gelişimi konusu sessizliğini korumaktadır. Bu tez Amerika, Avrupa Birliği ve Türkiye'deki kritik altyapı güvenliği konusundaki gelişmeleri bu bağlamda tanımlayıcı, yasal, kurumsal ve ekonomik uygulamaları araştırarak karşılaştırmaktadır. Bunu yaparken, bu tez, Türkiye'nin kritik altyapı koruması alanındaki mevcut durumunu ortaya koymayı amaçlamaktadır. Bu bağlamda tez, Türkiye'deki kritik altyapı güvenlik politikalarının politika başarısını da analiz etmektedir. Tez bulgularına göre, Türkiye, altyapılarının korunması konusunun gelişimini etkileyen kurumsal ve yasal boşluklar nedeniyle Amerika ve Avrupa Birliği'nden bu alanda çok geridedir. Bu bağlamda, Türkiye'nin izlemesi gereken politika girişimleri de tezde tartışılmıştır.

Anahtar Kelimeler: Karşılaştırmalı Analiz, Kritik Altyapıların Korunması, Politika Başarı Analizi, Siber Güvenlik

ACKNOWLEDGEMENTS

First and foremost, I would like to express my sincere gratitude to my advisor Assoc. Prof. Dr. Özgür Özdamar for his patience, motivation and guidance which were invaluable throughout writing this thesis. I could not imagine having a better mentor for this process. I also extend my grateful thanks to the dissertation committee members Assoc. Prof. Dr. Serdar Güner and Assoc. Prof. Dr. Pınar İpek for being on my thesis committee and for their priceless comments.

I would like to express my appreciation to my dear friends Berke Çaplı and Altay Özen for their insightful support on this project and helpful contributions. I would also like to extend a heartfelt thanks to Buse Dingiltepe for encouraging me to take initiative in my academic pursuits and always standing by me patiently.

Last but not least, I would like to express my heartfelt gratitude, regard and appreciation to my family, who has always supported and understood my academic endeavors. None of this would have been possible without them.

TABLE OF CONTENTS

LIST OF TABLES

CHAPTER I

INTRODUCTION

1.1 Prologue

Critical infrastructure systems form the basis of modern societies and they are essential to maintain national prosperity. Even though the scope of the critical infrastructure systems is varying, such systems generally include agriculture, water, power grid, transportation, communication and technology systems, and various public and private sectors. These sectors are essential to ensure the continuation of daily life. Critical infrastructure represents the complex systems which have become highly interconnected and interdependent. Even a failure of only one piece of the infrastructure causes the failure of other dependent systems, that can in turn affect the infrastructure in which the failure occurs. In such an environment, resilience and security of infrastructure becomes a national priority because when there is any damage or disruption of the services or operations critical infrastructure provides, there can potentially be hazardous effects to states' security, economy and also prosperity of citizens.

Critical infrastructure security mainly goes together with cyber-security. In a short period of time, cyber-attacks on critical infrastructure sectors, especially energy related sectors, have been increasing. The causes are most often, a shut-down of systems, a disruption of services and operations or allowing cyber-attackers to remotely control the affected systems. For instance, in 2003, the United States was faced with the three cyber-attacks which each targeted completely different critical infrastructure systems. While on August, the Northeastern part of the United States and Ontario province experienced a widespread power outage as a result of a software bug in the systems of electricity companies (Minkel, 2008), in the same month, “the computer worm infected the computer network of the Davis-Besse nuclear power plant operated in Ohio and rendered the plant’s monitoring systems inoperable for almost 5 hours” (Karanacak, 2011: 4). In October, the computer system of Houston, one of the busiest ports in the country, was attacked and the cyber-attack was done by a computer in the United Kingdom (Karabacak, 2011). The cyber-attacks on the United States’ critical infrastructure systems have continued. For instance, in 2013, the damage on such systems caused by a cyber-attack on the Silicon Valley’s power substation (Martinez, 2014). Whereas these examples refer the physical damage on infrastructure, the United States intelligence brought up that Russia may have used cyber ways to affect the outcome of 2016 American presidential election and it remains as a controversial claim.

Cyber-attacks on critical infrastructure were not only directed at the United States, but almost every country in the world is exposed to such a threat. In 2007, Estonia was subject to cyber-attacks, which lasted twenty-two days and targeted federal agencies including Estonian parliament, ministries, banks and media centers, as a result of political contention with Russia over the Soviet-era statue in Tallinn (Ottis, 2007). Ukraine is another European country that faced the wide-ranging cyber-attack on power grids in 2015. The cyber-attackers, which were conducted by computers in Russia, targeted the information systems of energy distribution companies and cut of the important amount of electricity flow for almost 6 hours (Zetter, 2016). While a several cyber-attacks continued in the Ukraine in 2017 that mainly affected the government agencies, financial and media institutions and specifically electricity suppliers, similar attacks on infrastructures were reported at same year also in Australia, France, Germany, Italy, Poland, Russia, the United Kingdom and the United States (Perlroth et al., 2017). Although it is not reported frequently, Turkey is also in danger of cyber-attacks that target critical infrastructure. For example, while in 2003, Batman Dam's computers were locked by a German company and due to this attack the company could not receive its payment, the computer virus named Conficker, that spread to the computer systems of many countries on January 2009, which also affected the Atatürk Airport's systems (Karabacak, 2011). In addition to these, towards the end of 2019, there was an unknown cyber-attack, particularly "a distributed denial of service" (DDoS) attack. A DDoS is a cyber-attack that aims to temporarily or indefinitely disrupt the services of a systems connected to the internet, in order to a computed or the network resources cannot be accessed by actual users. This DDoS attack targeted the banking and telecommunication sectors in Turkey.

Cyber threats against the critical infrastructure systems are forecasted to increase over the following years. Especially, western governments have seriously started to focus on the field of critical infrastructure protection through taking progressive steps in legal, administrative, and institutional areas. Even though critical infrastructure security is one of the most significant agenda items of developed countries, this field is not even discussed properly in Turkey. Even securing critical infrastructures is a crucial role under the cyber umbrella and the security of such infrastructure is not considered as an important cyber security issue in Turkey. The issues around critical infrastructure protection remains in the shadows of work on cyber-security. Only few experts and federal documents try to examine Turkey’s approach towards the critical infrastructure protection through displaying the historical evaluation of the concept in Turkey, other states and intergovernmental organizations such as United States and European Union. These analyses do not provide a successful comparison or draw a picture that reflects Turkey’s stance on the critical infrastructure protection. In this type of condition, the most fundamental question of to what extent Turkey is successful in ensuring country’s critical infrastructure protection compared to others is not answered yet.

This thesis attempts to investigate Turkey’s success in the field of critical infrastructure protection. Two important elements are targeted in protecting critical infrastructures; physical, or so-called kinetic, threats, and cyber threats. In this respect, this thesis specifically examines the role of cyber security in the protection of critical infrastructures. Rather than simply focusing on the historical evolution of the field in Turkey, this thesis has an aim to analyze Turkey’s shortcomings and achievements by combining the comparative analysis and policy success analysis as complementary to each other. By comparing the developments regarding the critical infrastructure protection and cyber-security in Turkey with developments in the United States and European Union, this study aims to find out what is missing in Turkey’s critical infrastructure protection. Moreover, Turkey’s up-to-date documented strategies regarding the critical infrastructure protection, is examined by implementing public policy success frameworks for a deep analysis of the reasons behind Turkey’s shortcomings in this field and after providing to the point and useful recommendations to solve the aforementioned shortcomings.

This thesis defends that Turkey has not yet grasped the importance of the critical infrastructure security unlike the United States and European Union. Turkey's lack of advances on policies regarding the security of such infrastructures is bringing the country to a deadlock on this issue. Specifically, as a result of Turkey ignoring the importance of infrastructure protection, the country does not emphasize establishing strong legal and administrative background in this field and due to the lack of enough works and background on infrastructure protection in Turkey, the country could not consider assigning critical infrastructure protection a more important role.

In order to discuss the importance of the critical infrastructure protection field, compare the United States, European Union, and Turkey's approach to the field and demonstrate the considerations regarding Turkey's ignorance on the field, this thesis is divided into five chapters including the introduction chapter.

Chapter II starts with presenting the evolution of the concept of security in international relations theories under debates around three main approaches; "national security", "international security" and "human security". This review helps the reader to understand main characteristics of security aspect. After providing a background theoretical discussion on security, this chapter also presents how security understanding is currently changing by describing the specific sub-headings; energy security, cyber-security and critical infrastructure security.

Chapter III illustrates the comparison about developments regarding critical infrastructure protection and accordingly cyber-security between the United States, European Union and Turkey. The comparison includes four categories. These are:

the definitional considerations on the issues of critical infrastructure protection; cyber-security and cyber threat, legal background, institutional structure and allocated specific budget. In this way, this chapter shows how these countries and intergovernmental organizations understand and practice the infrastructure protection.

Chapter IV analyzes the Turkey's "2016-2019 National Cyber Security Strategy", which is the up-to-date document that includes the practices for critical infrastructure protection, by considering the three dimensions of public policy analysis. The chapter investigates what the problems in Turkey's strategy on critical infrastructure protections are, through measuring the mentioned strategy's process success, programmatic success, and political success.

Chapter V concludes with a brief discussion of the findings and also provides recommendations to improve Turkey's critical infrastructure security.

1.2 Methodology

Methodologically this thesis uses two approaches. First, to compare the United States, European Union and Turkey's approaches and practices on critical infrastructure protection as well as cyber-security, attained definitions on critical infrastructure systems, cyber-security and cyber threats are analyzed. The legislative and judicial evolutions, duties, and implementation of institutions regarding critical infrastructure protection and cyber-security is also compared. Lastly, allocated budgets on such infrastructure and cyber security policies are examined. In this respect, I have drawn upon primary sources, such as archival records, laws and regulations, official statements, documented strategies, and actions plans, in both English and Turkish.

Second, to investigate Turkey’s policy success on critical infrastructure protection, Marsh and McConnell’s (2010) policy success framework, which points out the success of the process, the programmatic success and the political success as three dimensions of analysis, is adapted. This framework is applied on Turkey’s 2016-2019 National Cyber Security Strategy, as the most recently published strategy document of the Ministry of Transportation, Maritime and Communication, it includes the objectives for both cyber security and critical infrastructure security. In addition, to analyze the implementation of such strategy, Ministry’s Administrative Activity Reports which cover the terms from 2016 to 2019 is used.

CHAPTER II

THEORETICAL APPROACHES TO SECURITY

2.1 The Concept of Security

Security, as one of the most vital necessities for a human being, is generally conceived as to be secure against any kind of threat or fear. Although the security is understood as a core value, the political notion of the concept is revealed with the invention of the security policies in academia. When the United States' administration introduced the National Security Council in 1947, this development became a model for several other states and produced the introduction of the new political concept called security policy (The White House, 2020). Through this development, states have got a sense to conduct and also pursue a certain security policy. In this regard, the security policy is more than a defense and military policy. It is a combination of various approaches to security such as internal and external security policies, economic policies, or policies for influencing the world system (Heurlin & Kristensen, 2002).

While the concept of security is essential for the state in terms of its policy orientation, the conceptual analysis of security in the academic field was neglected until the 1960s (Baldwin, 1997). This neglect in academia was condemned by several studies through displaying that there were few and unsatisfactory attempts to define the concept of security (Buzan, 1984; Knorr, 1973; Smoke, 1975; Ullman, 1983).

Even so, there are some scholars who started to examine the concept, they explained their purpose by skipping the definitional problem and tried to form the state-centric concept of national security (Baldwin, 1997; Knorr, 1973). After realizing the neglect of the concept, Barry Buzan (1983) provides five main reasons for the neglect of security. First, security is difficult concept to define and explain. Second, the concept of security apparently overlaps with the concept of power. Third, there is a certain unwillingness to engage security by the critics of realist theory. Fourth, the security scholars and experts are not keeping up with the new technological developments and emerging policies related to security field. And fifth, the policymakers find the ambiguities around the concept security useful. Although Buzan mentions several factors to bypass the conceptual and definitional analysis of security, he admits that none of these reasons are rational enough to explain unmotivated scholars and security experts, which should clarify the concept of security (Baldwin, 1997; Buzan, 1984). Nevertheless, other scholars, who do not find Buzan's explanations convincing, perceive the concept of security as an "essentially contested concept", that gives rise to the problematic situation, regarding the subject and its recognition, by providing three reasons; ambiguity in its meaning, not fulfilling requirements for the classification, and even if the concept of security can be classified or defined, the implications of the concept may not be correctly specified (Buzan, 1984; Gallie, 1955; Gray, 1977; Macintyre, 1973).

In the same vein, it is generally accepted that the concept of security is way too broad and for this reason, it is hard to engage different approaches and school of thoughts to come up with a conclusion about the concept. However, the works and definitions based on the concept of security have been extended since the 1990s, especially after the Cold War. Therefore, some concepts and definitions of security have been described by different scholars. While Mohammed Ayoob (1995: 9) argues that "both security and insecurity is defined in relation to vulnerabilities, in terms of international and external means, that threaten or weaken state structures including territorial, institutional, and governing regimes". In the same manner, David Baldwin (1997) adds that to be secure, it is necessary to sacrifice various values, including marginal and prime values. Barry Buzan (1991) views that security is a most significant referent for states to determine conditions of threat, which can be tolerated or require immediate action. Despite the others' perception, Buzan supports that the concept of security is neither threat nor status-quo, but something in between.

The concept of security found a place within the academic field as a policy objective and scientific object through specifying the meaning of security related issues, such as "the actors whose values and interest are to be secure, the degree of security, the kinds of threat, the means for engaged threats, the cost of security actions and the consideration of the relevant time period" (Baldwin, 1997: 17). Within the literature, the three main pillars of security are primarily considered, and these are national security, international security, and human security. First of all, national security is defined as the security of a nation-state, in terms of political, economic and military means, which is conceived and pursued as a duty of the government (Romm, 1993). In the traditional approach, national security is predominantly understood as a military phenomenon, which focuses on determining enemies that can feasibly pose a threat and eliminates that threat by acquiring more military-based developments, establishing alliances or allying with states to possess the needed power (Buzan &

Hansen, 2010). Yet, others hold that national security contains various components other than only military security, such as “economic security, resource security, demographic security, border security, geostrategic security, informational security, health security, ethnic security, environmental security and cybersecurity” which are also closely correlated with the elements of national power (Paleri, 2008).

International security, or so-called global security, refers certain measures which are formed by states, international and non-governmental organizations to maintain safety and prosperity in the international system. These measures generally relied on military action or diplomatic actions like agreements, conventions and treaties (Buzan & Hansen, 2009). Moreover, international security is basically related to both internal and external security of different social systems, which take part in the world order (Balazs, 1985). For this reason, international and national are linked to each other, and international security can be assumed to be a reflection of national security. Whereas national security perceives insecurity as an external threat, as Jozsef Balazs (1985) mentions that there is no similar external dynamic within the concept of international security. More generally, the first two approaches of security give moral primacy to the nation-state as a significant element. In contrast to those approaches, a third approach of the security gives moral primacy to human beings above the security of nations and the international community. Specifically, human security is the prospective supports that “the individual is receiving from all state-centric security concerns” (Floyd, 2007: 40). Although the humanitarian element within security tries to emancipate the field and shift the paradigm from nations to individuals, there are two controversial claims existing in human security which are:

the protection of basic human rights is already duty of the international community, and human security opens room for humanitarian intervention.

After proceeding the debates around the concept of security and examining multiple components of security, in the next section, I will try to answer the question of how international relations theories engage with security. As a result, the next section displays that one of the security dimensions finds it essential to underline different approaches to the concept of security and to examine what security means under these approaches. For, we generally grasp the concept before starting to discuss an issue under a specific security subtitle.

2.2 Security in International Relations Theories

International relations theories predominantly offer insight to perceive why certain conditions occur in the international system and what the wide range of actions behind them by reflecting various assumptions are (Smith, 2007). More specifically, theories aim to explain actions to understand different ideologies through which individuals and nations consider the problems in international relations, establish, and give direction to their goals and assign duties (Aron, 1967). Within the discipline of international relations, several theories focus the concept of security to gain a deeper understanding and to analyze the driving factors and forces in the world order as a result of increasingly unpredictable global and catastrophic events, which bring attention to the study of security by policymakers and scholars (Tripp, 2013).

Therefore, this section displays the relation between the concept of security and international relations theories, and theories' perspectives towards the elements of national security, international security and human security by examining the arguments of traditional theories of realism and liberalism, and most recent theories of constructivism and critical theory.

2.2.1 Realism

Classical realism, or so-called political realism, has been defining "as the oldest and most dominant theory of international politics" with the concept of security settling at the center of realist thought (Walt, 2010: 1). Realism particularly emphasizes the concept of national security and defines the concept as "the preservation of a state's territorial integrity and physical safety of the general population by providing a particular sense of the use of the means of threat and control of power" (Carnesale & Nacht 1976: 2). Realism also supports that the insecurity of a nation-state is the main problem of the world system where self-interest is the primary duty and to be a secure state, it should deter and defend against threats. Therefore, the placement of security within the realist approach is understood through the examination of the main assumptions of realism. According to realism, the nation-state is the unitary actor in the international political system and always pursues its national interest, the decision-makers are rational, and state survives in the context of anarchy which refers the absence of international law and order (Antunes & Camisao, 2018; Tripp, 2013; Walt, 2010).

The first assumption of realism is that the state is the principle and unitary actor that always seeks to satisfy its own national interest. Whereas other agencies exist, as do individuals and multiple organizations, their scope and power are limited when compared with the state (Antunes & Camisao, 2018; Keaney, 2006; Morgenthau, 1948). This assumption is mainly based on the strong belief that human beings are egoistical and seeks power to be secure. In the same lane, realism focuses on “human selfishness, appetite for power, and the inability to trust others”, which eventually lead to predictable outcomes (Antunes & Camisao, 2018: 1). Since humans are organized under the state, state behavior is the reflection of human nature. In this sense, realists are skeptical towards the concepts of harmony of interest and internationalism. According to Hans Morgenthau (1948), the regulations and implication of international organizations are only the reflection of the interest of sovereign states. For this reason, the natural harmony of interest has no reality and meaning in the international system. The only reality, illustrated by Niccolo Machiavelli (1981), is the morality based on harmony, this is the product of power. The concept of internationalism also has the same difficulties because absolute international standards are not independent from the interests and policies of the state (Carr, 1946).

The second important assumption of realism is about the decision-makers, which refers to policymakers. It is assumed that the decision-makers are rational and have a duty to pursue state interest (Antunes & Camisao, 2018; Lebow, 2007). In that regard, Machiavelli (1981), in his work called “The Prince” written in 1532, points out that human rationality affects the security of the state. For this reason, the decision-makers’ first concern should be promoting national security. In order to fulfill this duty, decision-makers cope with internal and external threats and guarantee the survival of the state in the international political system. With this statement, realist thought revolts against the utopianism through turning its face to necessities of a sovereign state. When Henry Kissinger (1976) argues that how realistically decision-makers understand national security is a vital security concern, he underlines that the leaders should be the protector of security through determining rational action for security interests.

The third assumption of realism lies in its understanding of the international system. Realism sees international order as a corrupted system where self-interested sovereign states are competing under anarchy (Baldwin, 1997; Buzan, 1996; Morgenthau, 1948; Walt, 2010). This perception of realism towards international system has a dominant impact on the definition of concept of security as an element of anarchy. In this respect, the concept of anarchy does not mean a war against all. Still, it means that there is no legal authority to bind a state when it perceives that breaking an international order does not harm its interests (Morgenthau, 1948). That is why the absence of effective authority allows the power dilemma to continue. Therefore, the main security problem is that the inevitable conflict of interests, which have occurred between states possessing different power and capacity, makes one side more vulnerable against others (Carr, 1946). Generally, the nature of state becomes predatory in the anarchic international systems, where no one trusts each other, to be secure is security against all.

In his work called “Theory of International Politics” (1979), Kenneth Waltz tries to modernize the traditional realist approach through a systemic level analysis, which separates the analysis of unit-level factors and system-level factors. Nevertheless, the modern version of realism is defined as neo-realism or structural realism and carries a similar foundation with classical realism in terms of its security understanding. According to Waltz (1988, 1989), the state would use force to fulfill its goal under anarchy, but the main goal of the state is not power, it is security. In this regard, neo-realism argues that “the ordering principle of the international system, which is anarchy, is the primary source of the security problem” (Walt, 2010: 4). However, although neo-realists accept that the anarchy affects state behavior such as its foreign policy, as in classical realism, nature of the state is rooted in the relative power of the sovereign state. Therefore, the international system as an active arena is the playground for states to pursue their own national interests independently (Ashkezari & Firoozabadi, 2016; Walt, 2010; Waltz, 1979). Given this context, the anarchic system encourages states to compete even when they do not want to fight in every area, for this reason, anarchy is defined as a source of a security dilemma.

For neo-realists, the structure of the world system is based on the distribution of power, which deters the security of a nation. The structure only changes if states take actions against each other. However, because of most states have no power to change the structure and preserve its national security independently, they would try to balance against each other in order to increase their chance of survival (Walt, 1985; Waltz, 1979). Therefore, balance emerges either by internal or external means. While internal balancing refers to the developments in military power to equalize with other states, external balancing refers to creating alliances with a hegemon or counter stronger power (Waltz, 1979). Generally, neo-realists focus on states’ interactions and security concerns in the international system because other agencies like international organizations would not have an important impact on the international structure as much as states (Waltz, 1979, 1989). Then, even though neo-realism tries to develop the classical realist perspective by underlying the autonomous role of system-level factors, its approach about the security still relies on the concept of national security rather than international security, which is also absent in neo-realism as in classical realism.

In addition, the implication of security to survive in the international environment is also an important debate among neo-realists. Within this debate, two opposite perspectives exist, and these are offensive realism and defensive realism. Offensive realism argues that a state, whose primary motivation is survival, has offensive military capabilities, which gives it the ability to harm or even destroy others. This state would compete with other states because, in the anarchic system, a state cannot be certain about others' intentions (Mearsheimer, 2001). In contrast, defensive realism assumes that the offensive intentions minimize state' tendency to seek and comply the the balance of power, that is why it is in the state's best interest to preserve the status quo to ensure its security (Layne, 1993; Taliaferro, 2000).

Another modern version of realism named as neo-classical realism has an aim to develop both classical and neo-realist engagements by synthesizing the domestic and individual level analysis with a more systemic analysis based on foreign policy analysis. However, in terms of its security approach, neo-classical realism like classical realism and neo-realism has a state-centric perspective. Gideon Rose, in his article "Neo-classical Realism and Theories of Foreign Policy" (1998: 153), argues that "a state's foreign policy is determined by its power capabilities in the international political system and those certain capabilities depend on various intervening factors within the state itself". This means the decision-makers are also surrounded by domestic factors rather than factors only constructed by external means. Therefore, neo-classical realism claims that the state's foreign policy decisions are shaped by its relative material power and its placement in the international political system (Ashkezari & Firoozabadi, 2016; Rose, 1998).

As other realist thought, neo-classical realism supports that "means of politics is the struggle among states to reach power and security within the environment of scarcity, which indirectly point outs that anarchy is the main reason of competition between states" (Ashkezari & Firoozabadi, 2016: 96). In other words, neo-classical realism confirms the pressure created in the anarchical system affects the behavior of states in foreign policy choices, which means that independent systemic variables have an influence on states' foreign policy preferences. Therefore, in this type of relation, increasing power and securing its national well-being would become the priority of every state (Rose, 1998). In this respect, intentions of decision-makers as well as state structure and domestic factors play a significant role in shaping foreign policy (Rose, 1998; Schweller, 2003). After the explanation of basic assumptions of neo-classical realism, it is understandable that even though neo-classical realism gives weight to impacts of domestic and international structure on national foreign policy choices, it shares same approaches with classical realism in terms of security understanding through seeing a nation's security as a core value in the international system and accepting the importance of decision-makers to pursue state's national interest.

Whereas neo-realism focuses on one independent variable of competition between states and one dependent variable of international structure, neo-classical realism focuses on two independent variables, national and international structure and the outcome from their interaction, which is based on the foreign policy choices as a main concern in policy (Ashkezari & Firoozabadi, 2016). In this type of context, while neo-realists assume that states' intentions can never be truly understood, neo-classical realists support that such intention in the international political order can be conceived by various cognitive elements like perceptions, desires and threats, as well as systemic variables like distribution of power and state capabilities (Dunne & Schmidt, 2016; Rose, 1998). Although structural realism and neo-classical realism have different approach about the conceiving state's intention in the international system, these two realist theories match by providing a sense that whether states' intentions can be understood or not, security concerns always lie within any type of intention. At the end, by looking at the evolution of three main realist approaches, it can be concluded that even though each new approach tries to evaluate the theory, they are always particularly emphasizing on the national security rather than other types of security concepts.

2.2.2 Liberalism

The most optimistic international relations doctrines named as idealism, which completely dissents from the realist thought. Idealism claims that ethical and moral considerations are more vital than national interests in the international system, where there is no need for any type of conflict (Wright, 1952). More specifically, while realism focuses on the concept of the security dilemma, idealism constructs its own perspective based on nation-states' good intentions in the international system through deeply emphasizing the elements of international law and international organizations (Wilson, 1998). Despite the realist understanding towards anarchy, idealism supports the cosmopolitan and harmonious international order. Within this context, the idealist approach towards security is defined as collective security (Wilson, 2011). It means idealists' understanding of security contains elements of the of international security more than national security. Therefore, by giving sense to cosmopolitism, internationalism and collective security, idealism creates the basis of liberalism.

Liberal security understanding is generally the representation of internationality and is correlated with the two significant components of cooperation and democracy. According to liberals, the world peace and security are maintained and spread only by collective security. To provide a deeper understanding of international cooperation, it is useful to describe the concept and its relationship with collective security under the three categories. First, liberals support that international organizations play a crucial role in cooperation among states. Particularly, international law and agreements, which are established through common goals and constant diplomacy, are ensured by international organizations to sustain world order (Deudney & Ikenberry, 1999). Therefore, the states, who have a common goal and continuing interactions, can achieve collective security to preserve international security by setting up or participating in international organizations. However, the existence and practices of international organizations are primarily based on several conditions such as the willingness and participation of states as contracting parts, the functionality of treaties as constitutive parts and having a constitutional structure (Reus-Smith, 1997).

Second, the interconnectedness between states as a result of international free trade maximizes the possibility of cooperation and minimizes the possibility of conflict. The spread of capitalism with the help the operations and implementations of powerful liberal states and international organizations creates an free-market based, but also dependent international economic system. These conditions provide mutual benefits for the trade between states and makes war less likely through decreasing the disputes, because conflicts would disrupt the benefits of economic relations (Deudney & Ikenberry, 1999; Meiser, 2018; Shiraev & Zubok, 2015). Third, the basis of liberal international system is obtained from the international norms, which favor international cooperation, human rights, law and order, democracy, and accordingly collective security. Under this type of order, if a state disobeys the international norms, it is subject to different types of international enforcements and costs (Deudney & Ikenberry, 1999). However, the international norms sometimes do not create global prosperity because they are often contested by nations.

Democracy as another important element of liberal theory is discussed under The Democratic Peace Theory through describing its relationship with the concept of security. The democratic peace theory argues that democratic states are unlikely to get engaged in a conflict with one another (Meiser, 2018). There are two major explanations that exist to understand statements of democratic peace theory. First, democracies are emerged by international restraints on power such as domestic politics, voting, audience costs, transparency and a checks and balances system (Fearon, 1994; Pugh, 2005). For this reason, taking aggressive actions against others is not easy for the democratic states as a result of a complex check and balancing system within the domestic structure. Second, democracies tend to conceive each other as a legitimate actor in the international system, that is why, liberal democratic states do not fight against one another (Doyle, 1983). In the same vein, statistical analyses and historical cases prove that democracies do not fight with each other even when different variables such as trade, geographical affinity, alliance facilities and the distribution of power clash with each other (Doyle, 1983; Maoz & Russett, 1992, 1993; Owen, 2010).

However, although democracies choose to preserve the status quo, their behavior actually goes in two directions, the dyadic democratic peace, which essentially claims that liberal democracies do not fight with each other and the monadic democratic peace thesis which has a deeper understanding and asserts that democracies are passive towards all types of states, not only other democratic states (Rummel, 1979). The basis of democracy peace theory is based on the argument that democracies are peaceful agencies; however, the theory contains two contradictions which are the basis of a debate to display the ways democracies are not peaceful entities. According to the so-called Separate Peace Hypothesis, that refers to the community of security, democracies can practice aggressive behaviors against other non-democratic regimes (Lipson, 2003). Another contradiction in the debate argues that democracies may avoid the conflict with each other, but they have a high possibility to win the conflict because democratic citizens are the better soldiers (Lake, 1992; Reiter & Stam, 2002).

Although liberalism predominantly focuses on the peaceful international order, it is also embracing some elements of human security and national security, as well. When liberalism engages with the political regime types as a source of serenity in the world system, it touches upon the issue of human security. Liberalism internalizes the morality to preserve the right of individuals to life, liberty and prosperity and supports that these should be the main goal of governments because insecurity of individuals might become the new source of the threat, which can lead to international security problems (Tadjbakhsh & Chenoy 2007). Therefore, while liberalism regards the well-being of individuals which form the political system of the state, it believes that unchecked powers such as the monarchy and dictatorship cannot protect the individuals. For this reason, democracy is a necessity in terms of checking and balancing the states' use of power (Meiser, 2018). Moreover, by emphasizing that "the states make meaningful choices, and in that way, their security varies by the choices they pursue" (Owen, 2010: 4), liberalism affiliates state-centric language. In addition, liberalism assumes that the states' preferences and interests are shaped by various domestic factors and international groups (Moravcsik, 1997). However, although this statement also follows realists state-centric language, it also underlines that states are the heterogeneous rather than autonomous, and their actions are shaped by domestic properties as well. In this way, even the state-centric approach of liberalism does not entirely give priority to a state.

Neo-liberalism, as a revised version of liberalism, implements game theory to examine how and why states cooperate with each other or not within the international system in which they can form mutually beneficial arrangements and agreements with the institutions (Keohane, 1984). Generally, neo-realists support that states are always focusing on their absolute gain rather than relative gain against other states. In that way, neo-liberalism emphasizes on the distribution of possible profits, which affects the total gain of states. Neo-liberalism does not deny the anarchic international system. Still, unlike the neo-realism, it asserts that even in anarchy, cooperation between states can occur through mutual trust, international norms and institutions (Evans, 1998; Keohane, 1989; Keohane & Nye, 1977). Whereas neo-realists are mainly concerned that anarchy creates a competition to be secure and the notion of self-help disturbs the collective action, neoliberals support that self-help composes cooperative behavior and within the anarchic structure, states create self-help rather than self-help adapting states into the system (Wendt, 1999; Whyte, 2012).

Within this context, neo-liberalism advocates the three main principles of the concept of collective security. First, states have to give up the usage of military means to maintain the international order and status quo. Second, to meet the concerns of the international community, states have to emancipate their understanding of being a nation. Finally, states have to trust each other by being aware of how fear adversely affects international politics (Baylis, 2001: 305). Neo-liberalism also differentiates itself from liberalism in terms of its distinct perspective towards the issues of sovereignty and security. Whereas liberalism focuses on the political aspects in democracies by handling the interactions between the sovereign law and individual rights, neo-liberalism portrays that political success is reached by the relations between the domestic powers and notions of securitization through practices of governments and individuals (Whyte, 2012).

Neo-liberalism develops the mainstreams theory of liberalism and opposes neorealism in terms of security understanding by introducing the idea of complex interdependence. Complex interdependence emerges in four domains; focusing on a variety of channels of actions between domestic structures, interstate and institutional relations, the prioritization of subjects, as linked to changes of anarchy, and decline in military force and coercive power (Keohane & Nye, 1977). Within complex interdependence, neo-liberals focus on the promotion of security and the economy

(Baldwin, 1993). However, placement of the economy and security in neo-liberalism is still a controversial subject. On one hand, scholars argue that while the logic of absolute gain has a direct relation with the economic realm, the logic of relative gain concentrates on the security realm via militaristic means (Mearsheimer, 1994). On the other hand, others believe that there is no clear division between the security and economy as referent objects (Keohane & Martin, 1995). However, the most recent understanding called neo-liberal institutionalism comes to the scene to remove this uncertainty.

Neo-liberal institutionalism differs from the other theories as it does not ignore the impact of internal politics and emphasizes economic means as a referent object. According to neo-liberal institutionalists, practices of democracy and capitalism create the international system which not only ensures the status quo, but also creates the economic benefits for the participants (Baldwin, 1993; Keohane, 1989). In the anarchic world order, the modernization and sharing of technologies have started to pacify the component of the anarchy (Folker, 2010). In this regard, states start to pursue collective goals. Another important approach, called the Hegemonic Stability Theory, starts to be dominant in the international system regarding the decline of the powers of the hegemon by “a capitalistic economy and free trade system which are supported by the various formal institutions” (Colebourne, 2012: 2). Despite relying on state-centric thought, these institutions are desirable “because they reduce the transactions costs by rulemaking, negotiating, implementing, enforcing, information gathering and conflict resolution” (Navari, 2008. 39).

Furthermore, the institutions, which directs the international economy, are also durable. That is to say, the constant economic regime continues to exist even if the conditions that facilitated the institutions creation have disappeared because the creation of institutions are difficult and hard to reconstruct (Keohane, 1984). Therefore, the basis of neo-liberal institutionalism is the cooperation of economic means to create interdependence and solve the security dilemma because institutions mainly help to provide information, reducing transaction costs and changing the payoffs (Keohane, 1982). Basically, neo-liberal institutionalism sees the economy as a referent object and argues that international actors should promote institutionalization to reach collective security and international stability. Even though neo-liberal intuitionalism, as neo-liberalism, brings the elements of national security, they always combine the national elements with international elements and pursue the goal of reaching a global level of security.

2.2.3 Constructivism

Since its establishment in the early 1980s, constructivism has become one of the most pioneered theoretical thoughts among international relations theories. Rather than examining the components of security under the categories of national, international and human securities, constructivism dominantly focuses on the ontological and epistemological analysis of the security. Before engaging the constructivist approach towards security, it is beneficial to understand the promises of constructivism. According to constructivists, agencies continuously shape and also re-shape the international system through their actions and interactions. In this respect, constructivism is seen as a social theory, by concentrating on the social construction of the international political environment and ideational factors such as ideas, beliefs and norms, it tries to emancipate the borders of the study of security (McDonald, 2008).

The main assumption of the constructivism is that the world is socially constructed. Particularly, the nature of knowledge and reality is searched by ontological and epistemological approaches (Wendt, 1995). In this way, the concept of security is also a social construction. However, this statement does not specifically mean that there is no security or security does not have meaning. Instead, constructivists support that security is a context-specific social construction. Despite the working on developing a definition of security, constructivism emphasizes the premises to get better insight into "how security is given meaning within the various contexts and examines the implication of the concept of political practice" (McDonald, 2008: 64). Constructivism tries to answer the aforementioned question by focusing on the impact of particular and historical contexts regarding the social interactions between actors. Essentially, the notion of social construction is understood as a constructivist game theory by stating that security is a part of negotiation and contestation, and analytically neutral between the conflict and cooperation (Farell, 2002; McDonald, 2008; Wendt, 1995).

Other elements of constructivism are identities and interests. Constructivism argues that identities are the representation of actors, such as individuals, states, and institutions, which provides understanding of who they are, and what establishes their interests. For constructivists, identities constitute interests and actions that shape international political system.

This also maintains that elements such as reality and knowledge are also always under construction, which are not fixed and always open to change (Theys, 2018). Whereas anarchy generally seems to encourage self-help concerning security and inevitability conflict. Anarchy is also shaped by the states practices which are affected by the different ideational elements (McDonald, 2008). Then, anarchy can be conceived in different angles relying on the meaning that is attributed to it. In this way, it is clear that understanding security is based on identities and interests of actors, which has the ability to shape structure. If states instead held the alternative meanings of security, as cooperative, where states can maximize their security without adversely affecting others, or collective, where states define the security of others as a being profitable to themselves, in this case, anarchy would not lead to self-help (Wendt, 1992).

Aside from the identities and interest, social norms are also significant for the constructivism. Norms are generally defined by constructivists as a standard of appropriate behavior for actors and formations who have a certain identity (Katzenstein, 1996). Generally, norms are applied to dominant ideas to constitute appropriate and legitimate actions for the states as one of the key members of the international system (March & Olsen, 1998). For constructivists, the existence of norms, which differ in time, context, and action, is important to exert limits on sovereign state actions. Therefore, by creating borders, limiting, or enabling certain actions, the social norms regulate the practice of security. However, according to Theo Farrell (2002), constructivism focuses too much on the social norms within the security studies and faces two crucial problems. First, constructivism gives ontological status to unobservable objects through accepting certain norms as “having objective existence”. Yet, “the norms are not simply ideas floating around inside the actor’s head”. “Regardless of the norms are shared beliefs which are out there in the real world”, constructivism gives meaning to norms as material reality and actions. Second, “the social practices may be observed directly”, but not the shared the embodiment, which gives rise to the question of how one would know these shared beliefs (Farrel, 2002: 60). Therefore, the meaning of security which is shaped by social norms becomes problematic as well.

Since the 1990s, the international relations thought called the Copenhagen School emerged with an attempt to emancipate the study of security within the constructivist theory. The school mainly develops security studies by analyzing the neglected concerns among international relations theories such as environmental change, weapons of mass destruction, poverty, and human rights regarding state security policies.

With this type of engagement, the school is generally seen as a bold step that completely shifts security understanding from a state-centric understanding to a human-centric understanding. Specifically, the Copenhagen School examines security related issues under the three dominant conceptual pillars; the sectors, securitization and regional security complexes.

According to the Copenhagen School, the concept of security needs to be analyzed in the context of a state of exception, which refers to the idea that security problems are always important for the survival of certain referent objects such as the well-being of the state, territory, structure, society, identity, culture or economic system (Buzan et al., 1998; Peoples & Vaughan-Williams, 2010). To secure the referent objects, the sectors, which are defined as areas that entail a certain type of security interactions, are primary actors. The school considers the sectors, "including military, economic, societal and environmental sectors, as a path to encourage different forms of relationship relevant actors to develop and also encourage different meanings of referent objects such as security" (Buzan et al., 1998: 7-8). In this way, despite other international relations theories, the Copenhagen School tries to provide ontological and epistemological perspective while answering the questions of to whom is it secure for and how security is achieved.

The concept of securitization, within the school, refers to the discursive construction of any type of threat (Wæver, 1997). Generally, this concept is established through approaching the construction of security based on speech acts. In this sense, securitization is a process in which actors declare a particular issue, dynamic or other actors to be an existential threat to a certain referent object. If the securitization action is accepted by "the relevant audience, this enables the suspension of politics and the use of emergency measures towards the conceived threat" (McDonald, 2008: 69). Therefore, the securitization of subjects depends on the acceptance of the securitization action by audiences whose thoughts are shaped by the facilitating conditions, including speech acts, positioning of "the securitizing actor" and "historical conditions" correlated with the threat (Wæver, 1997: 252; Buzan et al. 1998: 31). Given this context, the concept of de-securitization is as significant as the securitization. While one object is securitized by the interactions of actors, speech acts and audiences, the other is de-securitized (Stritzel, 2007).

Regional security complexes emphasize the actors whose security process and actions are interlinked and, as a result, their security-related problems cannot be meaningfully analyzed or resolved by disregarding others (Buzan & Wæver, 2003). The security complexes are understood “in terms of mutually exclusive geographic regions such as focusing on security interaction and dynamics in Europe, America, Asia, Africa, and the Middle East” (McDonald, 2008: 68). Therefore, the assumption is that the regional level of analysis is vital for preserving global security dynamics, but it has been poorly investigated by other international relations theories. However, apparently the security of each actor in a region juxtaposes with the security of others. Then, the intense security interdependence in a certain region defines a region and the security perception of that region.

2.2.4 Critical Theory

The establishment of the critical security studies dates back to the 1990s, and it differs from traditional international theories by supporting that security can be handled according to a different approach which tries to emancipate the ways of thinking and doing security. Even though critical theory and constructivism share common ground such as focusing on ontological and epistemological answers, critical theory’s approach to the security is markedly different. According to critical theorists, the reason behind the ambiguity of the meaning of the security is not because of a lack of interest and effort, but because security is a “derivative concept”, which is understood as “a manner that is both constructed and political” (Booth, 1991: 104-119). Generally, the variety of the definitions of security are based on the specific context, as same as constructivist thought and political worldview. Therefore, the main goal of the critical security studies in uncovering the political mind behind security thinking through displaying “the legitimization of certain actors and policies” as “a part of the construction of particular political entities” (Browning & McDonald, 2011; 239; Olivares, 2018: 2). In this regard, the substantial achievement of critical security studies is revealing that politics and security are not separate dimensions. For critical theorists, failure to understand this relationship makes the world less secure.

By emphasizing the politics of security, critical security studies reveal the relation between the security and notion of emancipation. The notion of emancipation can be seen as “a freeing individuals from multiple constraints, which prevent them from making free choices” (Booth, 1991: 319). This normative intention of critical security studies, which also underlines a commitment to progression and opposition against the repressive structure of power, is important in understanding the concept of security as a goal of the one, which inevitably promotes the others (Booth, 2005). Moreover, in the political sides of security, the critical theorists also underline the necessity of communication actions and dialogue to solve security issues and identity differences. The development of the dialogue in the international environment would lead to “the emergence of universal norms” and “the creation of a more peaceful and cosmopolitan world order” (Fierke, 2015: 187; Olivares, 2018: 2). Therefore, on the one hand, when critical security gives weight to the emancipation of security, which refers to freeing the thoughts and actions of individuals, critical security comes close to the concept of the human security. On the other hand, when critical security pays attention to the issue of dialogue to create global norms, it shares the common perspective with constructivism, especially the Copenhagen school.

Although the various components of the critical theory are debated by scholars, the first step in analytical progress was made by the Welsh School to create a deeper understanding of security. The Welsh School engages with the politics behind the concepts and agendas related to security through de-centralizing the notion of the state (Bilgin, 2008; Booth, 2005). In this sense, while the Copenhagen School focuses on the de-securitization, the Welsh School tries to re-theorize the concept of politicizing security under the three main arguments, which are strategic, ethno-political and analytical considerations. First, according to the de-securitization argument, security is a tool of state elites and regimes. However, the Welsh School tries to examine elements of politicizing security through questioning state elites' usages of security, and state-centric and militaristic approaches (Bilgin, 2008). Second, when the definition of security is established by the state elites, depending on the historical and political context, security policies can rely on statist, militaristic and dehumanized agendas. Given these contexts, others, which believe that security is conceived globally but practiced locally, it should display their existence and insecurities (Enloe, 1996). And third, the critical theorists support that debates between the de-securitization and politicizing of security should be analyzed empirically, historically and discursively too because in this way, the political and social construction of the referent object eliminates the risk of being biased and region centric (Hayward, 2005; Bilgin, 2008). After this, it is clear that the critical theory tries to emancipate the security understanding by looking at the political aspects behind it.

Throughout this section, the stance of the most important and current international relations theories on the concept of security is examined. As stated at the beginning, the approaches of the given theories to security can be examined under three main headings: “national security”, “international security”, and “human security”. While realism dominantly seeks national security and liberalism tries to establish international security, sceptic and evolutionary theories such as constructivism and critical theory criticize previous approaches by emphasizing the more human centric or even cognition centric security understandings rather than sticking into national agency centric or international structure centric understandings.

However, in the developing and advancing world order, these three concepts of security are intertwined with one another. Therefore, the crucial thing is to talk and discuss the domains of security. However, the literature is stuck in the discussions over concepts that security domains are not or cannot explicitly be included due to the intertwined outcomes as stated earlier.

The following section mainly describes the three currently important subtitles of security, where the concepts of national security, international security and human security are intertwined. These are energy security, cybersecurity, and critical infrastructure security. These concepts are dependent on one another in a system. These three security domains now face a risk from which states, intergovernmental and non-governmental organizations, public and private sectors and even individuals need to refrain from; otherwise, the three domains would be affected simultaneously.

2.3 New Directions in Security

The phenomenon of security is the vital elements of the modern states that have to secure its nation and maintain internal and external prosperity. Within the constantly changing and developing world order, states are vulnerable against the several threats which imperil the three dimensions of the security at the concurrently. In this regard, the understanding of security is shifted from discussing general dimensions of the concept of security to emphasizing sub-areas under the security umbrella. In recent years, three significant sub-areas such as energy security, cyber-security and critical infrastructure security have started to dominate the studies and dialogues regarding the safeguarding of national, international, and human security.

2.3.1 Energy Security

Even though the concept of energy security is generally used to refer to “the relationship between national security and the availability of natural resources” (Overland, 2016: 122), there is no standard definition of the concept accepted globally. In this regard, while some understand it as an affordability of the energy to meet the requirements, others focus on the reliability and sustainability of the energy in a secured and uninterrupted environment (Deutch and Schlesinger, 2006; Overland, 2016). Even though descriptive debates on the concept have continued, it is clear the current model of energy was born with the 1973 oil crisis through focusing on overcoming the distribution of oil supplies from producer states because accessing energy is vital for modern economies (Yergin, 2006). Therefore, as have other components of security, energy security has become the crucial concern for the international system through ensuring the security of energy by national policies (Klare, 2008).

To deeply examine the importance of energy security, it is useful to examine different approaches which point outs energy as a referent object. First of all, Michael T. Klare (2008) underlines the singular importance of energy security.

According to Klare (2008: 484), the more complex and productive states have a greater need for energy because “complex state systems might not maintain a high rate of industrial production, provide decent living standards for individuals or even defend itself against other powers without holding sufficient natural resources”. For this reason, energy’s singular importance is vital for modern industrial societies (Klare, 2008; Lugar, 2005). In the same direction, Daniel Yergin (2006) asserts that maintaining energy security contains various important elements such as diversification of supply, resilience, recognizing the necessity of global integration, the importance of sharing information, spare capacity, free-market system, establishing security models, developing research and development facilities, maintaining technology-based energy market and production chain. In this regard, fulfilling energy requirements, which are essential for the welfare of the state, have become challenging as a result of population growth, urbanization, the industrialization process, income increases and individuals have started to use more energy-consuming devices (Klare, 2008). As a result, the concerns about the future of energy supply creates pressure on energy producers to deal with rising energy demands and energy security. To that point, the intervention of governments in the management of energy transportation and protection come to the scene through enhancing energy security by recognizing the globalization of energy security and accepting that the whole energy supply systems need to be protected (Yergin, 2006).

It is all known that energy plays a crucial role in the security of states as a means to provide power to its economy. More specifically, energy ensures the well-being of economic sectors while some sectors depending on the energy more than others. That’s why the term of energy security is predominantly understood as the safeguarding of the supply of available energy sources needed to meet the rising demand of a nation's sectors (Klare, 2008).

Accordingly, any kind of threats, such as "political stability of energy-producing states, the manipulation of energy supply, competition over energy sources, attacks on supply infrastructure, accidents and natural disasters", are settled in the energy security agenda of states (Wesley, 2007: 11-13). In this type of environment, two conditions become more dangerous for nations' energy security, and these are competition for energy and ensuring delivery of energy supplies which are also interconnected with each other. The first major energy challenge is the increased competition for energy sources as particularly over the distribution of oil and gas between developed countries. For instance, Group of Five within the Group of Eight countries met in 1975 to "regulate economic and energy policies after the devastating impact of the 1973 Arab oil embargo" (Maavak, 2006: 1), which is the result of the increase in inflation and global economic slowdown during the Yom Kippur War (Smith, 2006). In the same direction, energy competition between Russia and Belarus in 2007 created a negative impact on the world energy market (Finn, 2007).

The other major energy challenge is preserving the "delivery of crucial supplies" when the global energy supply system is becoming more globalized in currently with connected pipelines, transmission lines and maritime routes which make delivery of energy more complex and vulnerable against various threats (Klare, 2008: 485). Especially, the protection of overseas energy resources, most importantly oil, is becoming the challenge for developed countries. According to the National Energy Policy Development Group's Reports (2001) on foreseeable future of energy resources, oil is constituted %38 of the world's primary energy supply and it is expected to double in 2030. In this context, even though policymakers want to reduce the United States' dependence on foreign sources of oil because of the price volatility and uncertainty, they also emphasize that the United States' might not fulfill this goal. For this reason, energy security must be the major consideration for American trade and foreign policy. Furthermore, although larger consumers of oil such as the United States and even China consider eliminating their oil dependency on foreign producers through turning their face to domestic reservoirs, their dependency still continues (Klare, 2008). In this type of scenario, it is clear that energy security is a crucial requirement for both suppliers and producers around the world.

The energy security is also related to two important dimensions of nations which are the military dimension and the foreign policy dimension. Firstly, the military dimension as an instrument of energy security is mainly engaged by the United States as a major energy importing state. In this regard, the military dimension of energy denotes that if policymakers see any "need to protect overseas energy resource routes" and "help their main energy producers and alliances", the possible types of interventions can function to preserve energy security (Klare, 2008: 487). Moreover, the military dimension of energy security took the attention of the United States for first time in between 1979 and early 1980s. During this time, when the Soviet Union intervened Afghanistan as a result of the raising of Islamic insurgency movement in the region, the United States delayed the Soviet's control on the region which directly threats the energy reserves, especially oil, in the Persian Gulf, Indian Ocean and also the Straits of Hormoz (Klare, 2008). Therefore, President Jimmy Carter (1980) claims that the United States should re-construct the free movement of

Middle Eastern oil by military means. Since then, the United States' military attempts to control oil flow in the Middle East region, including Saudi Arabia, the Straits of Hormoz, the Persian Gulf and the Arabian Sea, still continues (Palmer, 1992).

Secondly, as Özgür Özdamar (2009) points out, regional and international foreign policymaking is key to preserving energy security. More specifically, while developed countries rely on energy sources, energy security has a direct relation with the foreign policy dimension by establishing and sustaining ties with the energy providers' countries (Klare, 2008). In this context, the foreign policy dimension of energy security should be understood by analyzing its regulation on both energy provider and supplier countries. In terms of energy provider countries, energy is the vital object in their foreign policy which improves their place in world politics. For instance, during the 1973 oil crisis, Iran and Saudi Arabia, as oil producers, emerged as powerful countries in the international political scene and then, their relations ultimately changed with the great Western powers. In this type of situation, Western powers' hands are tied because if they tried to use force to control oil producers in the Middle East, they would harm themselves more (Campbell, 1977; Kemp, 1978). In terms of energy supplier countries, the situation is more complex. The energy supplier countries have always had good relationship with energy producer countries. However, establishing the status quo in energy security is not an easy thing to achieve. For instance, the United States, in the short term, might face serious challenges in the foreign policy dimension of energy security such as various difficulties in "building alliances, strengthening collective energy security, asserting its interests with energy suppliers, and addressing the rise of state control in energy" to secure its own energy-related interests (Kalicki & Goldwyn, 2005: 571).

After previous debates, it is necessary to understand energy security's placement in international relations theories. Energy security has been integrated into major debates of international relations theories and especially takes attention of the realist, liberal and constructivist approaches. First, as realists recognize that international politics represent a struggle for power and within this environment, raw materials are vital to the national power of certain states. In the same direction, realist thinkers point out that with the discovery of oil, this energy source has begun to shape the nature of international politics (Morgenthau, 1948). More specifically, oil illustrates the vulnerabilities of states. Since then, various analyses focus on the growth rate of energy consumption and states dependency on it through emphasizing the conflicts that have a connection to natural resources (Belyi, 2007). In this regard, the concept of a security dilemma has become an important paradigm to secure strategic commodities like energy.

By tackling the concept of a security dilemma through engaging the dynamics of geopolitics and energy security, realists assume that with the emergence of the importance of energy "as a strategic commodity, there is a rising great power competition to reach and secure energy" (Mohapatra, 2017: 686; Moran & Russell, 2009). Therefore, while examining the connection between the paradigms of energy and realist international relations theory, the key components of the connection should always be considered, and these are "the availability of energy, demand for energy, pricing mechanisms and the nature of the actors who are competing for energy as the main source of dilemma" (Mohapatra, 2017: 686). However, in terms of the issues around energy security, neo-realists focus on the interaction between the anarchic international system and distribution of capabilities in this type of environment. According to neo-realism, the asymmetry in the distribution of capabilities, international actors have the fear to secure its relative gain rather than absolute gain because under the difficult conditions as a result of anarchy and asymmetry, the relative gain is a much better option (Powell, 1991; Waltz, 1979). Therefore, if one tries to correlate neo-realist assumptions with energy security, they can conclude that the fear of the defeated by more capable states and the asymmetric distribution of capabilities such as natural resources give rise to international instability and conflict among nations (Mohapatra, 2017).

Second, within the liberal international relations theory, approaches of liberal institutionalism and neo-liberal institutionalism mainly engage with energy security and its components. According to liberal institutionalism, international institutions are the key actors to govern and regulate cross-border energy trade and enhance energy security through promoting knowledge and information on any type of energy-related issues, establishing general legal binding institutions, constituting issue-specific agreements, forming practices for regional organizations and groups and regulating private commercial actors (Mohapatra, 2017). In this context, liberal institutionalism focuses on information-based institutions, legally binding institutional frameworks, and binding agreements to touch upon the international status quo in energy-related matters. While information-based institutions, such as the International Energy Agency, provide available data, transparent actions and raising awareness in the energy sector, legally binding institutional entities work for enforcing law and order at international level and institutionalize practices of economic systems through regulating trade, providing conflict settlement rules and mechanisms, international protection of investors and standards of contracts.

In addition, the binding agreements such as the Energy Charter Treaty, under the frameworks of the World Trade Organization, set practices for international arbitration favor conciliation between states and provides conciliation procedures by covering all energy markets (Mohapatra, 2017). In the same direction, neo-liberal institutionalists believe that institutionalism brings along “a more smooth and clearer bargaining process through distributing profits equitably among all the actors and facilitating cooperation” (Keohane & Martin, 1995: 45). For instance, the International Energy Agency and Organization of the Petroleum Exporting Countries are the two important institutions that regulate the flow of energy and “conduct the interdependent character of regulations” (Keohane, 1984: 29-30). Neo-liberal institutionalism also represents that notions of energy security like other economic subjects is related to the demand and supply chain which are controlled by the institutional mechanism, the International Energy Program and Coordinated Emergency Response Mechanism, which “regulates flow of energy and maintaining stockpiling of reserves for at least ninety days to meet any kinds of emergency situation” (Goldthau &Witte, 2010: 8, Mohapatra, 2017: 694).

Third, constructivism sees the notion of energy security by asserting that energy is playing a catalytic role in reviving the group identity by taking advantage of the weak institutional structure of certain nations to have leverage among natural resources. Moreover, this system helps powerful countries to bargain with the weaker institutionally structured countries to achieve dominance on the political structure which creates resource and identity conflict by taking advantage of the insufficient distribution, finance and aggravation mechanisms (Stokes, 2007; Colgan, 2015; Rustad & Binningsbo, 2012). As a constructivist approach, the Copenhagen School also focuses on multi-level approaches to international politics rather than only focusing on the international system.

However, the Copenhagen School does not separate energy security from other security sectors even though it predominantly engages with the importance of major sectors such as political security, economic security, regional security, environmental security and even specifically energy availability and sharing to discuss the issues around energy security. While political security refers to the notion that although security relations of states in anarchic international order continue, states are always looking for "energy self-sufficiency", in this type of environment, energy availability is an indirect means for military capabilities (Belyi, 2007: 354). In addition, the Copenhagen School defines economic security as the difficulty to foresee the behaviors and decisions of capitalist economies. In this regard, the concept of securitization is directly related to political perceptions towards the unpredictable energy market. Lastly, environmental security represents the "incompatibility between economic developments and the protection of natural resources" (Belyi, 2007: 354 -355). Therefore, by providing four components of energy security, the Copenhagen School's understanding of securitization of energy focuses mainly on the political structures in the international system.

Despite previous fruitful reviews about energy security, in today’s highly interconnected world system, issues around energy security have started to face new threats of cyber-attacks on energy. Currently, traditional energy technologies are becoming more connected to modern digital and cyber networks. Therefore, this increasing digitalization in the sector makes energy systems “smarter” and provides consumers to even more benefit from the energy systems (European Commission, 2020a; United States Department of Energy, 2020). However, digitalization of the energy sector creates vital risks such as an increased number of cyber-attacks and cyber-security incidents, which are the recent threats governments should take care to not ignore and the concepts that have been lacking in the previous literature about energy-related approaches.

2.3.2 Cyber Security

The information systems have been long considered as essential components of several political subjects such as diplomacy or conflict. Since the early 1990s, information has played a key role in international relations as a result of its importance for political means and have been increased by the proliferation of information and communication technologies into various aspects of industrialized states (Cavelty, 2015). In this condition, cyberspace, which unifies information, communication, database, and other means of cyber interchange forms the network ecosystem. Even though cyberspace is perceived as a virtual arena and often interchanged with the term, the internet, it is created by the physical elements such as servers, cables, computers or even satellites to connect global cyberspace (Dyson et al., 1996; Cavelty, 2015).

Therefore, ensuring the security of cyberspace should be one of the most important necessities. The concept of cyber-security mainly refers to “the protection of computer systems from the theft or damage to their hardware, software or databases, and even from the disruptions of operations and services they provide to society” (Sedkaoui, 2019: 59). If a certain state or actor uses technology to attack others, this action causes harm comparable to actual warfare and for this reason, these types of situations are labelled as cyber-warfare (Singer & Friedman, 2014). Meanwhile, states prefer cyber-attacks to dominantly control resources of others such as military forces, raw materials like natural resources, economic capabilities and critical infrastructure systems through engaging different types of cyber-threats, which could be espionage, sabotage, economic disruption or a surprise attack. For this reason, matters of cyber-(in)security are classified as an issue under the umbrella of security studies in international relations.

Until current times, different states have engaged in several cyber-attacks against others. For instance, during the Gulf War of 1991, even the United States’ military strategists considered cyber-warfare, this did not happen because the military was not able to win such a war or secure information dominance (Arquilla & Ronfeldt, 1993; Nye & Owens, 1996). However, this event shed a light on the possibility of emergence of the cyber-attacks. This type of attention towards cyber-security was also seen in the mid-1990s as well. In this regard, the North Atlantic Treaty Organization’s (NATO) intervention in Yugoslavia is understood as a first sustained use of the full spectrum of cyber-war elements through using propaganda, DDoS attacks and website and account hacking such as hacking Milosevic’s bank account by the United States. In the same way, the increase in the use of the internet during the state-led conflicts become the reason of labelling the 2000s as the age of war on cyberspace. For instance, the cyber-conflict between the American and Chinese hackers in 2001 is seen as the first cyber world war, which started with the American discovery plane's force into Chinese territory after a dispute with Chinese jet fighters (Cavelty, 2015). In 2007, Russia attributed DDoS attacks on Estonian federal systems because of the Estonian government's decision to re-place the Soviet-era monuments in Tallinn (Ottis, 2007). Whereas those cases represent defensive means, offensive aggressions in cyberspace started with the Stuxnet strike against Iranian nuclear program (Gross, 2011). In addition to these, during the Gaza crisis, Israel Defense Forces used cyberspace in offensive means through engaging in on-going cyber-attacks in the region (Newman, 2019).

By increasing the use of cyber-attacks, the critical infrastructures of nations have become the main referent object in cyber-security. Even though critical infrastructure protection requires actions more than cyber-security means, cyber-threats have always been the initial driver (Cavelty, 2015). For instance, while in 2009, Russia and China attacked the United States' electric grid, according to speculations, in 2015, Iranian Cyber Arms caused massive electric outages in 44 provinces in Turkey (Gorman, 2009; Halpern, 2015). Moreover, in 2015, Russian hackers made cyber-attacks against the Ukrainian power grid, especially against country's three main energy distribution companies to disrupt electricity supply (Zetter, 2016). In 2019, Russia claimed that its electrical grid was attacked by American hackers (Greenberg, 2019). This is why, states have been trying to secure critical infrastructure against possible external cyber-threats. In this regard, the United States Department of Homeland Security works with several industries and companies to uncover vulnerabilities against cyber-attacks and to help the well-being of state's economy and critical infrastructure through enhancing the security of the control system network and the building of smart grid networks (Holland & Mikkelsen, 2009).

As it is understandable that the cyber-attacks have been mainly conducted against the states' energy infrastructures. While the increasing modernization and digitalization in the energy sector make energy systems smarter and provide consumers more benefits from modern energy services, the digitalization process also puts itself into jeopardy as there is increased exposure to cyber-attacks and cyber-incidents, which are great risks against the energy supply and the privacy of databases (European Commission, 2020a). Generally, any type of attacks against the energy systems can cause a loss of power in a large area for a long time, and such attacks can turn into a natural disaster for states by obstructing methods for meeting energy demands. Therefore, according to the World Energy Council's report (2016), the cyber risk in the energy sector is not just a critical threat for nations' energy security but is also an important variant for a strong nation and economy. Since the energy sector is initially run by the private corporations and companies, which control the crucial part of the critical state infrastructures, the cyber-attacks threaten their systems and profits.

Currently, energy companies are mainly criticized because of their lack of spending on cyber-security while there is increasing danger. In this sense, Sourav Mukherjee (2019) underlines the four possible improvements for the energy sector to secure itself against possible attacks and these are: improving the insurance coverage for threats, ensuring that both large and small electricity generators and grind operations stand by government rules to protect critical infrastructure and have the resources to invest in cyber defense, financing public resources to educate cyber-security experts and finally, funding cyber-security based research studies. In the same manner, the European Commission (2020a) pays close attention to cyber-security issues and underlines the importance of the development of defense mechanisms by dealing with real-time requirements such as accelerating the reaction of energy systems against threats and establishing cascading impacts in which the electricity grids and gas pipelines are interconnected and combine legacy systems with new technologies.

2.3.3 Critical Infrastructure Security

The term critical infrastructure is mainly used to define systems and assets which are vital for the functions of a society and economy. In this respect, the term is associated with the different facilities, which are agriculture, the water supply, public health, transportation, security services, telecommunication, the economic sector and most importantly the energy sector in terms of its transmission and distribution of energy (Rouse, 2020). Therefore, as its mentioned in previous sections, the damage to critical national infrastructures, which includes "its destruction or disruption by natural disasters, terrorism, criminal activities or malicious interests", has an apparent adverse impact on the security of states and the well-being of citizens (European Commission, 2020a).

Currently, critical infrastructures are increasingly connected to cyber-space. The main reason of this is that "it is more cost-effective to manage large assets and systems with the help of software and network protocols rather than relying on human technicians" (Geers, 2009: 3). Nevertheless, the cyber nature of critical infrastructures makes them vulnerable, especially with societies' increasing dependence on critical national infrastructures. For instance, the 2006 blackout in

Europe, “originated in Germany but ended up affecting approximately 5 million households in France, and another 10 million households in Belgium, Germany, Italy, Portugal, Spain, and Eastern Europe, as well as reaching as far as North Africa” (Onyeji et al., 2014: 55). Therefore, these blackouts demonstrate the transnational dependency on the transmission of energy and highlight the potentially important cross-border impacts. In this sense, societies’ growing dependence on critical infrastructure systems lead to the birth of a new dimension of cyber-threats on critical infrastructure

In terms of the cyber-attacks against the critical infrastructure, while some mainly focus on the non-state actors’ engagement in pursuing cyber threats, others emphasize the nation-states’ engagement. On one hand, scholars emphasize that sovereign states are unlikely to seek cyber-attacks on critical infrastructure because the global economy is obviously interconnected, and would not try to harm others because it would also mean harming themselves (Geers, 2009). Therefore, scholars turn its face to non-state actors such as terrorist organizations by claiming, particularly, that critical energy infrastructure is an initial target of cyber-attacks by non-state actors. For instance, in 2013, a terrorist organization attacked Algerian gas plant, which is considered as one of the worst terrorist attacks on gas plants (Chikhi, 2013). On the other hand, others predominantly focus on nation-states as attackers. In 2015, the Ukrainian power grid was attacked by the Russian hackers. The cyber-attackers hacked the Ukrainian electricity network and switched off 3 power grids to electrical substations (Zetter, 2016). Moreover, in 2016, the Ukraine suffered another Russian cyber-attack. This time hackers struck an electric transmission station in

Kiev and blacked out one-fifth of the total power capacity of Ukrainian capital (BBC 2017).

After that, whether the cyber attacked is engaged by nation-states or non-state actors, it is clear that cyber-security risks represent a general threat against the energy sector, more specifically the electricity and oil and gas infrastructures. Tackling cyber threats in the energy sector is mainly dependent upon the business activities of those energy sectors which negatively affect the states' reputation, economy, and well-being of society (Onjeyi et al., 2014). In this regard, the difficulty with cyber-security risk is that it is highly "problematic to manage, monitor and measure" (2014: 56). Even identifying the likelihood and impact of cyber-attacks on critical energy infrastructure and the effectiveness of companies' capacity to mitigate them has proven very problematic. Nevertheless, even though an large number of cyber-attacks have targeted the electricity infrastructure of systems, energy security has become a vital consideration under the critical infrastructure sectors, this does not mean that other critical infrastructure sectors could not be faced with any cyber-attacks.

The integrated security concerns mentioned in this section have not only directed social science, technology, or military means. States and intergovernmental organizations have taken action to ensure the security of energy, cyber and critical infrastructure, as the consequences of threats to any of these infrastructures will harm the states deeply. However, although the first two concepts, energy as a valuable trade object and cyber space as a new reality in the world are highlighted by the states, critical infrastructure protection has been ignored. Indeed, critical infrastructures are the most important building blocks of a functioning state and the basis of public prosperity.

CHAPTER III

EVALUATION OF THE CRITICAL INFRASTRUCTURE SECURITY AND CYBER SECURITY PRACTICES IN THE UNITED STATES, THE EUROPEAN UNION AND TURKEY

In today's world, all technical devices are connected to the network systems which are potentially the back door for the cyber-attacks to exploit such systems. Even though critical infrastructures are not considered an important element of the nation's security, the number of security implications and operations of cyber-attacks on critical infrastructure systems are increasing. In this regard, dealing with why and how the critical infrastructures are protected from cyber threats has become a new reality for states. Therefore, in order to understand how states perceive the issues around critical infrastructure security in such a complex cyber environment and to compare the critical infrastructures and accordingly cyber-security in the United States, the European Union and Turkey, this section mainly analyzes the definitions of critical infrastructure, cyber-security and cyber threat, the legislative and institutional strength and how budgets are allocated to ensure these state's critical infrastructure protection.

3.1 The United States

3.1.1 Overview of Critical Infrastructures

Critical infrastructure, as a term, is generally used to describe several different assets and facilities that are essential for the functions of modern societies, such as shelter, heating, agriculture, water supply, health, transportation and communication, electricity, security services and various other economic sectors. While there is no commonly agreed on definition of this term, excessive dependencies between critical infrastructures are a common cause of failure (International Atomic Energy Agency, 2007; NSW Department of Justice, 2018). The failures caused by interdependencies have a significant impact on the functioning of critical infrastructure; as a result, the protection and mitigation of such infrastructure have to become one of the most fundamental considerations.

In this respect, the importance of critical infrastructure protection as a national program was, for the first time, displayed in 1998 in the United States with the Presidential Policy Directive 63 (PPD-63) issued by President Bill Clinton. Moreover, in 2003, President George W. Bush updated the directive through the Homeland Security Presidential Directive 7 (HSPD-7). Generally, both directives describe the United States as having such a vital critical infrastructure that any type of incapacity, incidents or destruction of such systems would have a destructive effect on the country's national, economic, and public security. Rather than only identifying the importance of the critical infrastructures through policy directive, the concept of critical infrastructure is defined under the Critical Infrastructures Protection Act of 2001 (2001: 6) as:

> systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters

The United States government accepts 18 critical infrastructure sectors under the Presidential Policy Directive 21 (PPD-21), which was passed in 2013 and revoked the previous HSPD-7, establishing one of the most important American national policies for identification and prioritization of critical infrastructure protection. According to PPD-21, the 18 American critical infrastructure sectors are: “chemical sector, commercial facilities sector, communications sector, critical manufacturing sector, dam sector, defense industrial base sector, emergency services sector, energy sector, financial services sector, food and agriculture sector, government facilities sector, healthcare and public sector, information technology sector, nuclear sector, transportation systems sector and the water systems sector” (Cybersecurity and Infrastructure Security Agency, 2020a). In this regard, unlike other countries and intergovernmental organizations, the United States embraces a high number of critical infrastructure sectors, especially those that are essential for the progression of the society. The designation of those sectors as a part of the national critical infrastructure is an important process because, in that way, the government determines sectoral priorities and then provides useful legislation, policies, and protection systems accordingly.

On November 16, 2018, President Donald J. Trump signed the legislation called the Cybersecurity and Infrastructure Security Agency Act of 2018, which abolishes the mission of the former National Protection and Programs Directorate (NPPD), which was designed to reduce and eliminate threats to American critical physical and cyber infrastructure. The NPPD also established Cybersecurity and Infrastructure Security Agency (CISA) which itself has several goals, such as providing free tools and resources for public and private sectors to increase their security, facilitating the assessment of critical infrastructure weaknesses, providing training, encouraging information sharing and fostering sectoral and international partnerships (Department of Homeland Security, 2019a).

Several governmental institutions exist in the country specifically to engage the national critical infrastructure. For instance, the National Infrastructure Coordinating Center (NICC) and the National Cybersecurity and Communications Integration Center (NCCIC) integrate the critical infrastructure partnership among sector owners and operators through working with them regarding certain issues (e.g. prevention, protection, mitigation, response and recovery actives) within the critical infrastructure protection. While NICC is mainly essential for critical infrastructure partners to “obtain 24/7 awareness and connect data and information for securing America’s physical infrastructure”, NCCIC applies “analytic resources, generates situational awareness, coordinates synchronized response and recovery efforts during the emergence of cyber threats or incidents by coordinating with law enforcement, national intelligence, international computer emergency readiness teams (CERT), national analysis centers and infrastructure partners” (Department of Homeland Security, 2013: 1-3). In order to ensure the successful and secured information flow between public and private critical infrastructure sector partners, the Homeland Security Information Network-Critical Infrastructure (HSIN-CI) was established (Department of Homeland Security, 2019b).

3.1.2 The Role of Cyber Security in Critical Infrastructure Protection

Whereas governments like the United States has taken several precautions to secure their critical infrastructure for a long time, as the current digital community becomes increasingly connected, the precautions should be modified in accordance with the evolving cyber threats. As Schatz et all. (2017: 53-57) point out, cyber-security is generally understood as “the protection of computer systems and networks from any kind of damage to their hardware, software, and other electronic data, as well as the disruption or intervention of the service they provide". In addition, the International Telecommunication Union (ITU) defines the term cyber-security as "a collection of tools, policies, security terms, risk management, training, practices, assurance, and technologies to protect the cyber environment and organizations' and users' assets which include connected devices, infrastructure, telecommunication, and information systems" (Solms & Niekerk, 2013: 97). Therefore, it turns out that cybersecurity objectives are predominantly associated with the systems' availability, continuity, and integrity of the cyberspace.

In the same direction, American institution CISA describes cybersecurity as "an art of protecting networks, devices, and data from the unauthorized access or criminal usage that disrupt the practice of ensuring confidentiality, integrity, and the availability of information" (Cybersecurity and Infrastructure Security Agency, 2019a). Nevertheless, not only the federal institutions in the United States define the term but also there are multiple legislations and enforcements legalize the definition of cybersecurity. For instance, the acts numbered as National Security Presidential Directive (NSPD-54) and Homeland Security Presidential Directive (HSPD-23) under Cybersecurity Policy (2008: 3) defines cybersecurity:

> prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation

Defining the term cybersecurity is important because the chosen definition determines the boundaries of actions that can be taken to enforce cybersecurity. By looking at the two mentioned definitions regarding the cybersecurity of the United

States, it can be concluded that any types of risk against national cyberspace and also critical infrastructure systems are issued as both crucial physical and cyber threats. In this regard, CISA's dealing with the definition of cybersecurity is important because CISA is seen as a main governmental institution to boost cybersecurity and combat critical infrastructure problems.

Another important issue is how to identify threats or attack types and how to strengthen the national infrastructure rather than being restricted to the definitional problem. The cyber threats in the United States include "natural disasters, environmental and mechanical failures, inadvertent actions of unauthorized uses" and also "deliberate threats from national governments, terrorists, industrial spies and organized crime groups, hacktivists, and hackers" (Cybersecurity and Infrastructure Security Agency, 2020b; Government Accountability Office, 2005). As a result of the digital information technology making the world so much smaller and more complex, critical infrastructure governments including the United States are not from such threats. For instance, the United States Department of Homeland Security (2018) has denounced the Russian government for using cyber threat actors to target American government institutions and multiple critical infrastructure sectors such as "energy, nuclear, commercial facilities, water supply, aviation, and manufacturing sectors" since 2016. Therefore, to overcome the cyber threats against the nation's cyberspace and critical infrastructure systems, the United States has implemented new legislation and also founded multiple federal organizations to cope with such a significant problem.

3.1.3 The Legal and Institutional Strength of Cyber Security and Critical Infrastructure Security

To handle the threats on critical infrastructure in cyberspace, the United States, first, has to legislate specific laws and enforcement procedures to draw a legal path for its security of cyberspace. In this sense, there are three main cyberspace and security regulations, which were the first attempts to mandate cybersecurity in the healthcare system, financial institutions, and federal agencies (to protect their systems and data and information), and these are: the 1996 Health Insurance Portability and Accountability Act (HIPAA), the 1999 Gramm-Leach-Bliley Act (GLBA), and the 2002 Homeland Security Act, which included the Federal Information Security Management Act (FISMA).

HIPPA was signed by President Bill Clinton in 1996 to modernize the flow of healthcare information systems, regulate healthcare insurance industries through the provision of protection against fraud and theft and to cope with the limitations on insurance coverage (Atchinson & Fox, 1997; HIPAA Guide, 2018). In 1999, Clinton also signed GLBA to modernize and develop the financial industry. Under the GBLA, the Financial Privacy rules were born—they force financial institutions to provide customers with a privacy notice that "explains the information collected about the consumer, where that information is shared, how that information is used, and how that information is protected" (U.S. Code No:6801; U.S. Code No: 6809). These rules and privacy agreements regarding the insurance and financial sector started to provide cyber protection for consumers and data providers. Even though these two laws did not cover every dimension of cybersecurity in the United States, they can be seen as the early foundations of the cybersecurity system within the nation.

In 2002, the FISMA was signed. The act generally defines and regulates the comprehensive frameworks to protect federal information and assets against cyber threats. More specifically, FISMA has brought attention within the federal government to cybersecurity and has explicitly emphasized a risk-based policy for cost-effective security. While in 2002 FISMA was responsible for "ensuring that appropriate officials are assigned with security responsibilities to review the security controls in federal systems and authorize system processing prior to operations" (National Institute of Standards and Technology, 2020), in 2014, FISMA was updated and new responsibilities were added: "codifying Department of Defense's authority to administer the implementation of information security policies for non-national security federal executive branch systems (including that providing technical assistance and deploying information technologies); clarifying the Office of Management and Budget's oversight authority over the government's information security practices; and eliminating inefficient reporting" (Federal Information Security Modernization Act of 2014: U.S. Code No:2521). Generally, with FISMA's regulation and enforcement, the United States was able to start strengthening its federal agencies in an increasingly cyber environment.

In addition to the three mentioned regulations, the United States also passed five important laws about the cybersecurity of the nation. In 2014, the government signed the Cybersecurity Enhancement Act of 2014 to "increase the number of public and private partnership to improve cybersecurity-related R&D projects, employ training and raise public awareness and preparedness for cyber threats preparedness" (Cybersecurity Enhancement Act of 2014: U.S. Code No:1353). In 2015, both the Cybersecurity Protection Advancement Act and the Cybersecurity Information

Sharing Act came into force. On the one hand, the Cybersecurity Protection Advancement Act requires several federal agencies to develop their cyber procedures regarding the essential risks and incidents, educate the public on securing information technology systems, develop safeguards to protect cybersecurity information networks against any type of threat, develop the capabilities of existing industry standards, especially regarding the critical infrastructure sectors, and allow private agencies, for cybersecurity purpose, to share and adopt NCCIC or other governmental measure indicators (National Cybersecurity Protection Advancement Act of 2015). On the other hand, the Cybersecurity Information Sharing Act only focuses on the information, data, and network sharing through the encouragement of the sharing of Internet traffic information between the United States government and several technology and manufacturing industries (Cybersecurity Information Sharing Act of 2015). With these legislations, the government gained the power to create a system for federal institutions, especially in terms of assessing the severity of cyber threats and attack of the private sector and managing industry-based standards.

Moreover, the United States has been making yearly updates Cybersecurity Legislation since 2015, with the last legislation made in 2019. With this most recent version, 31 American states have enacted this legislation, which mandates that both private businesses as well as government agencies: implement training and security practices; create task forces and commissions; research the use of blockchain for security; provide security for critical infrastructure' exempt cybersecurity operations information from public record laws; tackle the security of connected devices; regulate the insurance industry; provide funding for the improvement of security measures; and address the cybersecurity threats and attacks to elections

(Cybersecurity Legislation 2019). Whereas previous legislation had always focused on various domains of cybersecurity, the National Cyber Strategy of 2019 only addresses the issues regarding the critical infrastructure security of the United States. This strategy indicates that government partnership with the private sector is crucial for “embracing a collective risk-management approach to mitigate vulnerabilities and raise the base level of cybersecurity among different critical infrastructure” (The White House, 2018: 8). In that way, while the American government adopts a consequence-driven approach to prioritizing the practices that decrease the potential cyber threats and considerations, which could cause large scale or long-term adversaries for the national critical infrastructure systems, the strategy also uses deterrence strategy by identifying and eliminating malicious cyber threats.

Within the Department of Homeland Security, the Computer Emergency Readiness Team (US-CERT) is responsible for improving America’s cybersecurity posture, coordinating cyber information sharing, identifying and reducing the cyber threats and incidents, connecting and spreading cyber threat warning information and coordinating the response activities to these threats (Department of Homeland Security, 2020). US-CERT is also directly linked with the CISA which is one of the leading organizations in the United States that regulates critical infrastructure protection. Since 2016, to develop cybersecurity and critical infrastructure protection, CISA has also annually publish the National Infrastructure Protection Plan (NIIP) that focuses on developing technology, tools, and methods for strengthening the long-term security and resilience of critical infrastructure (Cybersecurity and Infrastructure Security Agency, 2019b). Beforehand, in 2013, the National Institute of Standards and Technology (NIST) Cybersecurity Framework was enacted with the signing of the Presidential Executive Order 13636, titled Improving Critical Infrastructure Cybersecurity, and “led the development of a framework to minimize cybersecurity risks to critical infrastructure systems, seeking feedback from the public and private sectors and incorporating best industry practices through the following five practices: to identify, protect, detect, respond and recover” (Jong-Chen & O’Brien, 2017: 2-3). In addition to these, various other federal agencies have worked to achieve the requirements of the several American laws on cybersecurity mentioned above and the most important ones are: the Department of Homeland Security, the Federal Bureau of Investigation, the Department of Defense, the Cyber Command under the United States Strategic Command, the Cybersecurity and Infrastructure Security Agency, the National Security Agency, the National Cyber Security Division, and the Comprehensive National Cybersecurity Initiative.

Table 1: The United States’ Agency Based Cyber Security Funding, 2018-2020 (Office of Management and Budget, 2020: 306)

The United States Agencies Total Cybersecurity Funding (in million dollars)

	FY 2018	FY 2019	FY 2020
Department of Agriculture	262	480	311
Department of Commerce	350	403	392
Department of Defense	8,048	8,734	9,643
Department of Education	104	139	143
Department of Energy	448	520	557
Department of Health & Human Services	359	474	460
Department of Homeland Security	1,859	1,921	1,919
Department of Housing & Urban Development	15	35	25
Department of Justice	821	824	881
Department of Labor	93	93	94
Department of State	362	363	400
Department of the Interior	88	103	101
Department of the Treasury	445	505	522
Department of Transportation	185	224	232
Department of Veterans Affairs	386	530	513
Environmental Protection Agency	21	44	45
General Services Administration	72	79	80
National Aeronautics & Space Administration	171	169	171
National Science Foundation	247	239	224
Nuclear Regulatory Commission	25	32	29
Office of Personnel Management	38	45	47
Small Business Administration	9	16	16
Social Security Administration	167	225	205
U.S. Agency for International Development	44	68	44
Non-CFO Act Agencies	362	382	372
Total (in billion dollars)	**14,978**	**16,645**	**17,435**

Over the years, the United States has also increased its spending on cyber-security. In the United States, each federal agency has its own cyber-security funding and Table 1 provides detailed documents on the cyber-security budget of 25 American agencies. Overall, cyber-security spending of the American government increased from 14.98 billion dollars in 2018 and 16.64 billion dollars in 2019 to 17.44 billion dollars in 2020.

3.2 The European Union

3.2.1 Overview of Critical Infrastructures

Critical infrastructure is vital for European societies. As the European Commission (2005) asserts, in line with the United States, critical infrastructure of the European countries includes various sectors of energy, information and communication technologies, water systems, food supply, healthcare, financial systems, public order and security, civil administration, transportation, chemical and nuclear industries, and space research. Because the mentioned physical and information technology facilities are essential to maintaining Europeans' way of life, any type of damage or destruction of critical infrastructure by natural disasters, terrorism, attacks or incidents would have serious consequences for the security of the European Union and the well-being of its citizens (European Commission, 2019, 2020). However, even though the United States declares 168sectors, the European Union mentions only 11 sectors as a part of the critical infrastructure.

According to the European Council Directive No. 114 (2008), the main responsibility to protect European critical infrastructure is given to member states and their operations. The directive also underlines that the existence of critical infrastructures that will have a cross-border impact on their destruction is covered under the European Critical Infrastructure (ECI). ECIs within European borders should be protected and monitored by a bilateral and multilateral collaborative effort between member states.

Even though the actions of member states are essential to securing critical infrastructure sectors in Europe, by determining the frames of the actions through legislation and institutions, the European Union could become an important coordination and audit center. The European Commission (2019) has launched the European Programme for Critical Infrastructure Protection (EPCIP) and an initiative called Critical Information Infrastructure Protection (CIIP) to improve the protection of critical infrastructure of European Union member states through strengthening the security and durability of vital information and communication technology infrastructure. Moreover, the Joint Research Center (JRC) under the European Commission coordinates the European Reference Network for the Critical Infrastructure Protection (ERNCIP) provides "technical support with experimental facilities and laboratories that can share knowledge and expertise in order to better align test protocols throughout Europe, leading to better protection of critical infrastructures and evaluating buildings' and transport systems' ability to resist all types of threats" (European Commission, 2019). In addition, the Geospatial Risk and Resilience Assessment Platform (GRRASP) is used for "the analysis of the complex network systems, such as analyzing critical infrastructure disruptions and cascading impacts at the regional or state level and identifying most vital or weak elements of the network, by considering the cross-sectoral and cross-border interdependencies between European countries" (European Commission, 2016).

As mentioned before, although the United States accepts the nuclear sector as a part of the critical infrastructure, the European Union's definition of the term of critical infrastructure does not exactly consider the nuclear sector within its explanation. Separately, the European Commission (2020) focuses on "the prevention of and response to terrorist attacks using chemical, biological, radiological, and nuclear (CBRN) materials and for the protection of public areas" because the European Commission asserts that any type of CBRN threat would be harmful for the critical infrastructure. For this reason, European Union member states "share their best practices, train together, and develop common capabilities". Moreover, to support those practices, the Commission adapted an action plan in October 2017 to enhance preparedness against CBRN threats and reduce the possibility of illegal acquisition of dangerous materials and incidents (European Commission, 2020). In this regard, the European Union also works closely with the external states and intergovernmental organizations such as the United States, International Atomic Energy Agency, the Organization for the Prohibition of Chemical Weapons, and NATO.

3.2.2 The Role of Cyber-Security in Critical Infrastructure Protection

Like the United States and other agencies, the European Union also defines the concept of cybersecurity in its own way. According to the Joint Communication to the European Parliament, the European Economic and Social Committee and the Committee of the Regions' Report (JOIN) (2013: 1), cyberspace has a significant impact on all parts of a society and citizens in terms of "fundamental rights, social interactions and economies" that mainly depend on information and communication technologies. Whereas open and free cyberspace has been promoting political and social inclusion globally, various government and public facilities should be protected within a cyberspace that opens a discussion about the cybersecurity. JOIN (2013: 14) defines cybersecurity as:

> the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure

However, Brookson et al. (2015), in the ENISA report, underline that the definition of cybersecurity must be wider to include protections against the different risks for agencies and data, specifically when the concept is understood as a synonym of information security. The complexity is even further raised by the popularity of the term cybersecurity in the mass media, which tend to use the term as a catch-all phrase that often attributes anything or everything that can disrupt computers or more broadly the Internet as cybersecurity threats. Nevertheless, in the military realm, institutions approach the term from an even wider and much more strategic phase by perceiving the term in connection with the terms of cyber defense and war. Given this context, although the European Union agencies do not comprehensively engage the term, Brookson et al. (2015) come up with five domains of cybersecurity within the European security realm, which are: communication security, operations security, information security, physical security and public security.

Cybersecurity incidents in Europe are increasing at an alarming pace. This could disrupt the critical infrastructure of the states as well as “the supply of essential services that citizens take for granted such as water supply, healthcare, energy, transportation, or communication” (JOIN, 2013: 1). RAND Europe’s report published by the efforts of the European Commission, points out the five cyber threats and these are: unauthorized access, destruction, disclosure, modification, and denial of services report (van der Meulen, et al., 2015). In addition, Europol (2018) and the European Court of Auditors (2019) considers any malware that includes viruses, trojans, ransomware, worms, adware and spyware, or DDoS attacks to be cyberespionage and attacks on critical infrastructure.

The European Union has been recognized that ensuring cybersecurity against diverse types of threats is critical for the prosperity and security of the member states. As European society's dependence on cyberspace grows, so the number of cyber threats and attacks increase as well. According to European Parliamentary Research Service (2019: 1), there will be "125 billion devices connected to the internet by 2030, and 90 % of individuals older than 6 will be online", which gives rise to concerns about vulnerabilities to cyber threats. More specifically, "given the accessibility and relatively low cost of operations, anybody, be they individuals, professional criminals, state or non-state players, could become a perpetrator" (2019: 2). Worldwide, countries are continually developing their offensive cyber capabilities because of the geopolitical realities and goals. With the number of attacks increasing so rapidly, the disruptive potential, especially in terms of financial damage, is alarming. The global cost of cyber threats is estimated at about €530 billion. This is why, Commission President Jean-Claude Juncker said in 2017 "that cyber-attacks pose more danger to democracies and economies than guns and tanks" (2019: 2).

Therefore, to protect the cyberspace of Europe, governments have several tasks to fulfill such as establishing safeguarded access, accountability and sustainability, respecting, and protecting fundamental rights in cyber world and maintaining the reliability of the cyber environment. Nevertheless, cyberspace is not controlled by a single entity. There are currently several stakeholders involved in "the management of cyber resources, protocols, and standards, and even in the future development of the Internet" (JOIN, 2013: 4). Especially, the private sector and commercial entities possess and operate in important parts of the cyber world and any initiative aiming to be successful in this area should consider the companies (COM, 2009).

As cyber operations entail many risks, such operations should be protected by comprehensive and extensive regulations. Existing cybersecurity regulations all cover different aspects of business operations and often vary by the region or country in which a sector operates. As a result of the differences in European states and infrastructure, the European Union should seek to implement strict cybersecurity standards and regulations. In this regard, the first step was defining the term of cybersecurity by shaping the perspective of member states.

3.2.3 The Legal and Institutional Strength of Cyber Security and Critical Infrastructure Security

The European Union became an observer organization to the Council of Europe's Convention on Cybercrime Committee in 2001. Also, COM/2001/0298 was issued to ensure citizens' communication and information security. Since then, the European Union improves its cyber resilience against the increased number of cyber threats and activities that has accelerated (European Court of Auditors, 2019). The Cyber Security Strategy of the European Union came to the scene with the 2008 global economic crisis to reduce the exposure and vulnerability of the European economy and increase the competitiveness of European countries (Kovacs, 2018). To do this, in 2010, the European Commission declared a strategy titled Europe 2020 which includes the five main objectives for cybersecurity and these are: "achieving cyber resilience, reducing cybercrime, developing cyber defense policy and capabilities, developing industrial and technological resources for ensuring cybersecurity and establishing an international cyberspace regulation to promote the values of the European Union" (COM, 2010: 8-9). During that time, the European Commission also announced the European Digital Agenda to establish a unified digital market for European Union member states and analyze the existing economic and social challenges such as interoperability of vulnerabilities and cybercrimes for developing and defining several actions in cyberspace (COM, 2010).

After declaring the Cyber Security of the European Union and European Digital Agenda, the General Data Protection Regulation (GDPR) and Directive on Security of Network and Information Systems (NIS) were started in order to regulate the European cyber environment. First of all, GDPR, which has an aim to create a common standard for data protection in Europe, was set into place in 2016 (EU GDPR Portal, 2020). More specifically, GDPR, based on the lawfulness, fairness, and transparency, gets information from the data controllers about when and how personal information is processed, stored, and handed over, and requires that the data controllers provide the customers with a copy of their personal information. GDPR also contains a very severe sanction tool. Regarding the GDPR legislations, while the penalty is no less than 4% of the annual turnover of the data controllers that violate the GDPR or in some circumstances the penalty equals 20 million euros, the directive also resorts to a penalty rate amounting to 2% of the annual turnover in case of failure to notify supervisory authority (Regulation (EU) 2016/679). Although GDPR is not directly related to issues such as state sponsored cyber threats or other cyber-attacks, it indirectly regulates the cyber environment of Europe by increasing the transparency of data management among European Union member states.

The NIS is also announced under the European Union's enforcement in 2016 that it was establishing the first overall high-level cybersecurity on the continent (Directive (EU) 2016/1148). The NIS directly affects the digital service providers and operators of essential services whose operations would be affected by a security breach of Europe's critical economic and societal activities (The Register, 2016). Under the NIS regulations, digital service, and data providers "should collaborate and exchange information with the other European Union regulatory bodies and data protection authorities" (JOIN, 2013: 4). In this context, security requirements mainly concern the technical measures that manage the risks of cybersecurity bodies in a preventative manner. When data providers and operators have to provide information that allows for an in-depth assessment of the information system and security policies in Europe, NIS tries to improve the preparedness and engagement of the public and private sector against possible cyber threats. As the large majority of global network and information systems are privately owned or operated in Europe, developing sectors' technical level and cyber capacity, their sharing of best practices and collaboration between public and private areas become a vital consideration.

In 2018, Regulation (EU) 2018/1725 of the European Parliament and of the Council, which is repealing the Regulation (EC) No 45/2001, engages with the personal data protection. Similarly, CERT-EU was established to "contribute to the security of the information technology infrastructure of all European Union agencies by helping to prevent, detect, mitigate and respond to cyber-attacks and enable cyber-security information change and incident response coordination" (CERT-EU, 2020). In addition, to provide the mentioned standards, CERT-EU collects and processes the data of European Union institutions. Moreover, CERT-EU also closely works with the ENISA. In 2019, the European Council (2020) adapted the Cybersecurity Act of 2019 which introduces the common cybersecurity certification system for creating specific information and communication technologies processes, products and services among member states, and clarifying ENISA’s important role as the European Union agency for cybersecurity and critical infrastructure protection. Besides these, cybersecurity efforts in Europe have a military dimension as well. For this reason, the High Representative under the European Union invites the member states and the European Defense Agency to collaborate in certain circumstances such as assessing operational cyber defense requirements, promote cyber defense capabilities, and develop cyber defense policy defense frameworks to protect networks within the Common Security and Defense Policy (CSDP) missions such as “risk management, threat analysis and information sharing” (JOIN, 2013: 3). Nevertheless, the collaboration also ensures the coordination with the international actors such as NATO, OECD, OAS, the UN, and other international partners to strengthen the defense capabilities and identify areas for open dialogue.

Among the different types of institutions, the most important one is the European Union Agency for Network and Information Security (ENISA), which was set up by the European Parliament in 2013 to regulate the member states’ actions of security breaches, and to create and implement policies. ENISA supports the member states’ cybersecurity structure and provides direct assistance by taking a hands-on approach to working with operation teams of the European Union (European Union Agency for Cybersecurity, 2020a; Regulation EU No 526/2013). In addition, to achieve increased cybersecurity awareness, ENISA is also working with other organizations such as Europol and Eurojust, and also piloted the “European Cybersecurity Mont” by collaborating with the United States on the Working Group on Cybersecurity and Cybercrime.

As mentioned before, to secure member states' critical infrastructure against any type of cyber threat, the European Commission (2019) also launched the European Programme for Critical Infrastructure Protection (EPCIP) and the European Reference Network for Critical Infrastructure Protection (ERNCIP). While the EPCIP aims "to improve the protection of critical infrastructure in Europe, especially regarding the information and communication technology infrastructure", the ERNCIP provides "technical support under the Directive on European Critical Infrastructures and carries out different research activities such as the development of methods and tools for international cybersecurity exercises, the assessment of the vulnerability of networked infrastructures in case of extreme space weather events, and the evaluation of the resistance of buildings and transport systems against explosions" (European Commission, 2019).

In addition, since 2008, Critical Infrastructure Warning Information Network (CIWIN) is operating to deal with the member states' common threats against their critical infrastructure such as threats and terrorist attacks. Under the European Union Directive 676 (COM, 2008), CIWIN is a forum, which is established by member states' representatives, for exchanging information on the protection of critical infrastructures and alerts to states and the European Commission on immediate risks and threats to critical infrastructures.

The European Commission (2019) also underlines that global navigation systems called the Global Positing Systems (GPS) and Galileo, in the coming years, would become the primary sources of European countries to ensure the safety of their critical infrastructure systems and operations.

As mentioned, ENISA is the essential branch under the European Union that specifically engages with the concept of cybersecurity. For this reason, ENISA holds and regulates the annual cybersecurity budget of the institution. While in 2018, the organization divided 11,449 million euros, this number increased in 2019 as 16,932 million euros and the draft budget of 2020 estimates this number will be 21,785 million euros (European Union Agency for Network and Information Security, 2020, 2019, 2018).

3.3 Turkey

3.3.1 Overview of Critical Infrastructures

As a commitment to the Cyber Defense Concept of NATO, Turkey prepared the National Defense Policy in 2009 which can be understood as a shadow of the first effort on critical infrastructure protection in Turkey. Whereas the policy reflects the importance of implementation, determination and protection of critical infrastructure, the document does not provide any specific information about what critical infrastructure is or how to ensure its security. In 2009, the draft law about e-government and information society was prepared by the working group under the Prime Ministry (Karabacak & Özkan, 2009). Since then, several other legislations have been published about the information technology issues in Turkey. However, like primer legislations, the e-government draft law also does not contain the expression “critical infrastructure”. Even though there are some signs to refer the concept, it is not clearly defined or explained (European Commission, 2015).

Whereas there is no official published law or legislation that directly engages with the definition of critical infrastructure in Turkey, the draft document prepared for the national cybersecurity strategy by the Turkish Information Security Association in 2012 touches upon the subject of critical infrastructure. The documents, as stated in Bıçakçı et al.’s report (2016: 7), assert that critical infrastructures are the national structures that:

> damages to or the destruction of which would hamper the continuity of public services and public order and; the partial or complete loss of their functionality would have detrimental effects on public health, safety, security and on economic activity and on the effective and efficient functioning of the government

Nevertheless, 2016-2019 National Cyber Security Strategy of Turkey (2016: 8) indicates only 6 critical infrastructure sectors as “electronic communication, energy, water management, critical public services, transportation, banking and finance”. As other elements of the nation, critical infrastructures should be protected from the several threats. In this regard, “the National Cyber Security Strategy and 2013-2014 Action Plan under the Ministry of Transport, Maritime Affairs and Communications in Turkey, which became effective under Cabinet Decision No. 2013/4890 dated to 25 March 2013” (2016: 5), suggests that Turkey’s critical infrastructure is vulnerable against various threats including cyber threats because the important part of the critical infrastructure and services rely on information technology systems to continue their operations and services. Also, Bıçakçı et al. (2016) add that in addition to systemic vulnerabilities of cyber space in Turkey, weakness in terms of critical infrastructure arose from the lack of knowledge among the society, institutions and high-level legislative processes regarding cyber security, less developed information technology system and inadequacy of national legislation.

3.3.2 The Role of Cyber Security in Critical Infrastructure Protection

There are multiple different definitions of cyber-security that exist in Turkey. In this context, Information and Communications Technologies Authority (2020) defines the concept as “a set of tools, policies, security concepts, security guarantees, guides, risk management approaches, activities, training, best practices and technologies used to protect the assets of organizations, organizations and users in cyber space”. In the same direction, 2016-2019 National Cyber Security (2016: 10) defines the cyber security as:

> protection of information systems that make up the cyber space from attacks, ensuring the confidentiality, integrity and accessibility of the information being processed in this space, detection of attacks and cyber security incidents, putting into force the countermeasures against these incidents and then putting these systems back to their states previous to the cyber security incident

While mentioned guides provide a definition of cyber security, they do not mention the main domain of the concept which is cyber-attack. In this regard, 2016-2019 National Cyber Security Strategy (2016: 9-10) defines cyber-attack as:

> operations carried out deliberately by a person and/or information system at any place in cyber space for the purpose of compromising the confidentiality, integrity or availability of information systems in national cyber space

Turkey, like other countries and intergovernmental organizations, is affected by several cyber threats. Most recently, Turkey was faced with two different global cyber-attacks. The ransomware called Purge appeared in 2016 and targeted regular users as well as federal and private agencies. The notorious Stop ransomware, encountered in 2018, attacked more than 20,000 users globally (Kaspersky, 2019). As a result, Turkey is in the top-ten countries affected by those cyber threats.

The United States and several other European countries were not affected by these two global cyber-attacks called Purga and Stop because they were not targeting of the attack. However, the United States and especially Germany, as a one of the biggest European countries, have been affected by the malware named Ryuk which first appeared in 2018 and has been active through 2019. The Ryuk is known for attacking large organizations and governmental and municipal networks (Kaspersky, 2019). Even though in previous years Turkey did not undergo the same level of cyber-attacks that targeted the United States and European countries, it is shown that Turkey is still open to any type of cyber threat against its infrastructure as well. What is important at this point is not which country is targeted by which malicious malware or software, but whether it is targeted at all.

Table 2: Percentage of Internet Users Attacked in Each Country by Purga, (Kaspersky, 2019)

Top 10 Countries	**Percentage**
1. Russia	85.59
2. Belarus	1.37
3. Turkey	0.85
4. India	0.80
5. Kazakhstan	0.74
6. Germany	0.62
7. Ukraine	0.54
8. China	0.46
9. Algeria	0.40
10. United Arab Emirates	0.40

Table 3: Percentage of Internet Users Attacked in Each Country by Stop (Kaspersky, 2019)

Top 10 Countries	Percentage
1. Vietnam	10.28
2. India	10.10
3. Brazil	7.90
4. Algeria	5.31
5. Egypt	4.89
6. Indonesia	4.59
7. Turkey	4.30
8. Morocco	2.42
9. Bangladesh	2.25
10. Mexico	2.09

Until 2017, Turkey accounted for a whopping 77% of all targeted malware and ransomware detections in Europe (FireEye, 2017). Since then, the apparent hazardous impact of cyber-attacks increased globally. In Turkey, cybercrimes and attacks were engaged for the first time in 1991 with Law No. 3756 under the Turkish Penal Code. In particular, Article 20 mentions the information crimes as unlawful seizures of programs or data from a computer through their use, transfer or copy with the aim of harming people. Afterwards, in 2004 Turkish Penal Code Law No. 5237 classifies information technology crimes under three group of activities and these are: "access to information technology systems, denial of the systems and its disruption, data destruction or modification, and misuses of debit and credit cards" (Bıçakçı et al., 2016: 24).

In this regard, the Information and Communications Technologies Authority (BTK) categorizes cyber threats under five groups and these are: blocking services attacks, malicious software including virus, worm, trojan, key loggers, adware and spyware, phishing, spam, and monitoring the information systems (Ünver et al., 2010). Although Turkey understood the importance of the cyber security and has started to declare several explanations and strategies to engage with the subject, unlike other states and intergovernmental organizations, Turkey does not recognize the essential relations between cyber security and critical infrastructure protection.

3.3.3 The Legal and Institutional Strength of Cyber Security and Critical Infrastructure Security

While the Turkish Penal Code Law No. 3756 introduced the information crimes with the amendment in 1991, Turkish Penal Code Law No. 5237 in 2005 expanded on the previous amendment by classifying the information technology crimes under three group of activities. Moreover, when the Anti-Terror Law No. 3731 implemented in 2006 lays out the elements of terrorist activities, it also points out the list of crimes that may result from utilizing computer systems (Bıçakçı et al., 2016).

In the early 2000s, several documents on the matter of cyber security "e-Turkey Initiative Action Plan (2002), e-Transformation Turkey Project Short-Term Action Plan (2003-2004) and e-Transformation Turkey Project 2005 Action Plan" (Bıçakçı et al., 2016: 24) were released and aimed to regulate and ensure the security of federal and public information.

Besides these, other laws were drafted through the late 1990s and first half of 2000s, titled the Draft Law on National Information Security Organization and Its Tasks by the Ministry of National Defense. This draft law would contribute to the establishment of National Information Security Supreme Board which would be work with the several different organizations such as “the Prime Minister, Ministers of Justice, National Defense, Interior, Foreign Affairs, Transport, Industry and Commerce, as well as the General Secretary of the National Security Council, the Undersecretary for the National Intelligence Agency, the Commander of General Staff Communications, Electronic and Information Systems, and the Scientific and Technological Research Council of Turkey (TUBITAK)” to regulate the nation’s information technology policies (Aksakal, 1999: 438-457). The Supreme Board would also be tasked with the evaluation of changes in Turkey’s information security legislation and the establishment of the National Information Security Institution to enable several functions such as determining cyber threats, information security policies and the regulation of software and hardware systems (Bıçakçı et al., 2016). However, the draft law was not passed as a result of there being no consensus on the final draft.

Since then, although Turkey does not have any comprehensive cyber laws and legislation about cyber security, only the Ministry of Transport, Maritime Affairs and Communications have been declaring national cyber security strategy documents. First of all, National Cyber Security Strategy and 2013-2014 Action Plan (2013: 10) states that “the objective of the strategies is to create a basis for achieving the cyber security of all services, data and systems of public agencies, cyber security information systems of critical infrastructure which are operated by the public and private sectors and minimization of effects of the cyber threats and incidents”. While 2016-2019 National Cyber Security Strategy reflects the same concerns and strategies as the previous document, it asserts that, for the 2016-2019 period, there are 18 strategic objectives determined and these are generally about meeting the security needs of information and critical infrastructure systems, creating a legislation to meet the international standards, improving awareness, training personnel, encouraging research and development and increasing the coordination between public and private sectors.

Whereas several government institutions and agencies are working for regulating cyber space, there is no specific strong institutional structure that exists to bring national security strategies to life. For instance, the Telecommunications Authority was founded in 2000 and it was transformed into the Information and Communications Technologies Authority (BTK) in 2008. BTK works as “a regulator of the telecommunication systems and has a duty to ensure authorization, inspection, dispute resolution, protection of consumer rights, regulation of sectoral competition and dealing with technical regulations” (Bıçakçı et al., 2016: 26).

To share the duties of BTK, the Presidency of Telecommunication and Communication (TIB) was founded in 2005. However, the organization made several attempts to block access to over 100,000 websites and TIB as Turkey’s telecom national authority shut down in 2016. Moreover, Cyber Space Defense Centre (SOSAM) was established as “a research center under the National Information Systems Program to gather statistics on traffic data and cyber-attacks, focus on threat detection, and issuing warnings and precautions” (Şentürk et al., 2012: 118). Nevertheless, currently SOSAM has become an ineffective institution.

In 2001, TUBITAK established the Common Criteria Test Center to conduct common criteria assessments, provide consultancy and training for technic products

(Informatics and Information Security Research Center, 2020). TUBITAK also began to participate in NATO cyber security exercises and coordinate the Cyber Emergency Response Team (CERT) since 2007 (Erciş, 2008). However, CERT in another name USOM currently work under the BTK.

In 2012, the Cyber Security Council was established with an aim to “determine precautions that will be undertaken to improve cyber security, the implementation and coordination of programs, guidelines and standards” (Cabinet Decision No: 3842) and the Cyber Incidents Response Center was founded to “identify threats, develop and share warnings” (Bıçakçı et al., 2016: 31). However, the Cyber Security Council was closed in 2018.

The country only has one data protection legislation named as Personal Data Protection Law No. 6698 declared in 2016 and asserts that private sectors have to comply with the data protection procedures which is to the extent the process of personal data otherwise the will be faced with sanctions. Under this law, Turkish Personal Data Protection Board (KVKK) was established.

Although there seem to be too many organizations established to regulate cyber security in Turkey, actually they are all work under the Ministry of Transport, Maritime Affairs and Communications. Since 2012, with the Cabinet Decision No: 3842, the Ministry of Transport, Maritime Affairs and Communications has the authorization to go forth with policy making and action plans on cyber security in Turkey. The strategy called 2016-2019 National Cyber Security Strategy and Action Plan (2016) is last and most comprehensive strategy of the ministry in terms of the issues around cyber security and critical infrastructure. The strategy has three significant principles to ensure Turkey’s cyber security, and these are: “ensuring the security, confidentiality and privacy of all information services, transactions and data provided as well as systems that cover cyber space entirely, determining cyber security actions to minimize the impact of cyber security incidents and attacks and ensuring the higher efficiency of exploration and investigation of possible threats by judicial authorities and law enforcements and developing critical information technologies and products to ensure cyber security” (2016: 9).

In this regard, the Ministry of Transportation, Maritime Affairs and Communication collaborates with “the Ministry of Foreign Affairs, Ministry of Interior, Ministry of National Defense, Undersecretariat of Public Order and Security, National Intelligence Organization, Turkish Armed Forces General Staff, Information and Communication Technologies Authority, Scientific and Technological Research Council of Turkey, Financial Crimes Investigation Board, Presidency of Telecommunication and Communication. The Ministry of Transportation, Maritime Affairs and Communication also works with the Sectoral Cyber Incident Response Teams (CIRTs) in the critical public services and water management sectors, transportation sectors, electronic communication, energy, and finance sectors” (2016: 16-19). In addition, the NATO Cooperative Cyber Defense Centre of Excellence’s National Cybersecurity Organization envision the modernization of military sector in Turkey through the cyber defense training and laboratory systems.

Even though there are different organizations, which are not strong and unified, trying to grapple with the issues around cyber security in Turkey, unfortunately, there is no authority or center of critical infrastructure protection. Only the Ministry of Transportation, Maritime Affairs and Communication published a document, which is not a legal document, about the recommendation for securing sectors' critical information infrastructures in cyber space which is based on voluntary actions. In this context, there is not even a cyber security budget in Turkey.

3.4 Comparison of Approaches to Cybersecurity and Critical Infrastructure Protection in the Unites States, the European Union and Turkey

While the previous section examines how United States, European Union and Turkey comprehend the issues around the cybersecurity and critical infrastructure protection in detail, this sector will provide a discussion of the meaning and significance behind the commonalities and differences on these states and intergovernmental organization's perception and strategies.

Turkey as various other states and intergovernmental organizations has recognized the importance and danger of cyber threats very early. While the European Union started to be engaged with the issues around cybersecurity at the beginning of 2000s, Turkey, like the United States, has been in the field since 1990s. However, the development of cybersecurity understanding in Turkey came from a different background. Whereas the concept of cybersecurity in United States and European Union was evolved by first considering the protection of personal data protection, securing federal institutions and economic activities which became the basis of the development of critical infrastructure protection, Turkey started to handle the issue as anti-terror warfare for a long time under the Turkish Penal Code Law No. 3756 dated 1991.

However, over a time, Turkey’s cybersecurity perception has changed with the constantly changing dimensions of cyber space. In the post-2010 period, Turkey shares the same approaches about the cyber security with the United States and Europe. For instance, in 2016 Turkish Personal Data Protection Law was signed as an attempt to secure individual level protection in a cyber environment. However, importance of critical infrastructure protection has never been clearly understood by Turkey.

Critical infrastructure is the backbone of societies and is vital for a nation’s prosperity regarding national, global, and human security. When a nation adopts a certain sector as a part of its critical infrastructure, it gives priority which asserts how that sector is valuable and essentially need to be protected to ensure security. Meanwhile, when there are cyber disruptions to the services critical infrastructure provides, nations and international organizations start to address cyber threats in the realm of critical infrastructure protection.

However, states and intergovernmental organization may have different approaches about what needs to be protected from cyber threat. In this regard, United States started to engage with the critical infrastructure protection in 1998 by Presidential Directive 63 and Homeland Security Directive 7 followed in 2003. Currently, Presidential Directive 21, which was signed in 2013, declares 18 sectors as part of the American critical infrastructure.

With this high number of critical infrastructure classification, the United States has become a leading state in world. Therefore, by prioritizing an important number of sectors under critical infrastructure systems, the United States displays that a country has several developed and interconnected sectors and it has the capability and strength to ensure the security of the aforementioned critical infrastructure sectors.

Comparisons of states and international organizations' definition process of cyber security also clarifies whether they do or do not share a common understanding on the subject, which is an essential part of the critical infrastructure protection. In the United States, the definition of cybersecurity is mainly provided by the National Security Presidential Directive 54, Homeland Security Presidential Directive 23 and Cybersecurity and Infrastructure Security Agency. The American definition of cybersecurity admits the terms as a unity of practices that protects the country's digital systems, networks, programs, information, and interdependent infrastructure from any kind of cyber threat and availability, integrity, and confidentiality of such entities. In this regard, CISA's engagement of defining the term also points out that cybersecurity and critical infrastructure protection is interlinked with each other in the United States. In addition, CISA and GAO also define the possible cyber threats against the United States clearly.

Legal background of the critical infrastructures in United States dates back to 1990s, however, with the raise of cyber threats on such entities since the 2000s, critical infrastructure protection has begun to be considered a part of cybersecurity. In this regard, while the United States passed several different laws and regulations within the scope of ensuring cybersecurity concerning the different sectors such as healthcare, insurance, banking and finance or security of federal institutions, the state also signed legislations to create common rules and regulations for cybersecurity. In this context, the United States also provided specific legislations and plans for national critical infrastructure protection such as National Infrastructure Protection Plan, Cybersecurity and Infrastructure Security Agency Act of 2018 and NIST Framework.

In addition, as the United States has several specific federal organizations to tackle with the cybersecurity issue, the state also has separate organizations to deal with critical infrastructure protection such as CISA, the National Infrastructure Coordination Center and the Homeland Security Information Network-Critical Infrastructure. Possessing these umbrella organizations is critical because they are only responsible for the regulations, strategies, changes, functions and sanctions on American critical infrastructure protection.

Even though the United States has a large number of specific institutions regarding cybersecurity and critical infrastructure protection, all these institutions possess their own cybersecurity budget which creates the United States overall cybersecurity budget. The United States openly shows each federal organizations' cyber security budget. While the American organization allocated 14,978 billion dollars in 2018 and 16,645 billion dollars in 2019. The country's 2020 cyber security budget raised to 17,435 billion dollars for 2020. When looked at Table 1 and Table 4, it is seen that the United States' all federal institutions have their own cyber security budget and this the United States allocated important amount of budget and country is also very planned to protect its infrastructure against cyber threats.

Table 4: Summary of the Unites States' Policies on Critical Infrastructure Security and Cyber Security

		United States
Definitions	**Critical Infrastructure**	Comprehensive Definition PPD-21, 2003, 18 national critical infrastructures: chemical sectors, commercial facilities sector, communications sectors, critical manufacturing sector, dam sector, defense industrial base sector, emergency services sector, energy sector, financial services sector, food and agriculture sector, government facilities sector, healthcare and public sector, information technology sector, nuclear sector, transportation systems sector and water systems sectors
	Cyber Security	Comprehensive Definition NSPD-54 /HSPD-23 & CISA
	Cyber Threat	Comprehensive Definition GAO, 2005: bot-network operators, criminal groups, foreign intelligence services, hackers, insiders, phishers, spammers, spyware/malware authors, terrorists CISA, 2020 adds: natural disasters, environmental, mechanical failure
Legal Background and Operations	**Legislations**	Specific Legislations PPD-63, HSPD-7, Critical Infrastructure Act of 2001, PPD-21, HIPAA 1996, GLBA 1999, FISMA 2002-2014, Cybersecurity Enhancement Act of 2014, National Cybersecurity Protection Advancement Act 2015, Cybersecurity Information Sharing Act 2015, Cybersecurity Legislation, 2015-2019, Cybersecurity and Infrastructure Security Agency Act of 2018, NIIP 2016-2018, EO 13636, NIST Framework
	Institutions	High Number of Specific Institutions Specific: Cyber Command, The National Cyber Security Division, Comprehensive National Cybersecurity Initiative, The National Cybersecurity and Communications Integration Center, US – EU Working Group on Cybersecurity and Cybercrime, CERT_US, Other: DHS, FBI, DoD, The National Security Agency
	Critical Infrastructure Protection	Having a Specific CIP Institutions CISA, The National Infrastructure Coordinating Center, HSIN-CI
Budget		All agencies total in billion $ 2018: 14,978 2019: 16,645 2020: 17,435

As the United States, the European Union has also prioritized specific sectors as European critical infrastructure. However, the European Union declares only 11 critical infrastructure sectors. Even though the European Union does not prioritize critical infrastructures as much as the United States, it still works effectively because each of the member states also have their own critical infrastructure. For instance, Germany divides national critical infrastructures into two categories called technical basic infrastructure and socio-economic services infrastructure and under them prioritizes 14 critical infrastructures (Federal Ministry of the Interior, Building and Community, 2009). Despite that, the European Union's understanding of what is critical differs from the United States. While the United States classifies specific sectors such as the dam sector or commercial facilities, the European Union has even more specific classifications on what sectors make up critical infrastructure such as space sector.

In terms of cybersecurity, the European Union defines the term almost the same way with the United States. While the European Committee's report called JOIN/2013 and ENISA see cybersecurity as a protection of interdependent networks and information infrastructure against cyber risks, they do not mention healing and improving these systems. However, as seen in the United States, the European Union's specific organization ENISA which is working on both the subjects of cybersecurity and critical infrastructure protection and providing a legal cybersecurity description. Moreover, Europol and the European Court of Justice also targets and defines the cyber threats clearly to fight against them.

Legal background of the critical infrastructures in European Union dates back to beginning of the 2000s. The legal attempts in the European Union emerged in the communication and information security areas. In this regard, the European Union even has binding regulations and institutions which can regulate the sanctions to member states, such as General Data Protection Regulation. In 2016, the first important framework regarding the critical infrastructure protection called NIS Directive was signed.

Currently, while the European Union has cybersecurity and critical infrastructure protection legislations as much as the United States, the Union has more specific and divided institutions such as the European Programme for Critical Infrastructure Protection, Critical Information Infrastructure Protection, the European Reference Network for Critical Infrastructure Protection, the European Union Agency for Network and Information Security.

Table 5: Summary of the European Union's Policies on Critical Infrastructure Security and Cyber Security

		European Union
Definitions	**Critical Infrastructure**	Moderate Definition European Commission, 2005 11 national critical infrastructures: energy, information and communication technologies, water systems, food supply, healthcare, financial systems, public order and security, civil administration, transportation and communication, chemical and nuclear industries, and space research
	Cyber Security	Comprehensive Definition JOIN 2013 & ENISA 2015
	Cyber Threat	Comprehensive Definition Europol & European Court of Auditors: viruses, trojans, ransomware, worms, adware and spyware, DDoS attacks, cyberespionage, and attacks on critical infrastructure
Legal Background and Operations	**Legislations**	Specific and Strong Legislations Cybersecurity Act of 2019, European Digital Agenda, GDPR, NIS, COM and JOIN Directives, CSDP, European Union Directive No. 114, Regulation (EU) 2018/1725, COM/2001/0298, Directive on European Critical Infrastructures
	Institutions	Moderate Number of Specific Institutions European Union Agency for Network and Information Security, European Cybersecurity Industrial, Technology and Research Competence Centre, CERT-EU, Europol, Eurojust, US – EU Working Group on Cybersecurity and Cybercrime
	Critical Infrastructure Protection	Having a Specific CIP Institutions ENISA, EPCIP, ERNCIP, JRC, CIIP, CIWIN
Budget		ENISA total in million € 2018: 11,449 2019: 16,932 2020: 21,785

Among these, ENISA is the precedes the Union organization to ensure the robustness of the critical infrastructure against cyber threats which hazardously effect national and pan-European level prosperity. Moreover, the European Union's cyber security budget is under control of the ENISA. While ENISA allocated 11,449 million euros in 2018 and 16,932 million euros in 2019, the number doubled as 21,785 million euros for 2020. It should be noted that while the cyber security budgets of 25 different federal institutions of the United States are examined, in order to consider the European Union's budget in this regard, only the budget of ENISA is shown. Also, even though this analysis does not embrace the European Union's member states separately, it should be not forgotten that European countries have their own cyber security budget.

In terms of Turkey, designation of critical infrastructures is more problematic. While the United States declares 18 sectors as part of the critical infrastructure and the European Union declares 11, Turkey only declares 6 sectors. The reason for this difference in Turkey can be explained using two reasons. First, the sectors, which are seen as a part of their critical infrastructure protection system in the United States and the European Union, are not very developed or not connected to cyber space in Turkey. For instance, whereas United States and European Union classify nuclear industrial sector under their critical infrastructure, Turkey does not because the sector is still developing and is expected to be completed in 2023.

In the same way, while the European Union gives importance to the space sector, Turkey does not even have initiative in this type of sector. Second, Turkey does not have the strong background to specify the sector as critical infrastructure as a result of economic problems, lack of resources or focusing on other priorities. Even though the United States prioritizes several sectors such as food and agriculture, the defense industry, manufacturing or healthcare, Turkey does not mention these sectors as a part of its critical infrastructure even though these are also essential parts of country.

However, Turkey defines the concept of cybersecurity in a same way the United States and the European Union does; cybersecurity is the unity of practices that protect countries' digital systems, networks, programs, information and interdependent infrastructure from any kind of cyber threat and ensure availability, integrity and confidentiality of such entities. Even though each state may focus on different domains of cybersecurity, they meet at the same point by giving importance to the physical and virtual entities and interconnecting infrastructures of the cyber world.

Moreover, they also target the same harmful activities as a cyber threat or attack. Therefore, the United States, the European Union and Turkey reflect the same comprehensive answers to questions of what cybersecurity is and what cyber threat is. Looking at the issue in this context, it can be argued that they share common threat perception and priorities in the cyber environment.

In Turkey, there is also no official published law or legislation about the critical infrastructures and their protection. Only a few documents and strategy plans talk about what critical infrastructures are, their importance and possible security practices without going into detail, mentioning its relation to cyber security and it does not give information about how to proceed legally in this subject. Basically, the problem is providing some statements in specific documents about critical infrastructures artificially without drawing any legal framework or sanctions.

Enacting a law or legislation on this issue needs to go through the process of policy formation which proves that before the law came out, debates are held, options are explored and interests consulted, and only then a decision is made. Therefore, the absence of any legal document on critical infrastructure in Turkey indicates the deficiency and also ignorance about the subject. Whereas the United States and the European Union have declared specific legislations about the protection of critical infrastructure, Turkey gives minor importance to this issue under the document called 2016-2019 National Cyber Security Strategy of Turkey.

Besides this, even the United States and the European Union have several different organizations which are specifically established to regulate critical infrastructure coordination, protection and cyber resilience. Turkey does not have any specific organization whose entire focus is on critical infrastructures. Instead of established specific federal institutions, the Ministry of Transport, Maritime Affairs and Communications have to deal with the critical infrastructure protection especially against cyber threats.

Even though Turkey does not have any legislation and institution regarding the critical infrastructure protection, the country tries to develop its cyber security through declaring new strategies. For a long time, the United States and the European Union made legislations and established specific federal organizations to promote and ensure their own cyber security. In this sense, while Turkey does not have any specific law or organization in terms of cyber security, it published several national cyber security strategies. For instance, BTK and TUBITAK were the two leading organizations which made several R&D and published cyber security reports.

However, since 2012, all authorities regarding the cyber security were collected under the Ministry of Transport, Maritime Affairs and Communications which publish national security strategies and action plans.

However, even these are problematic because the aforementioned mentioned strategies like the 2016-2019 National Cyber Security Strategy of Turkey do not provide separate strategies for different sectors and institutions. In addition, cyber security strategies and action plans always provide optional strategies like recommendations, whereas institutions of the European Union contain binding strategies for each of the member states.

Meanwhile, Turkey failed to create a specific and strong institutionalization process on cyber security issues. There are only a few organizations without an effective umbrella mechanism and coordination efforts to try to deal with the cyber environment. While the United States and the European Union have created a partnership, Turkey does not have any state partner or organization other than NATO.

In addition, the United States and the European Union have allocated a huge budget for cyber security. The United States openly shows all federal organizations' cyber security budget and European Union shares the ENISA's information. Unfortunately, neither the Turkish government nor the institutions responsible provide any official documents to inform the public on country's cyber security budget to protect the nation against cyber threats.

Table 6: Summary of the Turkey's Policies on Critical Infrastructure Security and Cyber Security

		Turkey
Definitions	**Critical Infrastructure**	Limited Definition 2016-2019 National Cyber Security Strategy 6 national critical infrastructures: electronic communication, energy, water management, critical public services, transportation and banking and finance
	Cyber Security	Comprehensive Definition National Cyber Security Strategy and 2013-2014 Action Plan & 2016-2019 National Cyber Security Strategy include the elements of psychical and virtual cyber entities, interconnection of the entities, protection, sustainability
	Cyber Threat	Moderate Definition BTK: blocking services and DoS or DDoS attacks, malicious software, monitoring the information systems
Legal Background and Operations	**Legislations**	Moderate Legislations The Turkish Penal Code Law No. 3756 1991, The Turkish Penal Code Law No. 5237 2001, The Anti-Terror Law No. 3731 2006, The Draft Law on National Information Security Organization and Its Tasks (not passed), Personal Data Protection Law No. 6698, National Defense Policy 2009, National Cyber Security Strategy and 2013-2014 Action Plan, 2016-2019 National Cyber Security Strategy
	Institutions	Moderate Number of Specific Institutions Specific: Ministry of Transport, Maritime Affairs and Communications (main), Sectoral CIRTs and Corporate CIRTs, BTK, Common Criteria Test Center and Cyber Space Defense Centre under TUBITAK, CERT-TR (USOM), The Cyber Security Council (closed), KVKK Other: Turkish Armed Forces, Turkish National Police, National Intelligence Service
	Critical Infrastructure Protection	Does not have any CIP institution
Budget		

After summarizing the condition of Turkey in terms of the issues around cyber security and critical infrastructure protection by comparing it with the United States and the European Union, whether the Turkey's policy is successful or not should also be discussed. Obviously, whereas different countries and organizations share common understanding about the cyber security and critical infrastructure protection, they obtain different policies and implementation that may give rise to variations in their goals and priorities. Therefore, comparing Turkey with others is not enough to draw a conclusion. For this reason, the following section will analyze the policy success of Turkey’s cyber security and critical infrastructure protection through adopting specific policy success framework.

CHAPTER IV

POLICY ANALYSIS ON TURKEY'S CRITICAL INFRASTRUCTURE POLICIES

4.1 Implementation of the Policy Analysis Method

Policy analysis, as a systemic and empirical study, refers to a technique that is used to examine the formulation, adoption and implementation of certain public policies with an intention to determine the relation between policies and their goals, and also formulate various different economic, social and public alternatives (Geva-Mary & Pal, 1999; Simon, 2016). In general, public policy analysis reflects a desire to understand, interpret or even explain how certain politics work. It also has ambition to formulate proposals and provide recommendations in order to form more effective and qualified policies.

With this in mind, two types of policy analysis direction are considered, and these are: "analysis of an existing policy" and "analysis for a new policy". While analysis of an existing policy, as an analytical and descriptive method, attempts to examine policies and their development, analysis for a new policy, as a prescriptive method, focuses on formulation of new policies and proposals (Bührs & Barlett, 1993). In the literature, there are various examples display that these two analysis types can both be complementary to each other and also can be applied together. At this point, the main interest and purposes of the present analysis is to help determine which type of analysis direction is conducted.

After determining the public policy to investigate, the empirical methods of analysis, which form another basis of the analysis, are divided into two: qualitative and quantitative analysis. Qualitative analysis in public policy studies involves the archival analysis, study of policy evaluation and history and examination of how certain problems are perceived and solved. Quantitative analysis involves cost-benefit analysis through focusing more on statistical analysis among the variety of issues surrounding the policy process (Simon, 2016). Nevertheless, the distinction between these empirical methods can also be blurred during the research. Whatever the type of empirical analysis method, it is important to keep track of evidence that cannot talk per se.

In relation this research's main goal, to investigate whether Turkey's critical infrastructure policies, which is in relation to cybersecurity policies, are consistent and successful or not, policy analysis methods will be applied in this section.

In this respect, the policy to be examined has been determined as an existing Turkish policy named 2016-2019 National Cyber Security Strategy. While as mentioned, Turkey does not have any specific law or legislation on critical infrastructure protection, this document is seen as the most up-to-date strategy explanation which also mentions the pursued policies and concerns about the nation's critical infrastructure. Also, this existing strategy, received from the Ministry of Transportation, Maritime and Communication's archive, will be analyzed by qualitative considerations regarding the specific policy success indicators. Indicators used to analyze Turkey's success on critical infrastructure protection adapted from Marsh and McConnell's (2010) policy success framework which classify the indicators of success under three categories; “process success”, “programmatic success” and “political success”.

4.2. Policy Success Analysis of the 2016-2019 National Cyber Security Strategy

The political and academic discourse on policy success analysis has not been formed a comprehensive method to examine the nature of success in this regard. Nevertheless, the efforts of several academics and collaborators improve the subject of the study the public policy success by creating a model that distinguishing the analysis of programmatic and political success (see Bovens et al., 2001). Even though this model gained popularity in literature, the debates around developing different dimensions are still continuing. Given that, Marsh and McConnell (2010) offer a more detailed framework to discuss and assess policy success by adding process success as a dimension into the analysis. In their work, the authors outline the three dimensions of policy success as process, programmatic and political through identifying the indicators, which is used to measure the political success’s relation to each different dimension, and the evidence, which have appropriate conditions in relation to each indicator.

The heuristic policy success framework, which has a three dimension, fits to study existing public policies and quantitative evidences to explore the success of certain policies. For this reason, the policy success of the 2016-2019 National Cyber Security Strategy in terms of critical infrastructure protection is investigated by a method adapted from Marsh and McConnell (2010).

Table 7: Policy Success Dimensions and Turkey's Success (Adapted from Marsh and McConnell (2010: 571))

Dimensions	**Indicators**	**Evidence**	**Turkey 2016-2019 National Cyber Security Strategy**
Process Success	1. Legitimacy in the formation of choice 2. Passage of legislation 3. Political sustainability 4. Innovation and influence	1. Absence of legal/procedural challenges and criticism 2. Analysis of amendments and voting patterns 3. Analysis of support from the different groups (e.g. ministers, stakeholders, interest groups etc.) 4. Analysis of statements, reports and comments about the policy	Moderate Success
Programmatic Success	1.Operational implementation 2. Outcome achievement 3. Use of resources 4. Policy serving a certain group	1. Analysis of internal program, policy evaluation and external evaluation documents 2. Analysis of internal program, policy evaluation and external evaluation documents 3. Analysis of internal efficiency evaluation and external audit reports 4. Analysis of different type of documents (e.g. party-political speeches, government reports and briefings, stakeholder repots, other commentaries etc.)	Low Success
Political Success	1. Government popularity	1. Analysis of opinion polls in relation to particular policy and government popularity, election results, media coverage	Low Success

The first dimension of Marsh and McConnell's (2010) public policy success framework is the success of policy formation process that refers to the stage of policymaking in which the policy options and interests are analyzed and discussed, which leads to decision making. Whereas policymaking sometimes does not follow linear process evaluation, this stage is important to strengthen and preserve the legality, acceptability and reconciliation of that policy. As it is shown in Table 7, the policy formation process is divided into four indicators which are legitimacy in the formation of choice, passage of legislation, political sustainability, and innovation and influence. Therefore, while the first two indicators regarding the approvability of the policy by large groups, others in turn concern themselves with the sustainability and impact of the policy.

The first indicator of policy formation process is legitimacy in the formation of choices that is about the legality of the policy through constitutional and quasi-constitutional procedures and accountability of the policy. Even though this 2016-2019 National Cyber Security Strategy is not discussed and comes as a force of legislation or laws with the force of a coalition, the strategy has a mentioned legal background. Given that, as it is explained in the strategy, the document was prepared and proposed by the Ministry of Transportation, Maritime and Communication which has been tasked with the duty of preparing policies and strategies on cyber security and related issues pursuant to "The Council of Ministers' Decision on the Execution, Management and Coordination of National Cyber Security Activities which was published in the Official Gazette Number 28447 and the Electronic Communication Law Number 5809" (2016-2019 National Cyber Security Strategy, 2016: 5) . Therefore, it can be said that the formation of the strategy does not face any legal or procedural challenges.

The second indicator of policy formation process is named as the passage of legislation is concerned with the policy being passed with no or few amendments. In this regard, since this strategy is not law or legislation, the amendment process of law making could not be applied in this strategy. As a result, this strategy is formed by the Ministry of Transportation, Maritime and Communication to specify the ministry's four-year goals on cybersecurity, the problem of amendments or voting required for its acceptance is even not an issue. Although there is no amendment or drafted document formed before the publishing of such strategy, seven evaluation meetings held by the institutions, which were responsible and associated with the previous strategy named the National Cyber Security Strategy and the 2013-2014

Action Plan, to discuss the achievements of the previous plans and create more innovative policy.

The political sustainability as a third indicator of the processes success focuses on whether the policy is supported by sufficient and diverse groups or not. During the preparation process of 2016-2019 National Cyber Security Strategy, "a meeting named Common Mind Platform was held with the participation of 126 experts from 73 different institutions such as public organizations, critical infrastructure operators, information technology sectors universities and non-governmental organizations to discuss and determine the strategic goals and actions that should be in the strategy. The strategy also points out that 11 Cyber Security Board member institutions, 15 regulatory and supervisory institutions and 16 sectoral CIRTs are in coordination with the Ministry of Transportation, Maritime and Communication depending on the 2016-2019 strategy" (2016-2019 National Cyber Security Strategy, 2016: 6). Even though these numbers can be interpreted as there a lot of groups that support this strategy, 16 sectoral CIRTs are all the federal representatives of the 6 critical infrastructure sectors in Turkey, this is not a sufficient number because Turkey at the beginning, could not determine the sufficient number of critical infrastructure sectors like the United States or European Union. Another problem is that while support of federal and public institutions is mentioned in the strategy, the attitude of private sector and corporate CIRTs towards the strategy are not mentioned. Therefore, it is not exactly said that the strategy relies on sufficient and diverse support.

Among the process success indicators, the last one is concerning the policy's innovative feature which is the most problematic one for the application of Turkey's

2016-2019 strategy on cybersecurity and critical infrastructure protection because unfortunately 2016-2019 strategy is less innovative and influential than the previous strategy. Turkey’s National Cyber Security Strategy and 2013-2014 Action Plan (2013: 10) tried to create a strong cyber infrastructure by fulfilling the three objectives; “ensuring cybersecurity of all services, processes, information and data, which are provided by public institutions, through using information technologies, ensuring the cybersecurity of critical infrastructure systems, which are operated by the public and private sectors, minimizing the negative impact of cybersecurity incidents and strengthening processes of investigation and prosecution of cyber incidents through law enforcement and judicial authorities”. In this regard, the 2013-2014 strategy also grouped the strategic action plans under the certain categories; improvement of regulatory measures, strengthen the judicial processes, establishing the national cyber indecent response organization, straightening the national cybersecurity infrastructure, raising awareness and training activities, developing national technologies and extending the scope of national cybersecurity mechanisms.

Even though 2013-2014 strategy seems like it mostly focuses on general requirements of cybersecurity, the strategy is also providing one of the most detailed action plans about the critical infrastructure plan under the section of strengthening the national cybersecurity infrastructure in Turkey after defining the critical infrastructure sectors in the country. In this regard, the action plan was prepared to improve the information security management program in critical infrastructures. The plan had aimed to determine the critical infrastructure which would become the direct target of cyber-attacks and that would be disturbed the public prosperity if damaged and conducting the sectoral risk analysis mechanism for critical infrastructures by mid-2013 with the works of responsible organization TUBITAK and other relative organizations which are responsible for the regulation of the critical infrastructure sectors. The 2013-2014 strategy had certain objectives for critical infrastructure security. According to action plan of the strategy, while CERT-TR and TUBITAK were responsible to determine the critical infrastructures that could be the target of cyber threats and conducting sectoral risk analysis, relevant public organizations were responsible to regulating and auditing the critical sectors.

Moreover, to achieve the objectives , it also set a goal to determine the requirements of sectoral emergency actions, completing the first yearly risk analysis reporting activities, determining and implementing the needs of sectoral business continuity plans in terms of its protection and continuously determining and implementing the sectoral security precautions again by related organizations, such as CERT-TR and TUBITAK and other responsible organizations which are responsible for regulating the sectors. Even though the 2013-2014 strategy was prepared in detail and explained every dimension of innovative action plan, Turkey did not achieve these desired goals especially those which concern critical infrastructure protection.

In the 2016-2019 National Cyber Security Strategy and Action Plan, which share the same objectives with the previous policy, it is stated that the cyber security strategies of other states are examined, and targets are added to the agenda in these strategy documents such as internet addiction, cyber espionage, cyber security expert training, and elimination of coordination weaknesses among cyber security institutions. Apart from these, the correct approach should be developed in Turkey's cybersecurity and cyber ecosystem condition and is stated as the integration of national security.

However, in terms of the critical infrastructure protection, the 2016-2019 strategy does not provide any innovate idea or clear action plan. Policy only states that one of the actions would create a national critical infrastructure inventory, meeting the security needs of critical infrastructure sectors and supervision of infrastructure by the relevant regulatory boards, which are the repetition of old policies, without providing any direction or answering how. In this regard, as Darıcılı (2019) asserts that the 2016-2019 National Cyber Security Strategy has been prepared with simpler and general expressions compared to the previous strategic policy. Therefore, it can be said that, even the 2016-2019 strategy was not innovative, it even took the critical infrastructure protection's importance backwards a few steps.

Programmatic success as a second direction in policy success analysis mainly focuses on evidence-based policy making through examining the implementation process of the policy. In this direction, the first indicator is the operational success of policy that is about whether or not the policy is implemented according to determined and approved strategies. Among the other indicators in programmatic success, the operational implementation is generally much more complex because of the increase in multilevel governance system in a world that requires tight bonds with different bodies and agencies, which are different from the institutions, in order to implement a policy (Exworthy & Powell 2004). In this regard, before examining the operational success of the 2016-2019 National Cyber Security Strategy and Action Plans, objectives of the strategy that is shown in Table 8 should be understood.

Table 8: 2016-2019 National Cyber Security Strategy's Objectives (2016-2019 National Cyber Security Strategy, 2016: 13-14)

1. Creating a national critical infrastructure inventory, ensuring the security needs of critical infrastructures, and creating checking mechanism of the critical infrastructure sectors by the relevant regularity board	10. In order to improve the efficiency of corporate and sectoral CIRTs, providing legislative support, making financial arrangements, meeting the need for qualified personnel, providing information technology infrastructure and developing information sharing within the scope of organizing national cyber incidents responses
2. Creating a legislation to conform the international standards including cybersecurity auditing standards	11. Establishing a strong central public authority to ensure the coordination in the field of cybersecurity
3. Developing the regulatory and supervisory awareness and sectoral competencies of regulating institutions, ministries in the frame of cybersecurity	12. Creating a national cybersecurity eco-system through the participation and coordination of public institutions, private sectors, non-governmental institutions, supervisory institutions, universities, software companies and all other stakeholders
4. Planning to protect information technology systems of institutions not only from attacks, but also protect from human error and disasters	13. Disseminating the best examples within the national cybersecurity eco-system providing consultancy services, sharing of weaknesses, threats, and useful applications
5. Enabling that each institution reaches a level of operating its own information security management process	14. To prevent the exploitation of weaknesses in domestic or foreign hardware product used in critical points of information systems, making vulnerability analysis and certification works
6. Raising awareness of corporate executives on cybersecurity	15. Creating a secure software development and supply management culture
7. Training qualitied personal in the field of cybersecurity, and encouraging personal, researchers and students to want to specialize in this field	16. To reduce the foreign dependency in cybersecurity, give importance to R&D activities and development of domestic products
8. Creating cybersecurity awareness in every segment of a society and in addition to works of educational institutions, enforcing written and visual media works on awareness	17. Improving national proactive cyber-defense capability to eliminate threats
9. In order to employ experts in the field of cybersecurity in public institutions providing legislative support, and improving personnel rights of the employee	18. To eliminate the anonymity, which is the biggest advantage of threats actions in cyber space, dissemination efficient log management and Internet Protocols Version 6 (IPv6) technologies

The 2016-2019 National Cyber Security Strategy does not specifically give a place to the objectives on critical infrastructure. Even if mentioned objectives are implemented successfully, of course, the nation's critical infrastructure sectors would be benefited. However, even though the previous 2013-2014 strategy provided a detailed action plan which includes specific objectives for the protection of critical infrastructure and plans for how to achieve those goals, the 2016-2019 strategy does not possess any detailed action or implementation strategy of those objectives. For instance, while the first objective indicates the importance of creating a national critical infrastructure inventory, ensuring the security needs of critical infrastructure systems and creating a checking mechanism, the strategy does not mention the implementations such as by whom, how and according to which criteria will be implemented and audited. This problem is also seen in other objectives. There is no objective implementation mentioned in the strategy such as which institutions will be responsible, how the budget will be set, or how long until the goals should be achieved. Therefore, it can be said that this strategy only displays the goals that should be achieved to ensure the nation's cybersecurity without offering any real strategy to achieve them or implementation strategies.

Moreover, another indicator named the outcome achievement is about whether the determined objectives are fulfilled and intended outcomes are achieved. In this regard, to examine the 2016-2019 strategy and action plan's success, the Ministry of Transportation, Maritime and Communication's four years administrative activity reports should be analyzed. First of all, the 2016 Administrative Activity Report includes the cybersecurity related implementations in the report and indicates that until the end of 2016, while 2 sectoral CIRTs and 180 corporate CIRTs were established, but no cybersecurity exercise, which are useful trainings and simulations to prepare and test institutions and sectors to respond to a specific set of circumstances in cyber space, were performed. Therefore, it is clear that, in the 2016, 2016-2019's strategy's objectives have not been achieved and no significant steps were taken to achieve this purpose.

The 2017 Administrative Activity Report asserts that there are various different sectoral CIRTs within the critical infrastructure sectors were continued to be established within the Banking Regulation Supervision Agency (BDDK) and Capital Markets Board in Turkey (SPK) in the financial sector, Information and Communication Technologies Authority (BTK) in the electronic communication sector, Energy Market Regulatory Authority (EPDK) in energy sector, General Directorate of Civil Aviation, General Directorate of Railway Regulation in transportation sector, Ministry of Health, Ministry of Justice, Ministry of Interior and Ministry of Environment and Urbanization in public services sector. In this regard, the number of established corporate and sectoral CIRTs has reached 812 as of December 2017. In addition, as it is mentioned in the report, to achieve the objectives of the 2016-2019 strategy, the 2017 National Exercise was conducted, awareness trainings were provided for senior managers in the sector, public spots were provided to raise awareness, draft document of Cyber Security Terms Dictionary was created and R&Ds for the establishment of a Training Simulator are continuing. These implementations did not cover a large part of the 2016-2019's strategy's objectives and by looking at the years after 2017, it can be said that these implementations were not enough even though 2017 was the year that demonstrates more effort than 2016 and 2018.

The 2018 Administrative Activity Report only provides information about the implementations regarding the cyber security and critical infrastructure protections and that the number of corporate and sectoral CIRTs had reached to 1090 as the end of 2018. Also, the last report, called the 2019 Administrative Activity Report, indicates that as of the end of 2019, the number of corporate and sectoral CIRTs reached 1283. In addition, the 2019 International Cyber Shield Exercise was held on December with the cooperation of the Ministry of Transportation, Maritime and Communication and Blekinge Institute of Technology (BTH) and also with the contributions of Cyber Security Alliance for Mutual Progress (CAMP) with participation of the International Telecommunications Union (ITU). Moreover, in 2019, the efforts were underway to prepare the new National Cyber Security Strategy and Action plan, which is planned to cover 2020-2023. However, the 2019 Administrative Activity Report also indicates some vulnerabilities in terms of the sector that the Public Integrated Data Center finds the completion rate as low as %53 whereas the number of funded sectoral and corporate CIRTs are way too high.

In the direction of programmatic success, use of resources is the second indicator to analyze policy success. In this regard, efficiency of the strategy to implement objectives of the 2016-2019 strategy is not known because while the strategy itself does not mention any resource or budget to achieve the mentioned goals in the action plan sections, the four activity reports also do not provide any information about the budget allocated to the fulfillment of Turkey’s cybersecurity and critical infrastructure security. One of the reasons for this problem is a lack of central authority to engage the resources to fight cyber threat and secure critical infrastructures because the Ministry of Transportation, Maritime and Communication has several different duties and considerations to fulfill rather than only focusing on cyber security and critical infrastructure protection.

The last indicator under the dimension of programmatic success, is focusing on whether the policy serves the interests of specific groups. Given that, policy can be successful if it benefits a particular actor, target groups or interest. In this regard, the 2016-2019 National Cyber Security Strategy mainly regulates the cyber needs of 11 Cyber Security Board member institutions, 15 regulatory and supervisory institutions and 16 sectoral CIRTs which are coordinating with the Ministry of Transportation, Maritime and Communication.

Lastly, political success is the final dimension of policy success analysis. In this dimension, a policy can be successful if it assists the government popularity through electoral success, reputation, or governance sympathy. In this regard, unfortunately the government does not use this type of national strategy to increase its government or electoral popularity. Looking at the news after the announcement of the strategy, it can be seen that to some degree strategy was stated as a path for technological developments in cyber environments, but the part of critical infrastructure protection is not mentioned or seen as an important action by the government.

4.3. Interpreting the Policy Success Analysis of the 2016-2019 National Cyber Security Strategy

Before proceeding to the interpretation of the analysis, two significant points should be emphasized. First, policy analysis of frameworks sometimes may not comply with certain policies because different policies have different natures such as regarding differences in the legal background, formation process or implementation procedures. In this regard, as stated in this section, Marsh and McConnell’s (2010) framework on policy success analysis is a heuristic approach, which only tries to broaden the options for evaluating public policies, not a model or theory. Second, as mentioned before, Turkey does not have any specific laws or legislations on critical infrastructure protection. For this reason, the 2016-2019 National Cyber Security Strategy, which mentions the importance of securing critical infrastructure systems and gives weight to the cybersecurity that is a key element in the protection of critical infrastructures, has been analyzed as a policy in this regard. Nevertheless, when Marsh and McConnell's (2010) heuristic framework for policy success analysis is applied to evaluate Turkey's 2016-2019 National Cyber Security Strategy, the outcome is unfortunately not very promising.

With regard to process success, which is the first dimension, Turkey's 2016-2019 strategy has seen moderate success. This process success has four decisive indicators; legitimacy in the formation of choice, passage of legislation, political sustainability, and innovation and influence. At this point, the first two dimensions are mainly about having a legal background and accountability. In this regard, the 2016-2019 National Cyber Security Strategy's gets its legal background through the Ministry of Transportation, Maritime and Communication which has a duty to publish such strategies with attained right from the Council of Ministers' Decision. In addition, the strategy is also accountable. Even though passage of legislation as an indicator points out the amendment process as a source of accountability, in terms of the 2016-2019 strategy which has a different nature than classic law and legislation, the amendment process can be replaced with the formation process of the strategy that different sectors participate in through the several meetings.

Although there is no problem in legitimacy and accountability of the strategy, the reason this dimension has moderate success is because there is little success in political sustainability and innovation. First, the political sustainability of the strategy is doubtful because even though various experts, different institutions and CIRTs participated in the formation of 2016-2019 National Cyber Security Strategy, the strategy only focuses on the policies regarding 6 critical infrastructure sectors and ignores other infrastructure providers and leads to sustainability in this respect. In addition, the strategy also ignores the reality of private sector and corporate CIRTs on the field through not embracing them. Besides this, compared to the strategies of previous years, it has been criticized to be less detailed, unplanned, and unsuccessful. Moreover, this strategy not only does not bring anything new but also has been criticized as being vaguer and lesser in scope in relation to previous strategies like the 2013-2014 one. This is why, it also fails the innovation part. Therefore, this policy stays at moderate in process success.

As for the programmatic success, the strategy does not contain a proper operational implementation which is one of the reasons the 2016-2019 strategy has low success in this dimension. First and most importantly, the strategy does not contain a proper operational implementation. There is no mention of how, by whom, when, and using which resources these 18 objectives will be achieved. Instead the objectives are only given like a recommendation. This makes objectives very difficult to achieve within 2019. Nevertheless, even though there are 17 objectives about the subject of cybersecurity, only one objective talks about critical infrastructures but this also superficially mentions the importance of the subject without setting a significant goal to achieve. However, when looking at the Administrative Activity Report that came out between 2016 and 2019 to analyze the outcome achievement, it can be seen that the objectives making practice exercise, raising awareness, providing training, increasing both of the sectoral and corporate CIRTs, making R&D for creating training simulator and cybersecurity dictionary and making cooperation with foreign institutions are achieved. Unfortunately, it also reveals that there is still no unity among the public agencies by declaring that Public Integrated Data Center completion rate too low despite the increased number of sectoral and corporate CIRTs even though the meaning of increase in those CIRTs and the function of these CIRTs is not even explained. Apart from that, looking at the overall objectives, it is hard to understand how the achievement of 4 or 5 objectives out of 18 in 4 years can be counted as a success. What about more important issues mentioned in the 2016-2019 objective such as raising employment rate, reducing foreign dependency and improving national proactive cyber defense capacity, developing regulatory and supervisory services and most importantly creating legislation. Besides this, the reports reveal that between 2016 and 2019, nothing has been done about the protection of critical infrastructures. Even if all mentioned objectives regarding cyber security were achieved, it would have been indirectly become the reason of protected in critical infrastructures. On top of these, the reports only give superficial details on everything.

As for the resource allocation as an indicator of programmatic success, the Administrative Activity Reports do not show any resource allocation to the cyber security nor critical infrastructures fields. The report shows resource allocation to the other fields and how they are used, but it is just both the cyber security and critical infrastructure areas that are missing here. Actually, this is a result of missing a central authority. The one success in this programmatic success area would be the strengthening of all public and private institutions’ cyber security infrastructure.

However, the lack of sanction power here is still a matter of debate. Therefore, it can be said that the strategy's programmatic success is also low.

Finally, for the political success, there is no document nor indicator that shows that this strategy has been used as a political tool. It cannot be expected to be a political success without there being a successful dimension of process success and programmatic success. While many other countries use the subjects of cybersecurity and critical infrastructure protection as a policy tool, Turkey does not. In this regard, it is clear that while Turkey has not successfully achieved any subjects regarding the cyber security and critical infrastructure protection, why they used as a policy tool now.

Overall, briefly it can be said that by comparing Turkey's situation regarding the issues surrounding cybersecurity and critical infrastructure security with the United States and European Union and analyzing the2016-2019 National Cyber Security Strategy's policy success, the same problem is revealed and this is the lack of sufficient definitional, legal, institutional and economic practices to embrace the issues surrounding cybersecurity and critical infrastructure security in Turkey. Specifically, the problems are revealing because there are not enough defined critical infrastructure sectors, an absence of authority and legislation and a complete lack of a complete rule on institutions, which are named as CIRTs to deal with the issue and absence of an allocated budget on critical infrastructure protection. Despite the problems in critical infrastructure security, and although there are certain purposes in ensuring cyber security, looking at the result, it seems that there are the same problems, as well. Also, at the center of this problem is ignorance. Throughout analyzing the policy success of the 2016-2019 strategy, the conclusion it is reached that Turkey does not give name to its problems and for this reason, the problem whose existence is not accepted is not tried to be solved. As a result of this ignorant and problematic loop in Turkey, cyber security and security of critical infrastructures cannot become a policy tool.

CHAPTER V

CONCLUSION AND RECOMMENDATIONS

Each international relations theory takes place in discussing the general lines of the concept of security, and throughout their additives, the approaches toward the concept can be divided into three categories: “national security”, “international security”, and “human security”. Specifically, while realist school of thought focuses on national security, liberal theories mostly engage with the considerations on international security. In addition, constructivism, and critical theory brings concept of human security with the promise of emancipating traditional international relations theories. In this regard, as stated in this thesis, the protection of critical infrastructure, that directly affects state security, the functions and scope of international organizations and the well-being of citizens, is expected to be an essential consideration in the mentioned international relations theories’ approach to security studies.

In a changing world system, these three dimensions of security are also intertwined with each other by the emerge of the new security directions, which are directly related to those theories’ security considerations, such as energy security, cybersecurity, and critical infrastructure security. Even though any type of vulnerability on those fields causes equally serious damage for nations and intergovernmental organizations and individuals, among these fields, the importance of critical infrastructure is the lastly understood. Especially in Turkey, this field still remains in its infancy.

Therefore, this thesis investigated what Turkey’s place in the position is to ensure the country’s critical infrastructure protection compared to others and whether Turkey is successful in this field. First of all, the study compares the evolution of the field of infrastructure security in Turkey with the developments in the United States and European Union. Throughout the comparison under the four classifications of definitive process, legal background, institutional structure and devoting budget, the study displays that Turkey does not exceed the United States and European Union’s situation in the field nor does it even equal them. While Turkey shares a similar understanding of cybersecurity with the United States and European Union, the country does not embrace all the critical infrastructures sectors unlike the United States and the European Union. Still, Turkey does have a moderate number of laws and legislations and specific institutions regarding regulation of cybersecurity, there is no law, legislation or specific institutions existing to deal with the critical infrastructure protection. In addition to that, while United States and the European Union devote a high budget to ensure their infrastructure security, Turkey’s Ministry of Transport, Maritime Affairs and Communications, which is responsible for this field, does not provide any budget or information for expenses for securing the infrastructure.

This thesis also analyzes the public policy successes of Turkey’s last strategy called the 2016-2019 National Cyber Security Strategy. According to this analysis this strategy was a largely unsuccessful attempt. This is because this policy fails to satisfy the criteria for success in process success, programmatic success and political success dimensions under the policy success framework. For example, the strategy not only lacks the needed sustainability and innovative perspective for the process success, but it also considered worse than its predecessor the 2013-2014 strategy. The strategy also contains no action plan, nor budget, expense, resource information, and the developments in the strategy will not achieve the objectives. Therefore, it fails in the programmatic success area as well. Finally, a strategy that fails in these will also fail the in political success area.

In general, when looked into both the comparative analysis and public policy success results, it can be seen that critical infrastructure protection is a serious problem in Turkey. The main problem here is that the issue never got the attention it warranted. Therefore, no laws to achieve and regulate the critical infrastructure protection ever came from the government and no institutions were ever made to regulate and secure critical infrastructure. The chaos and the irregularities on the subject make it impossible to make laws or action plans about it. The absence of relevant law prevents achieving even the smallest of the objectives, and no resources are allocated for it. In reality, this topic is one of the most important to cover in the cyber security field. This is because critical infrastructure protection is one of the main reasons for the cyber security field to exist.

According to the National Cyber Security Index (2020), Turkey is 45th in the cyber security field. This shows that Turkey lags behind many countries in this area. Having a vulnerable cyber security also means vulnerable critical infrastructures. The attacks on Estonia’s, Ukraine’s, and America’s critical infrastructures shows the seriousness of this issue. Therefore, the question becomes what needs to be done to protect critical infrastructures from cyber-attacks? Here are the recommendations that can be concluded from this thesis:

- The appropriate laws and legislations for Turkey’s critical infrastructures systems must be made. This way the field of critical infrastructure protection would be put into a legal perspective.
- Turkey needs to increase the, currently 6, critical infrastructure sectors. This way the number of sectoral and corporate CIRTs for different sectors would be increased and a lot of the infrastructures would become under protection.
- The Critical Infrastructure area needs to be taken out of the Ministry of Transport, Maritime Affairs and Communications institution and put into its own institution with its own specific resources and budget allocated. This way the critical infrastructure protection topic will gain a central authority and, therefore, will be saved from getting analyzed under other authorities.
- New institutions, which are established for the protection and control of critical infrastructures, or sectoral and corporate CIRTs should specifically allocate a budget for the development and security of critical infrastructures. This way necessary investments can be made, and action can be taken immediately in emergencies.
- The regulatory agencies need to be formed and should regulate all public and private sectors.
- Detailed annual reports about whether the action plans are achievable or not should be made and publicized. This way realistic objectives can be set and also can be informed by previous mistakes.

REFERENCES

Aksakal, A. (1999). National Information Security Structure and Roles, Draft Law). *Journal of Turkish Librarianship, 13*(4), 438–457.

Antunes, S., & Camisao, I. (2018, February 27). Introducing Realism in International Relations Theory. Retrieved from https://www.e-ir.info/2018/02/27/introducing-realism-in-international-relations-theory/

Aron, R. (1967). What Is a Theory of International Relations? *Journal of International Affairs*, *21*(2).

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is Coming! *Comparative Strategy*, *12*(2), 141–165.

Atchinson, A., & Fox, D. (1997). The Politics of The Health Insurance Portability and Accountability Act. *Health Affairs*, *16*(3).

Ayoob, M. (1995). *The Third World Security Predicament: State Making, Regional Conflict, and the International System*. Lynne Rienner Publishers.

Balazs, J. (1985). A Note on the Interpretation of Security. *Development and Peace*.

Baldwin, D. (1997). The Concept of Security. *Review of International Studies*, *23*(1), 5–26. doi: 10.1017/S0260210597000053

Baldwin, D. A. (1993). *Neorealism and Neoliberalism: The Contemporary Debate*. New York: Colombia University Press.

Baylis, J. (2001). International and Global Security in the Post-Cold War Era. In J. Baylis & S. Smith (Eds.), *The Globalization of World Politics: An Introduction to International Relations*. Oxford: Oxford University Press.

Belyi, A. V. (2007). Energy security in International Relations theories. *Higher School of Economics, Cathedra on Political Issues of International Energy*.

Bührs, T., & Bartlett, R. V. (1993). *Environmental Policy in New Zealand. The Politics of Clean and Green*. Oxford University Press.

Bıçakçı, S., Ergun, D., & Çelikpala, M. (2016). The Cyber Security Scene in Turkey. *EDAM*, 22–51. Retrieved from https://edam.org.tr/document/CyberNuclear/edam_cyber_security_ch2.pdf

Bilgin, P. (2008). Critical Theory. In P. Williams (Ed.), *Security Studies: An Introduction* (pp. 89–102). New York: Routledge.

Booth, K. (1991). Security and Emancipation. *Review of International Studies*, *17*(4), 313–336. doi: 10.1017/S0260210500112033

Booth, K. (2005). *Critical Security Studies and World Politics*. : Lynne Rienner Publishers.

Bovens, M., Hart, P., & Peters, B. G. (2001). *Success and Failure in Public Governance: A Comparative Analysis*. London: Edward Elgar Pub.

Brian, A. K. (2006). The Realism of Hans Morgenthau (Master's thesis). Retrieved FOM https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=3579&context=etd

Brookson, C., Cadzow, S., Eckmaier, R., Gerber, B., Guarino, A., Rannenberg, K., Górniak , S. (2015). Definition of Cybersecurity Gaps and overlaps in standardisation. *ENISA*, 1–35. doi: 10.2824/4069

Browning, C., & McDonald, M. (2011). The future of critical security studies: Ethics and the politics of security: *European Journal of International Relations*. doi: 10.1177/1354066111419538

Buzan, B. (1983). People State & Fear. Sussex, London: Whealsheaf Books.

Buzan, B. (1984). Peace, Power, and Security: Contending Concepts in the Study of International Relations. *Journal of Peace Research*, *21*(2), 109–125. doi: 10.1177/002234338402100203

Buzan, B. (1991). New Patterns of Global Security in the Twenty-First Century. *International Affairs*, *67*(3).

Buzan, B. (1996). The timeless wisdom of realism? In S. Smith, K. Booth, & M. Zaleweski (Eds.), *International Theory: Positivism and Beyond*. Cambridge: Cambridge University Press.

Buzan, B., & Hansen, L. (2009). *The Evolution of International Security Studies*. Cambridge: Cambridge University Press.

Buzan, B., & Hansen, L. (2010). Beyond the Evolution of International Security Studies? *Security Dialogue*, *41*(6), 659–667. doi: 10.1177/0967010610388214

Buzan, B., & Wæver, O. (2003). *Regions and Powers*. Cambridge: Cambridge University Press.

Buzan, B., de Wilde, J., & Wæver, O. (1998). *Security: A New Framework for Analysis*. Boulder: CO: Lynne Rienner.

Cabinet Decision No. 2013/4890. Retrieved from https://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1.htm

Campbell, J. (1977). On Power: Oil Power in the Middle East. *Council on Foreign Relations*.

Carnesale, A., & Nacht, M. (1976). Forward. *International Security, 1*(1).

Carr, E. H. (1946). *The twenty years' crisis, 1919-1939: an introduction to the study of international relations*. London, UK: Macmillan.

Carter, J. (1980, January). USA. Retrieved from www.jimmycarterlibrary.org.

Cavelty, M. B. (2015). Cyber Security. In A. Collins (Ed.), *Contemporary Security Studies*. Oxford.

CERT-EU. (2020). Privacy Statement. Retrieved from https://cert.europa.eu/cert/plainedition/en/cert_privacy.html

Challenges to effective EU cybersecurity policy. (2009). *European Court of Auditors*. Retrieved from https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf

Chikhi, L. (2013, January 21). Algeria vows to fight Qaeda after 38 workers killed. *Reuters*. Retrieved from https://www.reuters.com/article/us-sahara-crisis/algeria-vows-to-fight-qaeda-after-38-workers-killed-idUSBRE90F1JJ20130121

Colebourne, J. (2012, December 22). An Appraisal of Robert Keohane: Neoliberalism and Liberal Institutionalism. Retrieved from https://www.e-ir.info/2012/12/22/an-appraisal-of-robert-keohane-neoliberalism-and-liberal-institutionalism-in-world-politics/

Colgan, J. D. (2015). Oil, domestic conflict, and opportunities for democratization. *Journal of Peace Research*, *52*(1).

Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Network and Information Security: Proposal for A European Policy Approach / COM/2001/0298. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52001DC0298

Communication from the Commission to the European Parliament and the Council - Internet governance : the next steps COM/2009/0277. (2009). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52009DC0277

Communicatıon from the Commission to the European Parliament, the Council, the European Economic and Social Committee and The Committee of the Regions A Digital Agenda for Europe /COM/2010/0245. (2010). Retrieved from https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52010DC0245R(01)

Council Directive 2008/114/EC. (2008). Retrieved from https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

Critical Infrastructures Protection Act of 2001. (2001). (p. 6) Retrieved from https://www.congress.gov/107/bills/s1407/BILLS-107s1407is.pdf

Cyber Security Policy. (2008). (p. 3). Retrieved from https://fas.org/irp/offdocs/nspd/nspd-54.pdf

Cyber: How Big Is the Threat? (2019). *European Parlimantery Services*. Retrieved from https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/637980/EPRS_ATA(2019)637980_EN.pdf

Cybersecurity and Infrastructure Security Agency. (2019a, November 14). What is Cybersecurity. Retrieved from https://www.us-cert.gov/ncas/tips/ST04-001

Cybersecurity and Infrastructure Security Agency. (2019b, December 12). National Infrastructure Protection Plan (NIPP) Security And Resilience Challenge. Retrieved from https://www.cisa.gov/nipp-security-and-resilience-challenge

Cybersecurity and Infrastructure Security Agency. (2020a, March 24). Critical Infrastructure Sectors. Retrieved from https://www.cisa.gov/critical-infrastructure-sectors

Cybersecurity and Infrastructure Security Agency. (2020b). Cyber Threat Source Descriptions. Retrieved from https://www.us-cert.gov/ics/content/cyber-threat-source-descriptions

Cybersecurity Enhancement Act of 2014. Retrieved from https://www.congress.gov/bill/113th-congress/senate-bill/1353/text

Cybersecurity Information Sharing Act of 2015.Retrieved from https://www.congress.gov/114/bills/s754/BILLS-114s754es.pdf

Cybersecurity Legislation 2019.Retrieved from https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2019.aspx

Darıcılı, A. B. (2019). Analysis of Turkey's Cyber Security Policies; the Potential Cyber Security Strategy of Turkey. *Turkish Journal of TESAM Academy*, *6*(2), 11–33.

Deudney, D., & Ikenberry, G. J. (1999). The Nature and Sources of Liberal International Order. *Review of International Studies*, *25*(2), 179–196. Retrieved from www.jstor.org/stable/20097589

Deutch, J., & Schlesinger, J. R. (2006). *National Security Consequences of U.S. Oil Dependency*. New York: Council on Foreign Relations.

Directive (EU) 2016/1148. Retrieved from https://eur-lex.europa.eu/eli/dir/2016/1148/oj

Doyle, M. W. (1983). Kant, Liberal Legacies, and Foreign Affairs. *Philosophy and Public Affairs*, *12*(3), 205–235. Retrieved from http://links.jstor.org/sici?sici=0048-3915(198322)12:3<205:KLLAFA>2.0.CO;2-O

Dunne, T., & Schmidt, B. C. (2016). Realism. In J. Baylis, S. Smith, & P. Owen (Eds.), *The Globalization of World Politics: An Introduction to International Relations* (7th ed.). Oxford University Press. doi: 10.1093/hepl/9780198739852.001.0001

Dyson, E. (1996). Cyberspace and the American Dream: A Magna Carta for the Knowledge Age. *The Information Society*, *12*(3), 295–308. doi: 10.1080/019722496129486

Enloe, C. (1996). Margins, silences and bottom rungs: How to overcome the underestimation of power in the study of international relations. In S. Smith, K. Booth, & M. Zalewski (Eds.), *International Theory: Positivism and Beyond* (pp. 186–202). Cambridge: Cambridge University Press. doi: 10.1017/CBO9780511660054.010

Erciş, M. (2008) Turkey Computer Incident Response Center Coordination Center. *TÜBİTAK-UEKAE Information Technologies Security Conference*.

EU GDPR Portal. (2020). Complete guide to GDPR compliance. Retrieved from https://gdpr.eu/

Euopean Union Agency. (2020). About ENISA. Retrieved from https://www.enisa.europa.eu/about-enisa

European Comission . (2019, August 27). Critical infrastructure protection. Retrieved from https://www.citationmachine.net/apa/cite-a-website/manual

European Comission. (2020). Protection. Retrieved from https://ec.europa.eu/home-affairs/what-we-do/policies/counter-terrorism/protection_en

European Comission. (2020a, March 17). Critical infrastructure and cybersecurity. Retrieved from https://ec.europa.eu/energy/topics/energy-security/critical-infrastructure-and-cybersecurity_en?redir=1#content-heading-0

European Commission . (2005). A European Program for the Protection of Critical Infrastructures, Report. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52005DC0576

European Commission. (2013). *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace JOIN/2013/01*.Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013JC0001

European Commission. (2015). *EGovernment in Turkey*. Retrieved from https://joinup.ec.europa.eu/sites/default/files/inline-files/eGovernment in Turkey - February 2016 - Edition 13_00_v3_02.pdf

European Commission. (2016, June 6). Geospatial Risk and Resilience Assessment Platform. Retrieved from https://ec.europa.eu/jrc/en/scientific-tool/geospatial-risk-and-resilience-assessment-platform

European Council. (2020, March 6). Cybersecurity in Europe: stronger rules and better protection. Retrieved from https://www.consilium.europa.eu/en/policies/cybersecurity/

European Union Agency for Network and Information Security. (2018). *Statement of Estimates 2018* (pp. 1–10).

European Union Agency for Network and Information Security. (2019). *Statement of Estimates 2019* (pp. 1–8).

European Union Agency for Network and Information Security. (2020). *Draft Statement of Estimates 2020 (Draft Budget 2020)* (pp. 1–16). Retrieved from ttps://www.enisa.europa.eu/about-enisa/structure-organization/management-board/management-board-decisions/mb-decision-2019_1-annex1-draft-pd2020-2022/

European Union Agency for Network and Information Security. (2020). *Draft Statement of Estimates 2020 (Draft Budget 2020)* (pp. 1–16).

Europol. (2018). *Internet Organised Crime Threat Assessment*.

Evans, G. (1998). *The Penguin Dictionary of International Relations*. London, UK: Penguin Books.

Exworthy, M., & Powell, M. (2004). Big Windows and Little Windows: Implementation in the Congested State. *Public Administration*, *82*(2), 263–281.

Farell, T. (2002). Constructivist Security Studies: Portrait of a Research Program. *International Studies Review*, *4*(1), 49–72. Retrieved from www.jstor.org/stable/3186274

Fearon, J. D. (1994). Domestic Political Audiences and the Escalation of International Disputes. *The American Political Science Review*, *88*(3), 577–592. Retrieved from http://www.jstor.org/stable/2944796 .

Federal Information Security Modernization Act of 2014. Retrieved from https://www.congress.gov/bill/113th-congress/senate-bill/2521

Federal Ministry of the Interior, Building and Community. (2009). *National Strategy for Critical Infrastructure Protection (CIP Strategy)*.

Fierke, K. M. (2015). *Critical Approaches to International Security*. Cambridge: Polity.

Finn, P. (2007, January 11). Russia-Belarus Standoff Over Oil Ends, Clearing Way for Accord. *Washington Post*. Retrieved from https://www.washingtonpost.com/wp-dyn/content/article/2007/01/10/AR2007011002094.html

Fireeye. (2017). *Cyber Risk Reports*. Retrieved from https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-world-eco-forum.pdf

Firoozabadi, J. D., & Ashkezarİ, M. Z. (2016). Neo-classical Realism in International Relations. *Asian Social Science*, *12*(6), 95–99. doi: 10.5539/ass.v12n6p95

Floyd, R. (2007). Human Security and the Copenhagen School's Securitization Approach: Conceptualizing Human Security as a Securitizing Move. *Human Security Journal*, *5*.

Folker, S. J. (2010). Neoliberalism. In T. Dunne, M. Kurki, & S. Smith (Eds.), *International Relations Theories: Discipline and Diversity*. New York: Oxford University Press.

Gallie, W. B. (1955). Essentially Contested Concepts. *Proceedings of the Aristotelian Society*, *56*, 167–198. Retrieved from www.jstor.org/stable/4544562

Geers, K. (2009). The Cyber Threat to National Critical Infrastructures: Beyond Theory. *Information Security Journal: A Global Perspective*, *18*, 1–7. Retrieved from https://ccdcoe.org/uploads/2018/10/Geers2009_The-Cyber-Threat-to-National-Critical-Infrastructures.pdf

Geva-May, I., & Pal, L. (1999). Policy Evaluation and Policy Analysis: Exploring the Differences. In N. Stuart (Ed.), *Policy Analysis Methods*. Nova Science Publishers.

Goldthau, A., & Witte, J. M. (2010). Introduction. In A. Goldthau & J. M. Witte (Eds.), *.), Global energy governance: The new rules of the game*. Washington: Brookings Institution Press.

Goldwyn, D. L., & Kalicki, J. H. (2005). *Energy, Security and Foreign Policy*. Washington: Woodrow Wilson Center Press.

Gorman, S. (2009, April 8). Electricity Grid in U.S. Penetrated by Spies. *The Wall Street Journal*. Retrieved from https://www.wsj.com/articles/SB123914805204099085

Government Accountability Office (GAO). (2005). Department of Homeland Security's (DHS's) Role in Critical Infrastructure Protection (CIP) Cybersecurit.

Gray, J. (1977). On the Contestability of Social and Political Concepts. *Political Theory*, *5*(3), 331–348. Retrieved from www.jstor.org/stable/190645

Greenberg, A. (2019, June 18). How Not to Prevent a Cyber-war with Russia. *Wired*. Retrieved from https://www.wired.com/story/russia-cyberwar-escalation-power-grid/

Gross, M. J. (2011, March 2). A Declaration of Cyber-War. *Vanity Fair*. Retrieved from https://www.vanityfair.com/news/2011/03/stuxnet-201104

Halpern, M. (2015, April 22). Iran Flexes Its Power by Transporting Turkey to the Stone Age. *Observer*. Retrieved from https://observer.com/2015/04/iran-flexes-its-power-by-transporting-turkey-to-the-stone-ages/

Hayward, A. (2005). Emancipation in the Critical Security Studies Project. In K. Booth (Ed.), *Critical security studies and world politics* (pp. 189–213). Lynne Rienner Publishers.

Heurlin, B., & Kristensen, K. S. (2002). International Security. *UNESCO: Encyclopedia of Life Support Systems (EOLSS)*, 693–719. Retrieved from https://www.eolss.net/sample-chapters/C14/E1-35-04-02.pdf

HIPAA Guide. (2018). Why was HIPAA Created? Retrieved from https://www.hipaaguide.net/hipaa-for-dummies/

Hobbes, T. (1946). *Leviathan*. Oxford: Basic Blackwell.

Holland, & Milkensen. (2009, April 8). US concerned power grid vulnerable to cyber-attack. *Reuters*. Retrieved from https://in.reuters.com/article/cyberattack-usa/update-2-us-concerned-power-grid-vulnerable-to-cyber-attack-idINN0853911920090408

Homeland Security Presidential Diective 7.Retrieved from https://fas.org/irp/offdocs/nspd/hspd-7.html

Information and Communications Technologies Authority . (2020). Retrieved from https://www.şent.gov.tr/siber-guvenlik-genel-bilgi

Information Security Association. (2012). *National Cyber Security Strategy* . Retrieved from https://www.bilgiguvenligi.org.tr/wp-content/uploads/2016/03/Ulusal_Siber_Guvenlik_Stratejisi.pdf

International Atomic Energy Agency. (2007). *Iaea Safety Glossary Terminology Used in Nuclear Safety And Radiation Protection*. Vienna . Retrieved from https://www-pub.iaea.org/mtcd/publications/pdf/pub1290_web.pdf

Jong-Chen, J., & O'Brien, B. (2017). A Comparative Study: The Approach to Critical Infrastructure Protection in the U.S., E.U., and China. *Wilson Center*, 1–14.

Karabacak, B., & Özkan, S. (2009). Critical Infrastructure Protection Status and Actions Items of Turkey. *International Conference on EGovernment Sharing Experience*, 173–180.

Karanacak, B. (2011). Kritik Altapılar ve Kritik Altyapıların Korunması. *Siber Savunma Sempozyumu / TÜBİTAK-BİLGEM*, 1–17.

Kaspersky. (2019). *Story of the year 2019: Cities under ransomware siege*. Retrieved from https://securelist.com/story-of-the-year-2019-cities-under-ransomware-siege/95456/

Katzenstein, P. (1996). Introduction: Alternative Perspectives on National Security. In P. Katzenstein (Ed.), *The Culture of National Security: Norms and Identity in World Politics*. New York: Cambridge University Press.

Kemp, G. (1978). Scarcity and Strategy. *Council on Foreign Relations*.

Keohane, R. O. (1984). *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton: Princeton University Press.

Keohane, R. O. (1989). *International Institutions and State Power: Essays in International Relations Theory*. Boulder: CO: Westview.

Keohane, R. O., & Martin, L. L. (1995). The Promise of Institutionalist Theory. *International Security*, *20*(1), 39–51. doi: 10.2307/2539214

Keohane, R. O., & Nye, J. S. (1977). *Power and Interdependence*. Boston, USA: Brown.

Kissenger, H. (1976). Documentation: Foreign Policy and National Security. *International Security, 1*(1).

Klare, M. T., & Williams, P. (2008). Energy Security. In *Security Studies: An Introduction* (pp. 483–493). New York: Routledge.

Knorr, K. (1973). 'National Security Studies: Scope and Structure of the Field. In F. N. Trager & P. Kronenberg (Eds.), *National Security and American Society: Theory, Process and Policy*. Laxrance.

Kovacks, L. (2018). Cyber Security Policy And Strategy İn The European Union And Nato. *Land Forces Academy Review XXIII*, *1*.

Lake, D. (1992). Powerful Pacifists: Democratic States and War. *The American Political Science Review*, *86*(1), 24–37. doi: 10.2307/1964013

Layne, C. (1993). The Unipolar Illusion: Why New Great Powers Will Rise. *International Security*, *17*(4), 5–51. Retrieved from http://www.jstor.org/stable/2539020.

Lebow, R. N., & Smiths, S. (2007). Classical realism. In T. Dunne & M. Kurki (Eds.), *International relations theories*. Oxford University Press.

Lugar, R. (2005). Opening statement, Hearing on the high costs of oil dependency.' *Senate Committee on Foreign Relations*. Retrieved from foreign.senate.gov

Maavak, M. (2006). *Panoptic World: Globocops of Energy Security*. The Korea Herald.

Machiavelli, N. (1981). *The Prince*. Penguin Books.

Macintyre, A. (1973). The Essential Contestability of Some Social Concepts. *Ethics*, *84*.

Maoz, Z., & Russett, B. (1992). Alliances, Contiguity, Wealth, and Political Stability: Is the Lack of Conflict between Liberal Democracies a Statistical Artifact? *International Interactions*, *17*(3), 245–267. doi: 10.1080/03050629208434782

Maoz, Z., & Russett, B. (1993). Normative and Structural Causes of Democratic Peace, 1946–1986. *American Political Science Review*, *87*(3), 624–638. doi: 10.2307/2938740

March, J., & Olsen, J. (1998). The Institutional Dynamics of International Political Orders. . *International Organization*, *52*(4), 943–969. Retrieved from www.jstor.org/stable/2601363

Marsh, D., & McConnell, A. (2010). Towards a Framework for Establishing Policy Success. *Public Administration*, *88*(2), 564–583. doi: 10.1111/j.1467-9299.2009. 01803.x

Martinez, M. (2014, February 8). Sniper attack on Silicon Valley power grid spurs security crusade by ex-regulator. *CNN*. Retrieved from https://edition.cnn.com/2014/02/07/us/california-sniper-attack-power-substation/index.html

McDonald, M. (2008). Constructivism. In P. D. Williams (Ed.), *Security Studies: An Introduction*. Routledge.

Mearsheimer, J. (1994). The False Promise of International Institutions. *International Security*, *19*(3), 5–49. doi: 10.2307/2539078

Mearsheimer, J. (2001). *The Tragedy of Great Power Politics*. W. W. Norton & Company.

Meiser, J. W. (2018, February 18). Introducing Liberalism in International Relations Theory. Retrieved from https://www.e-ir.info/2018/02/18/introducing-liberalism-in-international-relations-theory/

Minkel, J. R. (2008, August 13). The 2003 Northeast Blackout--Five Years Later. Retrieved from https://www.scientificamerican.com/article/2003-blackout-five-years-later/

Mohapatra, N. H. (2017). Energy security paradigm, structure of geopolitics and international relations theory: from global south perspectives. *GeoJournal*, *82*, 683–700. doi: 10.1007/s10708-016-9709-z

Moran, D., & Russell, J. A. (2009). The militarization of energy security. In D. Moran & J. A. Russell (Eds.), *Energy security and global politics: The militarization of resource management* (pp. 1–19). Routledge.

Moravcsik, A. (1997). Taking Preferences Seriously: A Liberal Theory of International Politics. *International Organization*, *51*(4), 513–553. doi: 10.1162/002081897550447

Morgenthau, H. J. (1948). *Politics among Nations: The Struggle for Power and Peace*. New York, USA: Alfred A. Knopf.

Mukherjee, S. (2019). Implementing Cybersecurity in the Energy Sector. *University of the Cumberlands (Formerly Cumberland College)*.

National Cybersecurity Protection Advancement Act of 2015. Retrieved from https://www.congress.gov/bill/114th-congress/house-bill/1731

National Energy Policy Development Group. (2001). *Reliable, Affordable, and Environmentally Sound Energy for America's Future.* Retrieved from https://www.nrc.gov/docs/ML0428/ML042800056.pdf

National Institute of Standards and Technology. (2020). FISMA Implementation Project. Retrieved from https://csrc.nist.gov/projects/risk-management/detailed-overview

Navari, C. (2008). Liberalism. In P. D. Williams (Ed.), *Security Studies: An Introduction* (pp. 29–43). Routledge.

Newman, L. (2019, June 5). What Israel's Strike on Hamas Hackers Means for Cyberwar. *Wired*. Retrieved from https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/

NSW Department of Justice. (2018). *Nsw Critical Infrastructure Resilience Strategy Partner, Prepare, Provide*. Sydney. Retrieved from https://www.emergency.nsw.gov.au/Documents/publications/policies/NSW Critical Infrastructure Resilience Strategy 2018.pdf

Nye, J., & Owens, W. (1996). America's Information Edge. *Foreign Affairs*, *75*(2), 20–36. doi: 10.2307/20047486

Office of Management and Budget. (2020). Cyber Security Funding . Retrieved from https://www.whitehouse.gov/wp-content/uploads/2019/03/ap_24_cyber_security-fy2020.pdf

Olivares. (2018, May 2). Has Critical Security Studies Run Out of Steam? Retrieved from https://www.e-ir.info/2018/05/02/has-critical-security-studies-run-out-of-steam/

Onjeyi, I., Bazilian, M., & Bronk, C. (2014). Cyber Security and Critical Energy Infrastructure. *The Electricity Journal*, *27*(2), 52–60. doi: 10.1016/j.tej.2014.01.011

Ottis, R. (2007). Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. *Cooperative Cyber Defence Centre of Excellence*, 1–6. Retrieved from https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdff

Overland, I. (2016). Energy: The Missing Link in Globalization. *Energy Research and Social Science, 14*, 122–130. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3023146

Owen, J. M. (2010). *Liberalism and Security*. Oxford University Press.

Özdamar, Ö. (2009). Energy, Security and Foreign Policy. *ISA*, *3*(81). Retrieved from http://ozgur.bilkent.edu.tr/download/14Energy, Security, and Foreign Policy.pdf

Paleri, P. (2008). *National Security: Imperatives and Challenges*. Tata McGraw-Hill Education.

Palmer, M. A. (1992). *Guardians of the Gulf*. New York: Free Press.

Peoples, C., & Vaughan-Williams, N. (2010). *Critical Security Studies: An Introduction*. London: Routledge.

Perlroth, N., Scott, M., & Frenkel, S. (2017, June 27). "Cyberattack Hits Ukraine Then Spreads Internationally. *The New York Times*. Retrieved from https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html

Powell, R. (1991). bsolute and Relative Gains in International Relations Theory. *The American Political Science Review*, *85*(4), 1303–1320. doi: 10.2307/1963947

Pugh, J. (2005). "Democratic Peace Theory: A Review and Evaluation. *CEMPROC Working Paper Series*. doi: 10.13140/RG.2.2.36339.12324

Regulation (EU) 2016/679. Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj

Regulation (EU) 2018/1725. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1725

Regulation (EU) No 526/2013. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32013R0526

Reiter, D., & Stam, A. (2002). *Democracies at War*. Princeton University Press. doi: 10.2307/j.ctt7s7tq

Reus-Smit, C. (1997). The Constitutional Structure of International Society and the Nature of Fundamental Institutions. *International Organization*, *51*(4), 555–589. Retrieved from www.jstor.org/stable/2703499

Room, J. (1993). *Defining National Security: The Nonmilitary Aspects*. Council on Foreign Relations Press.

Rose, G. (1998). Neoclassical Realism and Theories of Foreign Policy. *World Politics*, *51*(1), 144–172. Retrieved from www.jstor.org/stable/25054068

Rouse, M. (n.d.). Critical Infrastructure. Retrieved from https://whatis.techtarget.com/definition/critical-infrastructure

Rustad, S. A., & Binningsbø, H. (2012). A price worth fighting for? Natural resources and conflict recurrence. *Journal of Peace Research*, *49*(4).

Sedkaoui, S. (2019). *Big Data Analytics for Entrepreneurial Success*. IGI Global.

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a More Representative Definition of Cyber Security. *The Association of Digital Forensics, Security and Law (ADFSL)*, *12*(2).

Schweller, R. L. (2003). The Progressiveness of Neoclassical Realism. In C. Elman & M. E. Elman (Eds.), *Progress in International Relations Theory*. MIT Press.

Shiraev, E., & Zubok, V. (2015). *International Relations*. Oxford University Press.

Simon, C. A. (2016). *Policy Analysis*. Encyclopædia Britannica, Inc. Retrieved from https://www.britannica.com/topic/policy-analysis

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.

Smith, C. D. (2006). *Palestine and the Arab–Israeli Conflict*. New York: Bedford.

Smith, S., & Smith, S. (2007). Introduction: Diversity and Disciplinarity in International Relations Theory. In T. Dunne & M. Kurki (Eds.), *International Relations Theories: Discipline and Diversity*. Oxford, UK: Oxford University Press.

Smoke, R., & Polsby, N. W. (1975). National Security Affairs. In F. I. Greenstein (Ed.), *Handbook of Political Science* (Vol. 8). International Politics.

Solms, R., & Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*(2013), 97–102. doi: 10.1016/j.cose.2013.04.004

Stokes, D. (2007). Blood for oil? Global capital, counter-insurgency and the dual logic of American energy security. *Review of International Studies*, *3*(2).

Şentürk, H., Çil, Z., & Sarıoglu, Ş. (n.d.). Cyber Security Analysis of Turkey. International Journal of Information Security Science, 1(4), 112–125.

Tadjbakhsh, S., & Chenoy, A. (2007). *Human Security: Concepts and Implications*. Taylor &Francis.

Taliaferro, J. W. (2000). Security Seeking under Anarchy: Defensive Realism Revisited. *International Security*, *25*(3), 128–161. Retrieved from www.jstor.org/stable/2626708

The Department of Homeland Security. (2013). Supplemental Tool: Connecting to the NICC and NCCIC. Retrieved from https://www.cisa.gov/sites/default/files/publications/NIPP-2013-Supplement-Connecting-to-the-NICC-and-NCCIC-508.pdf

The Department of Homeland Security. (2018, March 15). Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors. Retrieved from https://www.us-cert.gov/ncas/alerts/TA18-074A

The Department of Homeland Security. (2019a, September 20). Homeland Security Information Network - Critical Infrastructure.

The Department of Homeland Security. (2019b, October 29). Critical Infrastructure Security. Retrieved from https://www.dhs.gov/topic/critical-infrastructure-security

The Department of Homeland Security. (2020). US-CERT United States Computer Emergency Readiness Team. Retrieved from https://www.us-cert.gov/sites/default/files/publications/infosheet_US-CERT_v2.pdf

The European Union Directive 676. Retrieved from https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0676:FIN:EN:PDF

The Ministry of Transport, Maritime Affairs and Communications. (n.d.). *2016-2019 National Cyber Security Strategy*. Retrieved from https://www.uab.gov.tr/uploads/pages/siber-guvenlik/ulusalsibereng.pdf

The Ministry of Transport, Maritime Affairs and Communications. (n.d.). *National Cyber Security Strategy and 2013-2014 Action Plan*.

The Ministry of Transportation, Maritime and Communication. (2017). *2016 Administrative Activity Report.* Retrieved from https://www.uab.gov.tr/uploads/pages/butce-raporlari/2016-yili-idare-faaliyet-raporu.pdf

The Ministry of Transportation, Maritime and Communication. (2018). *2017 Administrative Activity Report.* Retrieved from https://www.uab.gov.tr/uploads/pages/butce-raporlari/2017-yili-idare-faaliyet-raporu.pdf

The Ministry of Transportation, Maritime and Communication. (2019). *2018 Administrative Activity Report.* Retrieved from https://www.uab.gov.tr/uploads/pages/butce-raporlari/2018-idare-faaliyet-raporu.pdf

The Ministry of Transportation, Maritime and Communication. (2020). *2019 Administrative Activity Report*. Retrieved from https://www.uab.gov.tr/uploads/pages/butce-raporlari/2019-yili-idare-faaliyet-raporu.pdf

The Presidential Policy Directive 63. Retrieved from https://fas.org/irp/offdocs/pdd/pdd-63.pdf

The White House (n.d.) *National Security Council*. Retrieved from https://www.whitehouse.gov/nsc/

The White House. (2018). *National Cyber Strategy of Unites States of America*. Washington. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

Theys, S. (2018, February 23). Introducing Constructivism in International Relations Theory. Retrieved from https://www.e-ir.info/2018/02/23/introducing-constructivism-in-international-relations-theory/

Tripp, E. (2013, June 14). Realism: The Domination of Security Studies. Retrieved from https://www.e-ir.info/2013/06/14/realism-the-domination-of-security-studies/

Turkish Personal Data Protection Law no. 6698. Retrieved from https://www.kisiselverilerinkorunmasi.org/kanunu-ingilizce-ceviri/

U.S. Code § 6801.Protection of nonpublic personal information. Retrieved from https://www.law.cornell.edu/uscode/text/15/6801

U.S. Code § 6809.Definitions. Retrieved from https://www.law.cornell.edu/uscode/text/15/6809

Ukraine power cut 'was cyber-attack'. (2017, January 11). *BBC*. Retrieved from https://www.bbc.com/news/technology-38573074

Ullman, R. H. (1983). Redefining Security. *International Security*, *8*(1), 129–153.

United States Department of Energy. (n.d.). Cybersecurity. Retrieved from https://www.energy.gov/national-security-safety/cybersecurity

Ünver, M., Canbay, C., & Özkan, H. B. (2010). *Kritik Altyapıların Korunması* (pp. 1–49). Bilgi Teknolojileri ve Koordinasyon Daire Başkanlığı.

van der Meulen, N., Jo, E., & Soesanto, S. (2015). Cybersecurity in the European Union and Beyond Exploring the Threats and Policy Responses. *RAND Europe*.

Wæver, O. (1997). *Concepts of Security*. University of Copenhagen.

Walt, S. M. (1985). Alliance Formation and the Balance of World Power. *International Security, 9*(4), 3–43. doi: 10.2307/2538540

Walt, S. M. (1991). The Renaissance of Security Studies. *International Studies Quarterly*, *35*(2), 211–239. doi: 10.2307/2600471

Walt, S. M. (2010). *Realism and Security*. Oxford, UK: Oxford University Press.

Waltz, K. (1979). *Theory of International Politics.* New York: McGraw-Hill.

Waltz, K. (1988). The Origins of War in Neorealist Theory. *Journal of Interdisciplinary History, 18*(4), 615–628. Retrieved from http://www.jstor.org/stable/204817

Waltz, K. (1989). The Origins of War in Neorealist Theory. In R. Rotberg & T. Rabbs (Eds.), *The Origin and Prevention of Major Wars* (pp. 39–52). Cambridge: Cambridge University Press. doi: 10.1017/CBO9780511601033.003

Wendt, A. (1992). Anarchy is what States Make of it: The Social Construction of Power Politics. *International Organization, 46*(2), 391–425. Retrieved from www.jstor.org/stable/2706858

Wendt, A. (1995). Constructing International Politics. *International Security, 20*(1), 71–81. doi: doi:10.2307/2539217

Wendt, A. (1999). *Social Theory of International Politics*. New York: Cambridge University Press.

Wesley, M. (2007). *Energy Security in Asia*. London: Routledge.

Whyte, A. (2012, June 11). Neorealism and neoliberal institutionalism: born of the same approach? Retrieved from https://www.e-ir.info/2012/06/11/neorealism-and-neoliberal-institutionalism-born-of-the-same-approach/

Wilson, P. (1998). The Myth of the 'First Great Debate'. *Review of International Studies*, *24,* 1–15. Retrieved from www.jstor.org/stable/20097558.

Wilson, P. (2011). Idealism and International Relations. In K. Dowding (Ed.), *Encyclopedia of Power*. SAGE Publication.

World Energy Council. (2016). *World Energy Scenarios*. Retrieved from https://www.worldenergy.org/assets/downloads/World-Energy-Scenarios-2016_Summary-Report.pdf

Wright, Q. (1952). Realism and Idealism in International Politics. *World Politics, 5*(1), 116–118. doi: 10.2307/2009091

Yergin, D. (2006). Ensuring Energy Security. *Foreign Affairs*, *85*(2), 69–82.

Zetter, K. (2016, February 3). Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. Retrieved from https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/