STUDY OF THE CYBER SECURITY MEASURES: COMPARATIVE WORK OF THE UNITED STATES AND TURKEY

Eylül Aydın

JUNE, 2021

STUDY OF THE CYBER SECURITY MEASURES: COMPARATIVE WORK OF THE UNITED STATES AND TURKEY

…

MA THESIS

DEPARTMENT OF POLITICAL SCIENCE AND INTERNATIONAL RELATIONS

Eylül Aydın

YEDİTEPE UNIVERSITY

June, 2021

PLAGIARISM

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

Eylül Aydın

23.06.2021

ABSTRACT

Cyber security is to protect data, networks, programs and other information from unauthorized access. Cyber security is very important in today's world due to some security threats and cyber attacks. Many companies develop software programmes for data protection. Cyber attackers use lots of software and code in cyberspace to commit cybercrime. It exploits weaknesses in software and hardware design by using malware. Today, cyber security threats are very dangerous for the security of the country due to high internet access. Therefore, cyber security is one of the biggest needs in the world. Cybersecurity breach is an ever-present threat facing any technology-based industry. It is especially dangerous for government agencies that hold sensitive civil and national security data in their information systems. This risk has pushed each country to create its own cyber security policy. In the globalizing world, one of the places where wars are now carried is cyberspace. In this direction, each country creates its own policy. In this study, Turkey's cyber security policy and the cyber security policy of the United States have been compared. It is aimed to compile the security policies by presenting the differences between the cyber attacks in America and Turkey and their approaches to attacks.

Keywords: Cyber Security, Cyber Attack, Cyber Security Policies

ÖZET

Siber güvenlik; verileri, ağları, programları ve diğer bilgileri yetkisiz erişime karşı korumaktır. Günümüz dünyasında siber güvenlik, bazı güvenlik tehditleri ve siber saldırılar nedeniyle çok önemlidir. Veri koruma için birçok şirket yazılım geliştirmektedir. Siber saldırganlar, siber suç işlemek için siber uzayda çok sayıda yazılım ve kod kullanır.Bu saldırganlar, kötü amaçlı yazılımları kullanarak yazılım ve donanım tasarımındaki zayıflıklardan yararlanmaktadır. Günümüzde yüksek internet erişimi nedeniyle siber güvenlik tehditleri ülkenin güvenliği için çok tehlikeli olmaktadır. Bu nedenle siber güvenlik dünyanın en büyük ihtiyaçlarından biridir. Siber güvenlik ihlali, teknolojiye dayanan herhangi bir sektörün karşı karşıya kaldığı her zaman mevcut bir tehdittir. Bilgi sistemlerinde hassas sivil ve ulusal güvenlik verilerini tutan devlet kurumları için özellikle tehlikelidir. Bu risk, her ülkeyi kendi siber güvenlik politikasını oluşturmaya itmiştir. Küreselleşen dünyada artık savaşların taşındığı yerlerden biri de siber uzaydır. Bu doğrultuda her ülke kendi politikasını oluşturmaktadır. Bu çalışmada Türkiye'nin siber güvenlik politikası ve Amerika Birleşik Devletleri'nin siber güvenlik politikası karşılaştırılmıştır. Amerika'da ve Türkiye'de gerçekleşen siber saldırılar ve ülkelerin saldırılara yaklaşımları arasındaki farklar okuyucuya sunularak güvenlik politikalarının derlenmesi amaçlanmıştır.

Anahtar Kelimeler: Siber Güvenlik, Siber Saldırı, Siber Saldırı Politikaları

ACKNOWLEDGEMENTS

To my mother Esra AYDIN and my father Dinçer AYDIN for their endless support and without whom this dissertation would have never been completed. Also to my dear friend Ali Can İlvan for always pushing me to go further with my work.

TABLE OF CONTENTS

LIST OF FIGURE

SECTION 1: INTRODUCTION

The dependence of countries on information technologies and especially the Internet is increasing day by day. Today, it is estimated that 294 billion e-mail messages are sent daily on the global network and 168 million DVDs of information are produced in one day. Youtube servers upload 864,000 hours of video daily, Netflix users watch 22 million hours of TV or cinema a day. Approximately two thirds of the world's population have internet connections and 20% have memberships in social networks. Again, 85% of the world population uses mobile phones and 15% of them shop via mobile phones (Climburg, 2012:76). These figures show how much the dependency on information technologies has increased.

Information technologies, besides the opportunities they provide for facilitating life, have led to the development of new concerns in terms of security. Now, in this new world, criminal acts such as theft and fraud have become possible without the need for physical contact or being in the same place with the victim. In addition, information technologies increased the communication skills of crime groups or terrorist organizations, strengthened propaganda opportunities and enabled the emergence of new fields of activity.

The globalization process, which has gained momentum in recent years, has started to decrease the importance of the borders of countries in terms of national security policy. Globalization, reshaped the power distribution channels of countries, revealed asymmetric power relations and resulted in a more comprehensive and different redefinition of national security needs. When wars and internal revolts are kept aside, the factors affecting the power balances between countries have changed as a result of globalization and the protection of the interests of the country has become more difficult than the pre-globalization period (Kay, 2004:11). In this change of balance, cyber security has come to the fore as a new and very critical element of the national security policy.

In this study, cyber security measures will be examined within the scope of international relations. Cyber security theories will also be examined by examining international relations theories. In this research cyber security measures of Turkey and the United States of America will be compared.

SECTION 2: LITERATURE REVIEW

After the World Wars and nuclear attacks that states committed against each other, conjoncture of the World was all about the status disputes. Countries tried to dominate the World by using heavy and destructive weapons. Basically if one had a powerful weapon that no other possess, that is the most powerful among them all.

Then the variables of the power system have changed after the globalization process. We have come a long way from sticks and stones to cyber warfare. To be able to understand the changes between attitudes in the international area, we have to look closely at the security concept.

The concept of security not only defined the armament methods, but also affected the functioning of politics. That being said, the aim of this chapter is to display the shifting policy of security towards decades based on grand international relations theories. The evaluation process of security to cyber security will be presented via realist, liberalist and constructivist theories of International Relations. The reason this study only examines the three mentioned theories is that; mainly these three theories have a focus on security concepts. The link between these theories and cyber security will be portrayed to form the basis of cyber security understanding in national security.

SECTION 3: DEFINING SECURITY IN INTERNATIONAL RELATIONS

3.1. Definition of Security

There are many different forms of understanding of the concept of security and it has changed and evolved significantly over time. But security has been a significant factor in international relations over the years. There are many types of sense of security. In the international system, security is more concerned about the safety of states and their people.

Robinson (2008:2) uses following phrases when he tries to define security: Security implies an absence of threat. This can be viewed as an absolute-either one is secure or one is not, threats exist or they do not –or, as is more usual, as a relative condition-one can have varying degrees of security, more or less protection from the threat. One can also view security in objective and subjective terms, in other words as an evaluation of how many threats people and institutions actually face and how much protection against them they actually have, versus how secure they feel.

As indicated above there are many different types of definition on security. Security is mostly interpreted as it goes along with the accumulation of power meaning that if you have a strong army and a strong economy to support it then one can indeed feel safe. Security has been considered as a service and power is the most crucial tool to achieve it. The traditional view of the security concept for many centuries was concerned with defending national sovereignty in terms of citizens, territorial integrity, and political autonomy, namely the system of government. In order to achieve this type of security, a strong and advanced military was a necessary instrument (Schaefer, 2013:7).

3.1.1. Security according to Realist and Neorealist Theory

The concept of security, which is one of the main elements that determine international affairs, varies according to time, place and conditions of the period, and with the advancing technology and changing conditions, the tools and equipment used in this context change and progress over time. In primitive times, human beings defended themselves against external dangers with fire, stone and sickle. Over time, defense tools used against risks and threats of varying quality and quantity have changed (Howard & Lipner, 2006:76).

In order to talk about the concept of security, there must be any risk or threat and also the question of what and whose security must be answered. The risks and threats in question also differ according to time, place and events, as well as the equivalent of who and what is security. The security phenomenon has been realized for the first time in human history with primitive tools and equipment to protect against external threats. While the concept of security has changed according to the general characteristics of each state, society's values, culture and geography throughout history, there is also a conflict-reconciliation relationship between individuals, groups and states, which is directly proportional to the security-threat relationship. Security is one of the main elements that determine international relations within the scope of state and sovereignty. The concept of security has been shaped according to the threats and risks that emerged under different conditions in different periods in the historical process. Along with these changing conditions, the meaning, content of the concept of security and the factors that make up the concept of security differ within the scope of international theories (Waltz, 1990:23).

Kenneth Waltz has been regarded as the founder and pioneer of neorealism, or structural realism as he calls it. Waltz has taken some pieces of classical realism and neoclassical realism as a starting point, such as the existence of an independent state and their operation in anarchy (Waltz, 2004:2). However, the point Waltz differed was his effort to provide a scientific explanation for the international political system. In Waltz's view, the best theory of international relations focuses on the structure of the central system, the interaction between units and the continuity of system changes. In classical realism, state leaders and their international decisions are the center of attention. In neorealism, on the contrary to realism, actors are considered as external factors. Because it is thought that the structure will compel them to behave correctly. However, Waltz, by separating the anarchic nature of the international system from domestic politics, emphasizes that the actors in domestic politics act within the limits set by the central authority or authorities called the state or government (Waltz, 1988:617). Neorealist or structural theory supports the notion that states' position in the international system largely determines their behavior. According to Waltz's neorealist theory, the main feature of international affairs is between the decentralized structure of anarchy and the state. Waltz recognized that states' core concerns are security and survival (Waltz, 2000:13). He also said that the biggest problem of the conflicts of the great powers is war and the biggest task is peace and security (Waltz, 2004:5).

According to Thomas Hobbes (1967:67), human nature has to establish security in order to set norms, and imposes penalties for performing these processes. A higher authority is essential for the realization of these conditions. This theory is the same on the basis of states. While individuals struggle among themselves for the goal they want to achieve, nations are in constant struggle for their own interests. There is a direct relationship between national interests and power, and nations have to act with policies that will obtain or retain power for their own goals in line with their own interests (Uğrasız, 2003: 143).

Inspired by Hobbes' views, Morgenthaue & Kennan (1965) stated that the state and the interests of the state, which are the sole and dominant actors of international relations, are more important than anything else, emphasizing that the international system is in anarchy and the absence of a higher authority in this system. By drawing attention to the environment of conflict between the sovereign states, international relations are seen as a natural state of war. By nature, people are physically and mentally equal, but equality brings insecurity. Because individuals have equal demands and goals from their equality, and therefore they are in constant struggle with each other, even enemies, in order to achieve their goals, so it is inevitable that they become a threat to each other. (Hama, 2017).

As a result, war emerges from insecurity. The power potential of a state should not be limited to technology or the strategic commodity it holds.

Geological factors such as geography, demographic characteristics and environmental assets constitute the power potential of a state. Realist theory focuses on military power as an element of power. States that hold military power in the international system can provide their security better than others. In a system where there are no international norms, states that maximize military power may remain in the system (Küçüksolak, 2012: 203).

During the Cold War, when realism was most effective, it caused the formation of blocs between the USA and the Soviet Union as a regional possibility between the newly independent nation-states. During this period, security policies developed in an ideologically based and two opposed international system, within the framework of an institutional structure as the Western and Eastern Bloc. In this period, an anarchic international environment was formed with the struggle for mutual power, and the security issue was conceptualized from a state and military threat-oriented perspective, which is at the center of the realist approach (Buzan, 2008: 112). The security of individuals, on the other hand, depends on the security of the state, and people are safe only as long as the state is safe . According to the realists, there is no permanent security situation in the society due to the bad nature of the human being, but security can be provided with a higher authority. It sees security for states as safe in the presence of a hegemonic power with the processes of the balance of a powerful system. Of course, there will be situations where the day balance is weak in some periods. In this way, while the realist approach adopted the military power in a very narrow scope against external threats, the neorealist approach emphasized that military power alone was not sufficient to ensure national security, and they advocated determining security policies in a very wide scope according to the types and targets of the threat sources. Liberalism is the opinion that defends the peaceful solution of security problems in the international environment in order to eliminate and rebuild the social and economic infrastructure problems that emerged with the destructive effect of World War I. Idealism shaped around liberalism, II. With the outbreak of the World War, it has been subjected to criticism. Especially with Edward Hallett Carr, one of the founders of realism, he came up with his criticism of the liberal idealist approach. (Carr, 1994: 72-87):

Although liberalism sees the state as an important actor, it does not make a definite judgment that it is the only actor. In international security studies, liberal theories have been studied extensively on the security of states and how peace can be achieved. The main differences between liberal theories occur in how security can be achieved, as will be seen below. The so-called neoliberal institutionalism approach argues that states focus on absolute gains, not relative gains, and that cooperation is possible. The existence of NATO as a joint defense and security organization after the Cold War shows that inter-state cooperation in the field of security is possible and attractive (Küçüksolak, 2012: 203). Under conditions of anarchy, where realist theory in international security passes abstractly through basic provisions, the issues of security cooperation are dealt with in more depth by liberal theory.

With the collapse of the world Eastern Block in the 1990s, it witnessed the rapid spread of neoliberal policies. These radical changes in the economic approach in the world have now necessitated the abandonment of the classical security understanding, which means defending the borders against foreign attacks with military measures. The point that should not be overlooked here is that the fundamental changes in the security approach are not caused by the collapse of the Soviet Bloc but by the neoliberal change in the economy and production model.

In summary, the security approach in the neoliberal era focuses on the security of the changing and globally circulating capital. Achieving new markets, investment areas, access to raw material reserves and cheap labor are vital for the security of capital accumulation. All these requirements are provided through the structural and functional transformation of nation states. In this transformation, the downsizing of the state with neoliberal policies and the transfer of even the security issues, which are among the fundamental duties of the state, to private capital are of great importance. Security policies are also used as a tool to achieve this transformation (Hama, 2017).

Developing and underdeveloped countries apply the approach of integration with the neoliberal market, which they define as a way of development and modernization, at the expense of the real interests of their countries and the increasing income gap between social classes. With the end of the Cold War, the risk of conflict between major states has decreased and security policies have been reorganized in this direction (Rosecrance & Thompson, 2003: 377). However, the risk of operations by large states against small states or the risk of internal conflict based on ethnic discrimination in underdeveloped countries is still relevant.

There are three main purposes of ensuring security in neoliberal theories. The first is to reorganize the socio-economic structures and class relations of capitalist countries, the second is to restructure international relations in the context of neoliberal structuring by placing international relations on the framework of developed underdeveloped or central and peripheral countries, and the third is to create an articulated world market (Kaygusuz, 2007: 147).

3.1.2. Liberal View of Security

The concept of security has been handled as a state-related and military-oriented phenomenon in traditional approaches. This classical perception of the concept changed towards the end of the Cold War, and the view that security should be examined in a broader perspective and should not be reduced only to the state and military dimensions began to spread (Best, 2017:377). In this context, it has begun to be widely accepted that security has other dimensions such as economic, environmental and social.

In the field of international relations, the concept of security has a different meaning than its daily meaning. Security in the international arena is based on power politics. In the classical military-oriented security understanding, the survival of the state and the vital threat to this situation are the main issues. In this understanding, measures such as the use of force to eliminate the threat are legitimate. Throughout history, states have prioritized the issue of providing security and prioritized the concept of power as a reason for the protection of the state (Tjalve & Williams, 2015: 47).

Liberalism represents the tradition of political thought that encompasses specific goals and ideals. Liberalism was influential in the history of political and economic thought in the 18th and 19th centuries, especially in Britain and the USA. Classical liberalism is built on concepts such as equality, freedom, and property. Liberalism constitutes the basic philosophies of enlightenment theorists (Browning & McDonald, 2013:241).

According to John Locke (1997:124), the basic principles of liberalism can be listed under four parts. The first is the equality of opportunity principle, which does not involve equal distribution of resources. The second principle is that individuals meet their needs in the most reasonable way conceivable and have the right to demand. In liberalism, the individual has the ability to comprehend physical and social realities. Therefore, people should be given the right to seek their happiness. The third principle is basically the handling of the individual and the emancipation of the individual. The best society is one that gives individuals more freedom. The fourth principle is private property, where individuals can achieve their private goals and realize their happiness.

Hugo Grotius (2012:158) argued that it is in the nature of man to live in an orderly and peaceful society. Also, according to Grotius, war is part of the natural state of international relations. He defends the view that the right mind justifies war by accepting the protection of himself as the basic principle. One of the theorists of liberalism, Charles-Louis de Montesquieu established a direct relationship between war and administration. He argued that there was a relationship between monarchies and war, arguing that authoritarian governments were more prone to war. Therefore, he saw democratic regimes as a factor that ensured peace (Arı, 2013: 294) also contributed to liberalism by defending the rational individual and “laissez-faire”. What matters in liberalism is to find a balance between security and freedom. In this direction, the aim of the state in liberalism is to create a safe environment inside and outside without harming individual freedoms. In liberalism, the raison d'être of the state is the problem of providing security. In order to ensure the security of individuals inside and outside, states can restrict freedoms to a certain extent. In this context, it is necessary to establish a security mechanism to be operated by states (Beriş, 2010: 93). From the beginning of the Cold War period until the end of the 1960’s, liberalism remained under the shadow of realism. After the bipolar system entered the softening process, non-state actors started to come to the fore. According to liberalism, which has a cooperation-oriented security approach, actors prefer to cooperate in line with the assumption of absolute profit. According to liberalism, which claims that wars are not caused by the anarchic structure of the international system, conflicts are caused by misperceptions. Liberalism suggests that collective security can be achieved as a result of the establishment of international law rules.

Issues related to social and environmental science have also started to be on the agenda as important vital areas in liberalism. With the increase of important issues, it has become impossible to create a hierarchy between the agendas. With the loss of military-oriented security understanding, the use of military force has also decreased. The possibility of using this power has decreased among the states that are in mutual dependence (Pirinççi, 2010: 25). According to Kant, with the support of liberal institutions, an environment of conflict and competition will not occur. The more countries around the world the democratic regime is adopted, the safer the environment will be (Arı, 2013:293).

3.1.3 Marxist View of Security

The Marxist approach displays an approach in the dimension of criticism of security rather than a conceptualization of the construction of security. Marxism was born at a time when workers were employed under severe conditions in a period of heavy capitalism after the Industrial Revolution. Karl Marx claimed that capitalism creates inequality and injustice in society and put forward a critical point of view. For this reason, it is known that the basic concepts in Marxist theory are social equality and justice. The development of class consciousness in society has been put forward as a solution to injustice. (Bagby, 2002: 172). In terms of security, Marx states that the class that owns the means of production prioritizes protecting its interests. As a result, it is the case that the ruling class reflects its attitudes towards its own interests as an overall security problem. In this case, the state has important duties. The state will consider situations that pose a threat to security as a security threat to the society, and the security policies of the state will become protective. However, in the Marxist ideology, it is also stated that the state is only an instrument that dominates power and assumes the role of patronage of the dominant class (Birdişli, 2011: 164).

The fact that the realist approach puts military power above everything and regards the state as the main and even the only actor in international affairs has been criticized economically and from a Marxist perspective. In the historical conditions in which Marxist theory emerged, Marx and his followers saw capitalism as a global system. For this reason, Marxism refuses to make a radical distinction between national boundaries and international affairs, and tries to analyze the dynamics of capitalism through the interplay and mutual interaction between the two, and with a political economy approach. It is possible to say that Marxism stands against the tendencies of excessive specialization and exclusion from each other (Uğurlu, 2014 : 89). The theories of Karl Marx and his successors have undoubtedly failed to focus on the system, its problems, conflicts, or possible future, which today are called international. The concentration of Realist and Liberal theory on states as the main actors of international politics contradicted Marxism's understanding of the relations of production and the class wars arising from these relations as the main carriers of history (Canbolat, 2006: 77-78). In both Realism and Liberalism, it has become essential to analyze the power and interest relations of the states that ground them at different points. Security preferred in Marxism was to focus not on the interests of states, but on the capitalist class that guided states according to their interests.

3.1.4. Constructivist View of Security

The main purpose of Constructivism, which entered the literature with Aleksandr Wendt and known as "Social Constructivism", is seen as bringing together Realism and Idealism (Wendt, 1999: 83-88). According to the constructivist theorists, the concept of identity has an important place when dealing with the concept of security. According to Alexander Wendt, one of the pioneers of constructivism, in this complex atmosphere molded by the ethnic, religious and cultural conflicts of the 1990s, traditional international relations theories failed to explain the unexpected and great change in the system (Wendt, 1995:72). This has led to a rapid increase in the number of researchers trying to make sense of the world through the ideas adopted by critical theories. Postmodernists, constructivists, neo-Marxists and feminists in critical theory have come to the stage claiming to fill this gap created by traditional theories in the discipline of International Affairs and have tried to offer a better method to explain what is happening in the world.

Constructivists differ from Neo-Realists in that they see the structure of the international system as a phenomenon that interacts with nation-states and is changeable. In this context, they argue that anarchy is formed as a result of the behavior of states and that anarchy is not a constant (Bruner, 1987:17-24). In the constructivist approach, the understanding of "national security", "national interest" or only the security shaped by military power, which was envisaged by the Realist approach, has been abandoned. In addition to accepting that security has a military infrastructure, it is argued that intellectual factors such as norms and values form the basis of these. According to the theory, security issues are constructed as security threats through word-acts. In this way, it becomes legitimate to resort to extraordinary means against the security threats that have been built. Power holders can choose to justify the sanctions they will impose by presenting the issues they want to take extraordinary measures as security threats (Bozdağlıoğlu, 2007: 149-150).

3.1.5. Copenhagen School and Security

The Copenhagen School has made three major contributions to international security studies academic literature: securitization theory, sectoral security approach and regional security complex theory. According to the Copenhagen School's approach, security is seen as a word-act. Moreover, issues can be presented as security problems through word-acts, and this is called securitization (Browning & McDonald, 2013:241). According to this theory, simply calling an issue security makes it a security problem. Other than that, the School is not concerned with whether the subject specified is a real threat. Because, from a constructivist point of view, it defines security as an intersubjective construction. The Copenhagen School's starting point is the idea of focusing heavily on the non-military aspect of European security. In this regard, the school was not content with defining and perceiving security as military security and expanded the concept by defining different security sectors other than military security (Stritzel, 2014:22). While this understanding challenges the military sector's monopoly over security efforts, it does not ignore the importance of the military sector. In examining each sector, the Copenhagen School examines different types of interactions:

Sector	Referent object
Military	State or other political entities
Political	Sovereignty
Economic	Firms
Societal	Collective Identities (Nations and Religions)
Environmental	Very broad (ranging from Human species to the rest of the biosphere)

Figure 2 1. Resources: ISD, 2008

Military sector force based relations; political sector authority, management status and recognition relations; economic sector trade, production, finance relations; social sector collective identity relations; the environmental sector is related to human activities and the biosphere of the planet. The military sector is concerned with the interplay of offensive and defensive capacities and states' perceptions of each other's intentions. In this regard, the main actor and object of reference in the military sector is still the state (Hama, 2017:3). Similarly, state sovereignty is the object of reference in the political sector. But differently, non-military threats gain importance here. Moreover, political organizations other than the state can also be a reference object in this sector. Although the political and military sectors are concerned with national security, they do not focus on the identity of nations. The social sector, on the other hand, deals with collective identity issues. The economic sector, on the other hand, focuses almost entirely on issues such as access to resources, finance and the market, which are necessary for the state to reach an acceptable level of prosperity and power. This sector is rich in reference objects, abstract systems such as states, classes, individuals and the global economy can be treated as reference objects (Oels, 2012: 191). Finally, the environmental sector focuses on the relationship between human activity and the biosphere. In its simplest form, the reference object of the environmental sector is the environment itself. With the securitization action, an issue is already shown as a threat, so it takes absolute priority over other issues. If this issue cannot be resolved, there is a perception that no other issue will matter. Thus, the relevant actors gain the legitimacy to solve this issue by using extraordinary means or by taking measures. Being aware of this situation, the actors who make the securitization label the subjects they want to use extraordinary measures as a security problem. Using the term 'security', the securitizer states that the issue is an emergency and thus demands to use all necessary measures to solve this issue, which it presents as a security threat (Watson, 2012: 279). In the act of securitization, it labels a securitizing issue as a security threat already and demands extraordinary measures to deal with this problem. However, academic analysis of securitization is not or does not necessarily investigate whether this issue is a real security problem that requires extraordinary measures. The analysis of securitization is about investigating and revealing the process of constructing a subject as a security problem and thus constructing it.

3.2. Cyber Security and Related Concepts

Cyber attacks, which have increased rapidly in recent years, have now turned into serious economic losses and loss of reputation. In September 2018, with a cyber attack on the Facebook database, hackers had access to the personal information of 30 million users (Terlizzi et al., 2017:228). The Facebook example reveals the cyber security problem in the digital world. These attacks, which were made in the past without any target, have been carried out in a targeted manner in recent times. Although countries and companies have increased their cyber security measures in order to prevent these attacks, these attack methods, the efficiency of which can only be measured at the time of the attack, pose an extremely high risk.

Cyber security terms and concept:

Cyber Asset: It is possible to include all of these devices and software and hardware components in the definition of "cyber asset", from classical computing elements (computers, servers, network devices, etc.) to components that automatically notify the service of the malfunction in the vehicles, from the television with internet connection (Von Solms & Van Niekerk, 2013:99).

a. Physical Cyber Assets:

When it comes to physical cyber assets, it should be understood the entities that are a physical mass of ICT, that must be protected by physical security measures, that are likely to be affected by environmental factors, can be physically transported, and can be exposed to physical effects (moisture, fire, power outage, theft). (Information: ICT stands for Information Communication Technologies)

b. Logical Cyber Assets:

In addition to all kinds of software and applications, they are assets that are formed from the occurrence of these assets.

Cyber Incident: An event in which physical or logical cyber entities are stakeholders in various ways. It refers to the violation or attempted violation of the confidentiality, integrity or accessibility of the information and industrial control systems or the information or any data processed by these systems (Terlizzi et al., 2017:229).

Cyber Space: Digital environment consisting of information systems spread all over the world and space and networks that connect them or independent information systems. (2016-2019 National Cyber Security Strategy)

Cyber Warfare: Attacks against the specified targets using computer and information technologies and IT-based attacks that affect national security (Bashir et. Al., 2017:153).

Cyber Weapon: All malicious software that has the ability to attack (Collins & McCombie, 2012:82).

Cyber Terrorism: Terrorist acts carried out in cyberspace using cyber assets (Kenney, 2015: 113).

Cyber Crime: If any crime finds the opportunity to be committed in a cyber environment and the act performed in this environment can be defined as unlawful, this is considered as a cyber crime. Cyber crimes are classified in three groups as "cyber crimes committed against the state and public order", "cyber crimes against property" and "cyber crimes committed against individuals" (Collins & McCombie, 2012:82).

Cyber Defense: It can be defined as the set of measures to be taken to protect vehicles, equipment, systems and infrastructures working on cyber defense information systems against cyber threats and attacks (Collins & McCombie, 2012:81)

Cyber security is also to determine the security risks and vulnerabilities in cyber space and to take necessary security analyzes and measures in order to protect the assets of institutions, organizations and users from unwanted threats and dangers. (Bada et al., 2019: 2) Cyber security covers the processes of protecting information and communication technologies that make up cyber space from cyber attacks, ensuring integrity and accessibility, detecting attacks and cyber security incidents, operating response mechanisms against these detections, and then returning the systems to their previous state. Basic principles of cyber security: Confidentiality, accessibility and integrity concepts are also referred to as the "CIA trio" (Simon, 2017).

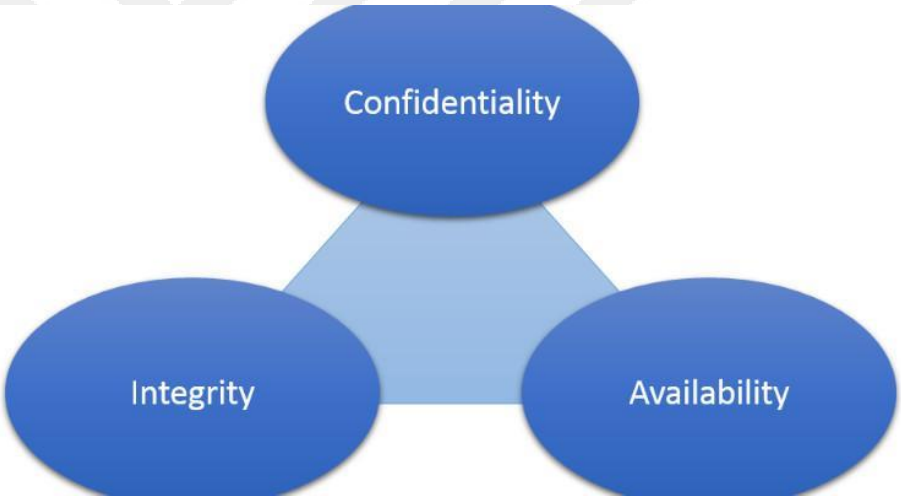

Figure 2 2 CIA Trio

1. Confidentiality: It is the protection of the confidentiality of information, preventing unauthorized access to information. It refers to the special protection of data (Singer & Friedman, 2015: 57). In other words, the message can only be seen by the sender and the recipient.

2. Accessibility: Protection of the speed and quality of access to information, uninterrupted access to data or resources, or prevention of access losses (Simon, 2017).

3. Integrity: It is the prevention of unauthorized alteration of data or resources in the system and ensuring their integrity. It is the fact that factors such as the accuracy, consistency, content, and order of the data as it moves from the source to the target can only be made by authorized persons (Newman, 2000:4).

In addition to the three basic principles of cyber security, there are additional security principles such as accountability, undeniability, identity verification, reliability, record keeping, access control, security and flexibility, which are important for information security. Accountability is the traceability of all actions to the user, the person performing the action. The rapid development of technology in the information age we are in, and the blurring of the physical borders of the countries, have revealed the threat of cyber-attack. This has added a new one to the security concerns of the states and caused them to change their classical security understanding. Countries' perspectives on cyber attacks and threats vary widely. Some countries use cyberspace little or not at all, while others use it too often for their own benefit. Countries that use cyber activities frequently are more technologically advanced and generally do not lean towards a global cyber security concept as they benefit from these activities (Hathaway et al., 2012:824).

3.2.1. Cyber Concept

As can be seen from the definitions given above and the figure presented, the scope of cyber security and defense is wide. When the threats to cyber assets are examined, the importance of this issue will be understood better. In the figurative sense of cyber assets and concepts, the importance and value of digital soils is also high. We have to protect our digital lands with the same precision as we protect our lands. The importance of cyber security and defense is summarized in the articles given below (Hu et. Al., 2016:449-452) ;

- Personal, institutional or national information assets are the most important values of countries. It is essential for the protection of the information assets of societies, institutions or organizations and nations as well as personally important. Although there are many legal and humanitarian reasons for this, its institutional and national importance is also high. Giving the necessary importance to the cyber security of both the public and the private sector is to give importance to the future of the country.

- In countries where efforts to become an information society are increasing rapidly, personnel, institutions and organizations at all levels using information technology have to know and apply the concept of information security. This is important and necessary to protect our property, reputation, health, dignity and perhaps our lives. If this is not taken into consideration, serious problems such as damage to corporate or personal images, shaking of trust in institutions or individuals, loss of workforce and time, high costs of restoring the system, loss of information or data, and sometimes not being able to recover the lost ones will cause serious problems.
- Ensuring the confidentiality, integrity and accessibility of cyber data is a must to both increase competitiveness and protect and maintain the commercial image.
- Cyber environments are environments where different data, environments, systems, documents and information, processes, standards, policies and most importantly critical structures are located. The size, scope and diversity of data in these environments are increasing and obtaining value from these data is becoming widespread. However, data protection is also necessary, as the violation, abuse and exploitation of these data increases.
- To protect existing assets, it is necessary to counter threats and dangers from a wide variety of sources, such as fraud, espionage, sabotage, destructiveness, fire and flood. Resisting viruses, spyware and malware, cyber attacks, hackers, and service attacks is now important for every user as well as for organizations. It is also important to provide cyber security in terms of eliminating these dangers.
- Data protection now has legal consequences. The implementation of laws and regulations is important and a must for the fulfillment of legal obligations.
- Protecting existing cyber assets, providing a high level of security, minimizing losses, minimizing risks, developing new technologies, producing new information, transforming opportunities into investments are important for establishing a healthy cyber security ecosystem and economy.

- Dependence on information systems and services means businesses are more vulnerable to security threats (Chou, 2013: 79). The interconnection of public and private networks and the sharing of information resources increase the difficulties in establishing access control. In addition, new technologies, infrastructures, algorithms used, applications and services are constantly changing and developing, bringing with it new attacks. It is necessary to eliminate the threats and dangers that may occur due to these.
- Considering that new approaches, technologies, perspectives and applications such as Artificial Intelligence, Internet of Things, Big Data, Deep Learning, Quantum Computing rapidly increase, new threats and dangers will occur, and there is a greater need for cyber security and defense.

It is worth noting that security begins with the activation of an institution or organization and continues throughout the time it survives. The healthy execution of this continuity depends on the careful monitoring of the growth or contraction of the institution or organization by the users or the responsible persons, and the timely taking of the necessary steps. In today's competitive conditions, they have to attach great importance to cyber security in order to protect people, institutions and even their countries that will provide benefits, profits, economic advantage and competitiveness (Carr, 2016:44). In cyber environments, there are communication systems, natural gas control and transmission systems, air traffic control centers, computer and communication systems, similar critical infrastructures and networks, critical software and many similar applications and systems. As attacks on these environments may cause disruption of national services, confusion, confusion or chaos, ensuring cyber security is a must.

3.2.2. Cyber Security Elements

Ensuring a high level of cyber security depends on factors such as confidentiality, integrity, authentication, accessibility and non-denial to pay attention.

Confidentiality is to ensure that data can only be accessed by authorized persons (Yeboah-Boateng, 2013: 29). In other words, they are attempts to prevent data from being obtained by unauthorized persons.

Authentication can be defined as the authentication of authorized users or the determination or authentication of the user (Liu et al., 2020:4566).

Integrity is another element of cyber security. It can be defined as ensuring the accuracy of data and processing methods, ensuring the immutability of the content, or verifying that data is sent from one medium to another unchanged (Reed & Gonzalez, 2012: 1).

Accessibility; It is an attempt to ensure that authorized users have the right to access information and related resources, to ensure that authorized users have safe and continuous access to systems, or to take the necessary measures to ensure continuity of service (Simon, 2017).

Accessibility is defined as an attempt to take the necessary measures to ensure that the authorized users have the right to access information and related resources, to ensure that the authorized users have access to the systems continuously, or to ensure the continuity of the service (Ismailova, 2017: 259).

Inability to deny; In fact, as the name suggests, the message or information source cannot deny the message or message sent. In other words, it is to prove the message sending or receiving transactions of the authorized user or to ensure that the sending or receiving transaction cannot be denied.

In order to resist cyber attacks, it is necessary to intervene in cyber incidents within a certain system, and to take these steps by following certain steps.

For a high level of protection; It is necessary to follow cyber environments, cyber assets, attacks, attackers, attack tools, attack techniques, techniques and technologies to prevent attacks, develop solutions, follow current standards, apply and control them.

3.2.3. Resisting Cyber Attacks

Actions that endanger the cyber environment, damage it or drag it into an unknown situation are perceived as a threat. Identifying threats that may occur in the cyber environment is important in order to determine the measures that can be taken against these threats. Threats can occur as a result of harmful or deliberate acts, or sometimes can be caused by an event committed by people unknowingly (Thomas, 2018:7). For example, the wrong configuration of the permissions given during the creation of a new user in the system is an unwanted action, but it can create unwanted effects on the cyber environment. The science of encryption, which is as old as human history, and the history of encryption that sheds light on today, contain many issues that should be taken as a lesson for societies who want to reach the level of contemporary civilization. The security of the environments where data, knowledge and self-knowledge are hosted and transmitted, all societies that want to develop and progress must constantly stand on, follow innovations and develop their own methods.

To understand the importance of the security of cyber environment and systems and to ensure their security one should(Kadivar, 2014:5);

- understand the extent and scope of threats, attacks, vulnerabilities, technologies and solutions,

- grasp the terminologies used,

- know and follow current techniques and technologies closely,

- know and apply standards,

- establish and monitor policies and

- It is necessary to take it seriously to minimize the risks that may be encountered in cyber security and defense.

Paying attention to these issues will reduce the percentage of threats and hazards that may be encountered. It is useful to remind here that these issues are necessary but not sufficient for complete security. The threats that cyber security deals with can be examined under five headings: Hacktivism, Cyber Crime, Cyber Sabotage, Cyber Terrorism, Cyber Warfare.

Each threat type has a motivation, actors, and goals (Andress & Winterfeld, 2013: 70-81; Bashir et. Al., 2017:153);

In Cybercrime, cybercriminals use computer technology to capture personal information, learn trade secrets or conduct malicious internet research.

Cyber Terrorism: It is an attack that is supported and based on a political infrastructure, against computer systems, computer programs, important data, and results in the damage of the other party who is bystander in the event.

Cyber Sabotage: Hackers use computer networks to obtain confidential information by unauthorized access to servers maintained by a country or organization. The counterpart of real-world agents in cyberspace has been hackers with this definition.

Cyber Warfare is a digital attack organized by another country in order to disrupt public services operating against a country, damage its reputation and reduce its credibility.

Hacktivism is the misuse of a computer system or network for a social or politically motivated cause. Hacktivism draws the general attention to the subject that the person who carried out the movement and called the hacktivist is trying to impose. Although they are mostly made up of individuals, there are also some coordinated hacktivist groups (Anonymous, LulzSec etc.).

Today, the concept of information security, which has a wide range of effects from personal losses to international disputes, has attracted attention to cyber security policies as well as concerns. However, it is seen that academic and industrial studies on information security concentrate on application and technological solutions. The increase in the tendency of the attackers to open the doors over the less costly people instead of spending effort and time to overcome the technological measures, which is the starting point of information security and in recent years, has once again demonstrated the importance of the concept of awareness (Von Solms & Van Niekerk, 2013:98). In parallel with the increase and diversity of attacks and threats, security measures are also increasing, access to systems is carried out by teamwork and processes for solving complex information compared to the past. Difficult access to the system requires the attackers to follow a systematic method. Understanding threats is only possible by understanding the methods and steps used when carrying out cyber attacks. The first two steps of the cyber attack lifecycle are information gathering and discovery, which are often intertwined. Attackers use server scanning and port scanning methods to infiltrate systems. Some measures can be taken to minimize the margin of error by training and improving the skills of people, who are the weakest link of the system against cyber attacks at personal, institutional and national levels (Kostyuk & Zhukov, 2019: 318).

3.3. Cyber Security Policy in Turkey

The main factor that makes Cyber Security one of the most discussed issues today is the increasing usage rate of people, namely the careless and weak link in the technological chain, in the information and communication technologies sector. Before computers and the Internet became an indispensable part of people, threats in the cyber field and their solutions were mostly carried out by experts in their field. In other words, the people who attacked and defended this attack were well-equipped and qualified people in this field. But in line with today's technological progress and people's interest in it, the size of the cyber threat is increasing day by day. The emergence of cyberspace has brought many security risks for both users and security institutions of nation states. It is now possible to reach national secrets by targeting those who use cyber space, targeting financial institutions. It is very difficult to determine who carried out cyberattacks, because attackers rarely leave behind traces and even try to hide their own positions. Despite these difficulties, nation states are compelled to deal with cyber threats with their own resources (Karabacak et al., 2016:526). Therefore, the first indicator of how open nations are to cyber threats is the country's own capabilities and cyber security perception. This section examines the developments in cyber security policies and legislation in Turkey. Cyber attacks against a country's assets do not have to originate within the country's own borders. However, Turkey constitutes an interesting case because in 2013, only 46 percent of Turkish citizens had internet access. Turkey was the third major origin of cyber attacks in the world (Göztepe et al., 2014:3).

Before they became national security issues, cyber attacks were mainly issues of public order and law enforcement. So before armies began to take interest in cyberspace as a new battlefield after land, air, sea and space, nation states first focused on using cyberspace to commit illegal crimes. This trend has also been observed in Turkey. With the Turkish Penal Code numbered 5237, which entered into force in September 2004, the definition was expanded and the concept of cybercrime was added to the criminal law. In other counts of the law related to this subject, crimes against personal life, illegal blocking of communication, theft, corruption, gambling, forgery and counterfeiting, committed by using computer systems such as computers and communication devices, are included. In parallel with these developments, steps have been taken to establish institutions responsible for the execution of policies in the cyber field in the country (Akbulut, 2017:155). As might be expected, the establishment of dedicated institutions has accelerated the country's policy-making efforts, enriched its legislation on the Internet, and enhanced the country's capabilities. Generally, these institutions focused on the order and legal aspects of cyber security and left the cyber warfare dimension to the Turkish army. Research institutions have constituted the main exception to this. These institutions work in the development of reliable local software and hardware in all aspects of the cyber security architecture of Turkey, and therefore continue to operate in a close relationship with the military.

A report published by the Information and Communication Technologies Authority (BTK in Turkish) in May 2009 stated that the country should take certain steps to strengthen its cyber security legislation (Bıçakçı et. Al., 2015:12). Among them; There is a need for regulations on how to investigate cyber-attacks, regulating how to collect evidence, and clarify the powers of the security forces and the judiciary in the cyber field with the governments and the procedures on this issue. After the Cyber Security Strategy Workshop held in June 2012, a recommendation document was published by the Information Security Association (TR Ministry of Transport, 2012);

· Publication of the National Cyber Security Strategy Document.

· Establishing a National Cyber Security Council.

· Raising awareness in the field of cyber security and spreading the culture of cyber security.

· Stricter measures to be taken to protect personal and corporate data.

· Strengthening international cooperation (the document lists EU, ENISA, Council of Europe, UN, NATO and OSCE).

· Establishing a national cyber security R&D policy and encouraging the development of national technologies.

· Taking steps to increase the scientific studies conducted on the subject in universities.

· Taking steps to improve the cyber security capabilities of institutions and security units.

· Establishing independent centers to conduct cyber security penetration tests for institutions.

The ambiguity of cyber space also affects security concepts. Concepts such as cyber espionage, cyber espionage and cyber intelligence are often used interchangeably because of their similar meanings. In fact, they all depend on similar attack methods and similar technologies. However, finding out whether the perpetrator of the cyberattack is a state or an organization is a difficult matter. States exploit the uncertainty or ownership of cyberspace for their own benefit. The most basic feature of cyber intelligence is to collect information with various cyber tools in order to respond to cyber security threats. The National Intelligence Organization (Milli İstihbarat Teşkilatı in Turkish) is one of the units responsible for collecting the necessary intelligence to prevent cyber security threats in Turkey before they happen. In this context, the policy is to record, analyze and collect information, documents, news and data by using all kinds of technical intelligence and human, procedures, tools and systems in foreign intelligence, national defense, counter-terrorism, international crimes and cyber security issues to deliver (Hekim & Başıbüyük, 2013:137-140).

At the end of 2013, Turkey was shaken by a corruption scandal that emerged with leaked tapes and phone calls. In the following months, many voice recordings were published, including recordings from a highly sensitive and high-level meeting held at the Ministry of Foreign Affairs, and the investigations investigating the origin of these recordings reached important institutions in early 2014. Following this, the Cyber Security Council was tasked with the approval of policies, strategies and action plans on cyber security. The Cyber Security Council takes the necessary decisions for the effective implementation of these policies, strategies and action plans throughout the country, makes the final decision on the recommendations on determining critical infrastructures, determines the institutions and organizations that will be exempt from some or all of the regulations on cyber security and other duties determined by the law has been held responsible for fulfilling it. Although Turkey has improved its presence and capabilities in cyberspace over time, this has not been at the same level in all areas. As a result, although great progress has been made in some areas, the expected progress has not been achieved in other areas (Ünver, 2017:124). Nevertheless, the number of government agencies dealing with cybersecurity has increased in the last few years, and Turkish security forces have placed additional emphasis on combating cyber threats. In addition, the politicization of some issues has been a factor that makes it difficult for Turkey to develop its capabilities in cyberspace; The failure to enact important draft laws is an example of this. As a result, Turkey continues to lag behind its major allies and even hostile states in terms of its preparations in the field of cyber security. In this context, the possibility that rival states support such structures or organize direct hostile cyber attacks by hiding their identities further complicates Turkey's threat outlook.

Cyber security is defined as a set of tools, policies, security concepts, risk management approaches, activities, training, applications and technologies used by institutions and organizations in the cyber environment to sustain individual users' existence. (Ünver et al., 2011) The main objectives in this matter are to ensure accessibility, integrity and confidentiality in information matters. If we are to group the attackers in general, first of all, hackers (Black, White, Gray) who have high level of knowledge and skills in the field of information technologies serving personal interests or criminal organizations, and are separated according to their hat colors in terms of their actions; secondly, other groups that want to publicize their political and social propaganda, protect public interests rather than personal interests, and oppose censorship; thirdly, it would be correct to indicate as state-supported groups working on an international scale.

SGE (Cyber Security Institute), which has been operating within the body of BİLGEM (Information and Information Security Advanced Technologies Research Center) since 2012, contributes to the formation of the necessary knowledge in the field of cyber security (Bıçakçı et. Al., 2015:12).

In order to be suitable for digital transformation and to produce the necessary policies in the field of cyber security, the cyber security strategy was published for the first time in Turkey in 2012, and the second plan was shared with the public four years later. With the Electronic Communications Law, new regulations such as security against unauthorized access and observance of communication confidentiality were introduced in the field of cyber security. The necessary statistical data were collected with the 1st National Cyber Security Exercise, organized under the coordination of TÜBİTAK BİLGEM and the Information Technologies and Communication Institution, and the exercise held with the participation of public, private and non-governmental organizations. In addition, the International Cyber Security Federation, which was established to increase cyber security awareness in the public and to create a system based on advanced technology, also operates in the field of cyber security (Hekim & Başıbüyük, 2013:137-142). The Informatics Association of Turkey, established in 1971 as the world's first association in the field of informatics, is the largest and well-established non-governmental organization in the informatics sector of Turkey. In addition, efforts to establish a Cyber Security Academy continue in order to have well-equipped human resources. As a result, the idea of creating a Cyber Security Law was put forward (Bozdağlıoğlu, 2007: 149-150). One of the leading works in the military field is the Cyber Defense Command, which was established under the General Staff. This command works to make the cyber security of other commanders in the General Staff effective and has achieved significant success in international exercises. It has become inevitable that the critical point in terms of intelligence activities is cyber threat intelligence. Behind this situation lies the fact that almost millions of cyber attacks occur daily. In order to manage this crisis, there is the "Signal and Electronic and Technical Intelligence" department established within the National Intelligence Organization of Turkey. When the cyber security studies in Turkey are examined, it is seen that the cyber studies do not show enough development and the planned policies cannot be implemented exactly (Senol & Karacuha, 2020:3). When we examine the problems, the problems generally encountered are legal gaps, legislative deficiencies, uncertainty of power of law enforcement and judicial authorities, and lack of technical expertise.

3.4. Cyber Security Policy in the USA

The globalization process, which has been accelerating in recent years, has started to reduce the importance of the borders of countries in terms of national security policy. In this section, cyber security policies of the USA, official policy documents and related literature are examined. The national security policy refers to a plan based on the use of all military and civilian resources and tools of a nation in a collective and coordinated manner in order to "carry out defense tasks" and "protect national interests" (Szabo, 2019:503). Every country has a national security policy, either implicitly or explicitly. While open security policies are read from documents and plans, covert policies can be predicted by reading the steps taken by countries regarding their security over time and predicting the direction of the moves. Handling national security as a comprehensive public policy is a requirement of the "national security perception" that is quite changing today. State administrations, especially after the World Wars, consider national security only as military attacks against the country and military-political strategies to be taken against these attacks is a wrong attitude today. Approaching the issue of cyber security from a national perspective, Cavelty (2014: 703) argues that cyber security vulnerabilities are increasing day by day and in line with this, personal and national cyber security is decreasing. While states will take steps to set more centralized and strict rules to protect critical infrastructures and reduce security gaps by increasing cyber security, individuals want to preserve their freedom of movement in cyberspace for their own freedom. For America, the freedom offered to individuals and companies (especially software companies) in cyberspace also brings along expanding security gaps in terms of national cyber security. As a solution to this dilemma, the cyber security policy, which includes broad definitions and interdependent variables, will be established on the basis of a consensus by determining individual and national security priorities is considered (Bashir et. Al., 2017:153). Cyber attacks, disruption of economic growth, terrorism, epidemics, internal riots, migration and new threats to and from globalization are also within the scope of national security. In this context, national security is not only a policy focused on military strategies, but also policies that protect public order and public interest.

The United States of America (USA) is one of the most important cyber powers that dominate cyberspace today, with the contribution of its economic and technological superiority. On the basis of the cyber power of the USA, there are new generation derivatives of the network technologies developed as a result of the military competition with the Soviet Union during the Cold War period. In order to understand the cyber security policy of the USA, it is useful to first determine from which components and actors this policy was created. The first comprehensive document published on cyber security in the USA is the "Secure Cyberspace" document published by the White House in 2003 (WH, 2003). When this document is examined, it is seen that the term "cyber security" is mentioned only three times in the document and it is seen that the term secure cyberspace is used instead. In the document, cyber space has been described as "the space formed by hundreds of thousands of computers, servers, modems, switches, fiber optic cables that are connected to each other and provide the functioning of critical infrastructures" (WH, 2003: vii). The document contains the directives of national and federal institutions dealing with cyber security and specifies the steps that the state and local government agencies, private sector companies, non-governmental organizations and citizens will take to improve collective cyber security. According to the Secure Cyberspace document, there are five national priorities in ensuring national security. These priorities are a national cyberspace security response system, a national cyberspace security threat and vulnerability defense program, a national cyberspace security awareness and development program, government's cyberspace security, national security and international cyberspace security cooperation. The cyber security strategy document published in 2011 consists of five strategic priorities. These are the organizational development of the defense department, the acquisition of new defense contents, public-private cooperation, establishing strong relations with other countries and increasing creativity. In 2014, it made a written statement regarding the cyber security cooperation between the White House Press Office and the EU (WHOPS, 2014). This cooperation is on issues such as internet governance, internet freedom, and protection of human rights in cyberspace. The topics included in the cooperation are international cyber space developments, online promotion and protection of human rights, implementation of international law in force, development of cyber security criteria, international security issues such as behavioral norms in the cyber environment, and cyber security capacity development in third party countries. These developments and new components made a new strategy necessary. With these aspects, the strategy document published in 2015 seems to give importance to concrete steps, as underlined previously. In this regard, apart from the strategic goals specified in other documents, this document also includes practices carried out to achieve strategic goals. In line with all these investigated issues, it is observed that the USA is a leading country in developing cyber security policy. While the nationality of the cyber infrastructures it creates keeps the country's cyber dependency at a minimum, the fact that critical infrastructures are mostly dependent on cyber infrastructures weakens the cyber defense function of the country.

It cannot be predicted how much cyberspace can damage the national security areas of states. Therefore, it may not be possible to predict the risks posed by cyberspace to state security. It is estimated that some of the attacks detected so far may have caused more than one trillion dollars damage to the states annually (Kane, 2010: 5). Today, when we cannot even follow the speed of technology, the integration of technology with the internet creates a very dynamic structure. When we look at the elements of this dynamic structure, we can see that it has a complex and multidimensional content. Many elements ranging from individuals to international companies and states are included in this structure. In order to ensure the security of networks in this complex structure, states must carry their high-level security policies to the digital world and cyberspace. Because there are many scenarios about the damages that may occur in the cyber world. For governments, continuous and up-to-date work in cyberspace is important to maintain a balance. As mentioned above, a general definition for the concepts of cyberspace and cyber security is still not possible. Since the perpetrator of cyber attacks is unknown, it cannot be evaluated within the framework of international law. The fact that it is not possible to determine whether the source of cyber attacks is states or individuals is one of the main reasons why this assessment cannot be made (Gürkaynak & İren, 2011: 265). In addition, states try to make their own national software, to create content information of software and to produce local password systems in order to ensure their cyber security. The USA, which wants to manage and dominate the cyber space system, which is the main concept that constitutes globalization, has started to lay its technology foundations in this direction. After September 11, 2001, it is stated as the date when everything changed in terms of security for the USA. After this date, it has become very difficult to predict the location, time and source of threats. The risks of cyber threats are also defined in the same way. It cannot be predicted when, from where and by whom the cyber threat will come. For this reason, the security understanding of the 21st century is shaped within the framework of globalization trends due to the rapid development of technology and the internet (Sliwinski, 2014:471). The work of the USA in the field of cyber security is shaped on the basis of taking proactive measures against possible threats by establishing operational units.

SECTION 4. COMPARATIVE WORK OF UNITED STATES AND TURKEY

The globalization process, which has been accelerating in recent years, has started to reduce the importance of the borders of countries in terms of national security policy. Globalization has reshaped the power distribution channels of countries, revealed asymmetrical power relations and led to a more comprehensive and different redefinition of national security needs (Okoro et. Al., 2017: 106). When wars and internal revolts are kept aside, the factors affecting the balance of power between countries have changed as a result of globalization, and the protection of the interests of the country has become more difficult than in the pre-globalization period.

Cyber threats are no longer limited to the damage they cause to computer systems (infiltration, stealing information from systems and putting false information into systems). It emerges as an asymmetric type of warfare to the extent that it harms the communication systems, computer systems, energy and transportation networks, military command and control systems of a country that can be considered as critical. The idea that cyber threats will be one of the important threats in the coming years; It has started to be accepted by the whole world (Giri, 2019: 663). For this reason, it is very important to build more effective defense systems and to prepare emergency preparations. It has become necessary to detect attacks immediately when they occur, to build a virtual or physical barrier, and to develop regional and national cyber security policies (Herrera et. Al., 2017:2). Countries continue to develop policies and strategies for the cyber environment in order to provide a safe cyber environment, to protect the components that are part of the cyber environment against cyber attacks, to intervene in attacks, to punish the attackers, to establish the necessary legal legislation and to establish structures that will carry out all activities (Catota et. Al., 2019: :2).

It would be correct to briefly talk about hybrid wars, which is a top title before cyber attacks. Hybrid warfare has found its way into the summer for a long time. Similarly, many derivatives such as "hybrid conflict", "hybrid war", "hybrid threat" are frequently included in studies (Danyk et. Al., 2017:12). Hybrid wars are a combination of symmetrical and asymmetrical warfare in which friendly forces conduct traditional military operations against enemy forces to maintain stable control. Therefore, hybrid wars are fully equipped wars with both physical and conceptual dimensions. Accordingly, different from other wars in hybrid wars, success is required in many areas with different tactics. In this different type of war it will not be easy to defeat any other enemy.

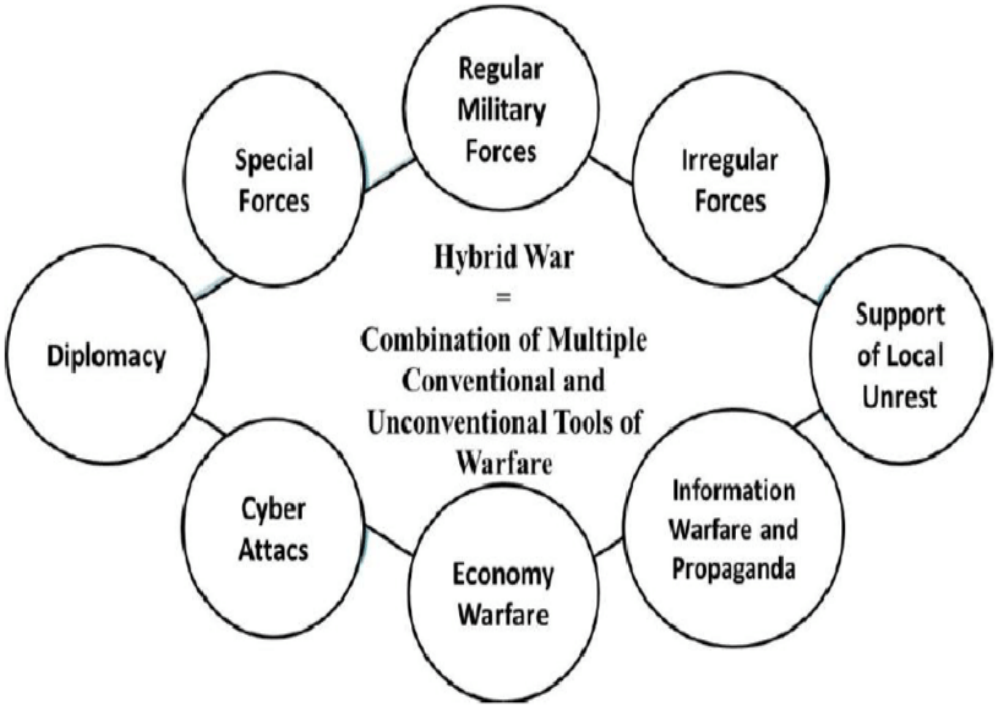

Figure 3.1 Hybrid War

Resource: Pikner, 2016

Cyber attacks are also part of hybrid warfare today. In this balance change, "cyber security" has come to the fore as a new and very critical element of the national security policy. In this study, the cyber attacks on the USA and Turkey and the actions taken were explained and the actions taken by the two countries were compared.

4.1. Cyber Security As A Critical Part Of The Us ' National Security Policy

Today, it is known that computers, which have become an indispensable element in personal and corporate understanding, were first developed for communication, encryption and decryption, and then their use gradually increased. The Internet emerged with the ARPANET, which was established in the 1960s by the US Ministry of Defense to transfer data from computers to other computers in order to continue to use military communication without damage in case of a possible war (Crocker, 2019:17). The use of the Internet has become widespread all over the world due to the fact that it provides communication, information exchange and also the connection between computer users. The use of information only by persons authorized to access it is its privacy. This access is such as reading written information or viewing the information stored in information systems only by authorized persons. Only the authorities should be aware of the existence of sensitive information. The integrity of the information is that the information has not been changed, partially or completely deleted. Accessibility means that the stored information can be accessed by authorized persons when necessary.

The USA, one of the two great actors of the Cold War and defined as a superpower in the world, chooses some universities to base the information systems in the public and private sectors and creates various R&D institutes. (Moretti et. Al., 2019:3). Since the beginning of the 20th century, with technological developments, the USA has gained a rapid acceleration in becoming a strong actor in cyberspace. While the Internet was used only in the military platform before the 1990s, it started to become civil after the 1990s. With the demilitarization of the Internet, new regulations were made in cyber security strategies in this period. In these periods when the internet was used by individuals, it was more important to ensure the cyber security of the individual and the society. With the rapid connectivity of virtual social networks to each other, the concept of globalization is increasing. Since cyberspace is not a concrete concept, concrete security measures cannot be taken in this area. Cyberspace, which has a complex structure, will continue to constantly generate new threats. The concept defined by the USA as security in cyberspace can be explained within the following objectives; Providing security by establishing systems aimed at resisting attacks from hostile states, creating intelligence or providing counter-intelligence (Maschmeyer, 2021: 1-11).

4.1.1. Cyber Attacks Targeting the United States

In general, cyber attacks occur in two ways. It is accepted as the first method that a virus focus remotely placed on the computer deletes the data in all memory. The second is the methods that aim to make the system and networks unusable or insecure by the virus that enters the computer in a way that may be relatively less harmful (Lin, 2010: 63). The purpose of cyber attacks is often uncertain. Creating intelligence by capturing personal or corporate information can occur with motivations such as an apolitical attack without a cause, or the control and management of computers and technological items connected to the Internet. Cyber threats vary in terms of methods and how they are made. In the event of a possible cyber attack, the measures to be taken by the states carry a complex structure. Below, some cyber attacks against the USA or allegedly committed by the USA are examined below.

Attack on the US Military Computer (1990)

The hacker named Mc Kinnon was arrested for allegedly attacking US military systems. McKinnon worked with a group in the 1990s on cyber-attacks and, considering that the USA kept some information about aliens from the world public, planned an attack that would last for twelve years. In 2001-2002, with the emergence of this attack, the USA suffered losses of approximately $ 800,000 (BBC News, 2012).

Gulf War (1993)

After the collapse of the Soviet Union, one of the most important events in the Middle East is the Iraq War, also known as the 1st Gulf War. The Iraq War also contains important features of the Hybrid War. This war is an example of the USA's cyber attacks on other countries. These are the wars that the USA has started against Iraq at two different times. The first consists of attacks using smart weapons and advanced computer technology in 1993 (de Miranda Rios et al., 2021:186). In the second attack in 2003, the USA notified the Iraqi commanders by email that it would invade Iraq and sent a call to surrender without fighting. It is claimed that many Iraqi soldiers also responded positively to this call (Al tae et al., 2020:469-471) Since the Gulf Wars can be followed live on television and the internet, it is defined as a communication war (Bıçakçı, 2012:12). These are the wars that the USA has started against Iraq at two different times. The first consists of attacks using smart weapons and advanced computer technology in 1993. In the second attack in 2003, the USA notified the Iraqi commanders by email that it would invade Iraq and sent a call to surrender without fighting. It is claimed that many Iraqi soldiers also responded positively to this call (Al tae et al., 2020:469-471). Since the Gulf Wars can be followed live on television and the internet, it is defined as a communication war (Bıçakçı, 2012:33).

When all these issues are examined, it is revealed that the 1991 Iraq War was also an important war in terms of security studies. Accordingly, in this environment where the unipolar world system started with the collapse of the Soviet Union, the Cold War ended, many changes were experienced and the policies implemented were revised, wars are expected to differ. The combined use of air, land and sea elements in the war and the positive effect it created has revealed the importance of joint operations in today's wars. Internet and communication technologies were used actively, and in this sense, it was the first war in which these techniques were used. The live broadcast of the war deeply affected the world public opinion, with millions of people watching the operations live as if they watched a Hollywood movie. Another important issue in the Iraq War is the secretly listening to the Iraqi communication lines with technological tools during the operation and interfering with the communication from time to time. Communication of Iraq was completely captured in this way. Therefore, there is no coordination opportunity between the troops (de Miranda Rios et al., 2021:186). In this sense, the 1991 Gulf War has also gone down in history as a war in which cyber attacks took place and their effectiveness emerged. The Iraqi army, whose communication lines and air defense system were rendered dysfunctional, was defeated in a short time.

Hainan Island Incident (2001)

The Chinese plane crashed as a result of the US spy plane colliding with a Chinese plane over the South China Sea. The damaged US plane had to land on Hainan Island. Thereupon, a "self-defense operation against US aggression" was initiated by about 80,000 Chinese cyber attackers against the US government. Later, this event was described as the First Internet War (World Wide Web War I) (Vest, 2007:76). This is the "World Wide Web War 1" attack known as the first cyber war. It is the first cyber attack against the USA by a Chinese group. The collision between the US EP-3E aircraft and the Chinese Shenyang J-8 aircraft on April 1, 2001, caused this cyberattack. After the cyber attack, the official website of the White

House was closed for hours, and the official website of the Ministry of Justice was also completely locked. On many US websites, the Chinese flag was waved and Chinese anthems were stolen (Smith, 2012).

Titan Rain Attack (2003)

It is a cyberattack called Titan Rain. It is claimed that the attack was carried out by China. It is known that it was made against US military bases, defense lines and aviation companies. It is estimated that high confidential information, which is of great importance for the state, is accessed. Titan Rain is known as the most intense attack against the USA (Lewis, 2005:1-2). Titan Rain is a planned attack on American computer systems in 2003. Most attacks are Chinese based. As a result of these attacks, hackers managed to enter the computer network of important organizations such as Lockheed Martin, Sandia National Laboratories, Redstone Arsenal and NASA.

2003 Iraq War

One of the tactics used by the USA during the 2003 Iraq War was to cut off the communication of the Iraqi army by using electronic warfare and cyber warfare (Hmady & Mobarak, 2010:1-4). In this way, the Iraqi army units were deafened, and their ability to receive information from each other and convey instructions was restricted. This war is another example of the USA's cyber attacks on other countries. During the 2003 Iraq War, psychological warfare and perception management techniques were used, and important activities were carried out in this regard through the Iraqi army and the Iraqi people. Apart from these, important perception operations and psychological war activities were carried out by methods such as radio messages, sending e-mail messages to Iraqi soldiers so that they do not participate in the operations (Sheldon, 2012: 208-209). It can be stated that these activities were effective in the defeat of the Iraqi army without any significant resistance and in the overthrow of the Saddam administration in a short time.

WikiLeaks Documentation (2010)

WikiLeaks is an internet news portal organization with internet-based leaks. Assange pioneered the founding of WikiLeaks in 2006. He is a member of the WikiLeaks board of directors, consisting of nine members, and is also a press spokesperson. The meeting of the world public with WikiLeaks has been a matter of illegally obtaining confidential documents consisting of detailed correspondence between the US Department of State and US Embassies around the world and leaking them to the world public opinion through the website. The diplomatic secret correspondence of the USA, which started to be shared with the public as of 2010, is important in terms of being the most secret document leaked to the public so far (Maurer, 2011:10). With the release of these secret documents, the material and moral pressures on WikiLeaks and its most authoritative name Assange have increased. In the first place, the WikiLeaks site was constantly exposed to cyberattacks and the site had problems with its domain name and server. The publication of WikiLeaks documents revealed that the rapidly developing communication technology could be used to reveal the secret lives of individuals and states (USA), and the information revealed in this context could have serious consequences for international relations and state-society relations. It is clear that the WikiLeaks Incident has brought new discussions to the cyber security literature. In this respect, this scandal has revealed the fact that, despite all the measures taken, the confidentiality of any information stored in the digital environment cannot be guaranteed and the human element in the system can always cause leaks (Hintz, 2013:146-149). The difficulty faced by a huge technological power like the USA, even while preserving the information it needs to maintain its global power, is very important in terms of showing why ensuring cyber security is important for the survival of states in today's world. In this respect, during the WikiLeaks Incident, it gave the image of a country that had difficulties in controlling the secrets that the USA kept in the digital environment.

US Unmanned Aerial Vehicle Attack (2011)

Traces of viruses have been found on the computers of pilots, especially in drones used in Afghanistan and other battlefields. It is not known for what purpose these viruses, reported by the US Air Force Command, were prepared. It is still unknown how far the virus, which is known to record all key movements of computers, spread in the US Air Force and by which forces and for what purpose (Javaid et al., 2012:586).

Attacks of the US Intelligence Services (2011)

Threats from cyberspace can be very diverse. Countries may not be able to manage important mechanisms that are at the key point in terms of control, and data on national security of states may be stolen. The magnitude of the risk and the damage that can be done is parallel to the knowledge, experience and hardware status of the attacker or persons. For this reason, it is not possible to make a clear inference about how cyber-attack activities carried out by states against other states are done. Because in 2011, the intelligence units of the USA carried out 231 known cyber attacks targeting North Korea, China, Iran and RF (Chapper, 2011).

Edward Snowden (2013)

The event that brought Snowden to the world agenda is the fact that he gave the confidential information he obtained within the scope of his duty in the NSA (National Security Agency) to the officials of The Guardian Newspaper and the publication of some of these documents. Snowden, who left the CIA in 2009, started to work in private companies operating under the NSA, and while working at the Hawaii office of a company named Booz Allen, one of these companies, he started leaking information about US intelligence methods to The Guardian reporter Glenn Greenwald (Miller & Walsh, 2016:193). The US is insistent on ensuring that the information leaked intensely occupies the world public opinion and that Snowden is silenced or returned to the USA. The reasons for this are that Snowden disclosed the cyber espionage capacity that the USA has been maintaining for years by making the most of technological opportunities. By using the cyber capacity developed by the NSA, the USA collects information about its own citizens, as well as the citizens of the countries that its allies and countries regard as enemies. These include contact information of politicians and important personalities over the internet, mobile phones and other special software programs. During Snowden's tenure in Hong Kong, it was handled within the scope of a party change operation carried out independently or jointly by Chinese or Russian intelligence. In terms of cyber security, the Snowden Incident has shown that it is very difficult to keep all kinds of information collected, archived and analyzed as intelligence in the digital environment and by using network technologies in the 21st century world (Verble, 2014:16). For this reason, in order to prevent the emergence of such scandals, the fact that states should continue their cyber intelligence activities with as transparent and democratic methods as possible has been proven once again with the Snowden Incident.

Cyber Attack in the US Presidential Election(2016)

In the national presidential elections of the USA, it is stated that Russia intervened in cyber attacks for the first time (Inkster, 2016:23-26). It is known that during the election period, Hillary Clinton, Trump's rival, accessed information about these cyber attacks and made them public. At that time, President of the United States Obama, on the other hand, warned RF President Putin to stay away from the US elections. At the same time, the necessary instructions were given by the government to the relevant American intelligence units and requested to be investigated. Russian Intelligence Officers living in the USA have been deported on the grounds that they are related to the issue (Lam, 2019:2197). The imposition of sanctions on Russian technology companies operating within the borders of the USA has also come to the fore in connection with these attacks (The New York Times, 2016).

Until now, American officials have held anonymous cyber elements responsible for the vast majority of cyber attacks on critical electoral systems or electoral systems that have been observed to operate without instructions from hostile countries such as Russia, China or Iran. On the other hand, American officials note that unidentified cyber elements are seeking vulnerable and vulnerable points by trying to trap state and local administrations.

Equifax Data Leak (2017)

Experts consider that the possession of personal information of 143 million people in the US, with a population of 324 million, is a major security concern across the country, and they point out that the private information of two out of every five people in the USA is at risk (Berghel, 2017:72-76). Company officials state that the incident was detected on July 29, 2017, prompt action was taken to stop it, and that no unauthorized access to the company's core credit reporting database was found.

2020 State Attacks (2020)

The American Cyber and Infrastructure Security Agency (CISA) said the new hacker attack posed a "serious threat" to the government, states and cities, as well as infrastructure and the private sector. Several top federal agencies were targeted in the attacks. These include the trade and energy ministries. According to the information obtained so far, hackers have managed to gain access to the systems of government agencies and companies with the software of SolarWinds firm (Levin, 2021:17).

CISA noted that it would be "extremely complicated" to purge systems that the attacker has infiltrated from attack. It has been noted that the attacks have been happening since at least March. CISA stressed that the aggressors or intruders have proven to have "patience, operative security and sophisticated feat. Different committees in the US House of Representatives launched a joint investigation into the attack. Jim Inhofe and Jack Reed, Republican and Democratic leaders of the US Senate Security Committee, pointed out that much is unknown about the cyber attack in question. The senators stated that they knew that the cyber attack was still ongoing and that it contained phrases that it was an operation belonging to Russian intelligence (Bansal et al., 2020: 1517-1520).

From this point of view, we can reflect on America's policies against cyber attacks. The following explanation is important in order to see the approach style of America, which uses the information environment most effectively as a technology leader country, against cyber threat and cyber war.

At the meeting of US Secretary of Defense Leon Panetta with businessmen on October 11, 2012 in New York, it was stated that America is facing the possibility of "Cyber-Pearl Harbor", cyber tools of enemy states or radical groups control America's critical infrastructures (Wirtz, 2017:759). He stated that they could use them to capture energy resources, pollute water channels, fill a train with chemicals and direct it for attack purposes, and also stated that the worst possibility is a coordinated attack against critical infrastructure systems and physical damage may occur.

In his speech, Leon Panetta emphasized that when they receive the threat of an attack with such serious consequences, they can respond to these attacks for the security of the nation. This statement is noteworthy in that it sees the classical right to wage war against the state that threatens the United States with cyber attack, as well as it raises the implications of the classical right to respond to cyber attack in terms of international law and armed conflict law (Lawson & Middleton, 2019).

Since cyber warfare requires a high level of interdependence between digital networks and infrastructures in terms of politics and technological competence in terms of aggressors, NATO changed its doctrine according to cyber warfare and started studies to discuss the technical and legal aspects of the issue. In June 2011, NATO Defense Ministers, of which the United States is a member, adopted the revised NATO Cyber Defense Policy. This policy includes community-based efforts on cyber defense. In October 2011, a consensus was reached by the Ministers on the details of the Cyber Defense Action Plan. In the Cyber Defense Policy, cyber threats are defined as potential resources to fulfill the collective defense task stated in article 5 in line with the new Strategic Concept (Doğrul et al., 2011:7).

The cyber attacks experienced have changed the American approach to events. The cases that took place in the cyberspace so far have shown that (Tatar et al., 2014:211);

- Cyber warfare is real and primitive cyber weapons have been used so far, and the parties have not put their real capabilities and weapons into action. This is because the parties do not yet want to show off the abilities they have in their hands. There are comments made that these attacks could end a nation when using the real capabilities of the US and other parties.
- Systems that people need and rely on, from banks to defense radars, are accessible from the cyber environment, and these systems can be deactivated or rendered unusable without ever allowing them to be used.
- The nature of the cyber environment and the complexity of the techniques used show that any cyber conflict situation can easily become global and will attract many states to this war.
- In cyber warfare, the time of the attack and the impact of this attack on the opposite side occur almost simultaneously. This situation also puts the decision-making processes and the time they have in their hands significantly difficult for crisis managers.

Not every attack or malicious activity in the cyber space we have examined above is within the scope of cyber warfare (For example Edwars Snowden's situation). When defining cyber warfare, it is useful to explain the most used and sometimes confused terms in the cyber environment for a better understanding of the subject (Robinson et al., 2015: 72). These attacks are considered that it is important to explain the meaning of the terms cybercrime, cyber espionage and cyber terrorism, which are among the malicious cyber movements carried out in cyber space.

The USA sees cyberspace as a strategic target, in line with the spread of the internet and its penetration into every aspect of life. The USA has set the main goal to ensure the security of the internet, which has been used in basic services for economic growth, global competitiveness and the welfare of its society. In addition, the USA focuses primarily on the technology sector, critical infrastructures, defense and financial service sectors in order to ensure cyber security. It tries to raise the public awareness of cyber security to a high level by cooperating with private companies, academics and non-governmental organizations (Borum et al, 2015:319). There is no doubt about the position of the USA as the main actor dominating cyberspace and the internet. Under this leadership position, the USA allocates a large budget to ensure its cyber security and endeavors to train millions of cyber experts by focusing on cyber wars, which it considers inevitable.

4.1.2. Fundamental Measures of the US Cyber Security Strategy

The beginning of the evolution of US cyber power can be traced historically to the 1930s. In this context, a similar device, which can be seen as one of the first functional computer examples, was produced by the US Navy. However, the US administration established the Advanced Research Projects Agency (ARPA) in February 1958 in order to compete with the USSR in the scientific field (Kott, 2014:3). With the Cuban Crisis, discussions about what kind of measures should be taken to affect ARPANET from these attacks in case of a possible nuclear war started to occur. After the foundation of the Internet, ARPANET was negatively affected by the first computer worm software named "creeper" in 1971. In this context, the mentioned software has been evaluated as the first possible threat sign in the cyber field. At this point, together with their competitive motivation, it is seen how successful the scientists and cultural people of the USA and the USSR were in grasping the importance of cyber space based technologies (Maynard, 2019: 16). In the 1980s, with the increase in the use of personal computers, participation in networks started to increase and as a result, with a virus infiltrating ARPANET in 1980, communication in ARPANET was interrupted for 72 hours (McKelvey, F., & Driscoll, 2019:33). Upon the increase of threats in ARPANET, the US Department of Defense decided to create a new infrastructure where confidential military data would be communicated, and in addition to ARPANET, it established the creation of an infrastructure named Militarynet (MILNET). This institution was closed in 1990 as part of the establishment of networks such as the National Science Foundation Network (NSFNET) (Buzai, 2014: 87).

According to Waltz, it focuses on the fact that the structure of the international system is shaped by an anarchic process and the aims of protecting the sovereignty and security of each state in this system. This situation prevents the states from cooperating for a long time, as the international system in an anarchic structure encourages the insecurity between the states. As a result of the fierce competition between the US and the USSR during the Cold War, in accordance with neo-realist paradigms, the cooperation opportunities of the two states were restricted (Kott, 2014:11). Significant investments in their military capacity have been paved, and as a result, the international system has become much more insecure. By encouraging this situation during the Cold War, it also made a serious contribution to the creation of the digital space, which is now called cyberspace. As a result of these investments, with the new generation developments in cyber space technologies, network technologies were first used by the US Army during the 1st Gulf War in 1990-1991 with a capacity that has not been experienced until that day (Borum et al, 2015:317). We analyzed these attacks in the previous section.

In these years, the US administrations have read the developments in the field of cyber space technologies in their own country as an opportunity to develop their military capacity and have accelerated the process of establishing institutional infrastructures in this regard. In addition, in the 1990s, the documents, doctrines and plans that form the basis of the current cyber security strategy of the USA started to be announced to the world public opinion(McKelvey, F., & Driscoll, 2019:36).

Strategies prominent in published declarations (Borum et al, 2015:320):

- It is necessary for the US public and private sector to act together in order to protect the critical infrastructures,

-The cyber attacks experienced to date do not yet have a level that will completely collapse the US crisis infrastructures, however, these attacks may damage the system,

-Therefore, it has been stated that the US administration must take precautions within the scope of the subject.

Five structures have been established in order to protect the national cyber space;

-National Cyber Space Response System

-National CyberSpace Defense Vulnerabilities Recovery Program

-National Cyber Space Awareness and Training Program

-Official Institutions Against Cyber Attacks Structuring

-National and International Cyberspace Cooperation

In the document prepared by Obama's instruction in 2009, it is basically stated that some measures should be taken to eliminate the problems in the US cyber defense system and that the national cyber security system can only be effective if these organizations act together and in coordination. In 2014, the document named Draft Strategy for Improvement Critical Infrastructure Cybersecurity aimed to develop common standards and methodologies for the protection of critical infrastructures by cooperating with the private sector and official institutions (Newmayer, 2015:9). As can be seen in the aforementioned plan, it includes a comprehensive plan aiming to protect critical infrastructures, which are of great importance for the economic welfare of the USA and the security of its country and which are mainly controlled by private industrial organizations.

The US administration, which is sensitive about increasing cyber security; Significant progress has been made in ensuring network security, creating a common situational awareness of the state, government and private sector partners in preventing threats, and reducing existing vulnerabilities to establish an emergency defense front against threats, and taking swift action to prevent unauthorized access.

Another prominent strategy is to increase the number of cyber fighters by CYBERCOM in 2013, with the increase in the size of threats coming from the internet. In this context, it has almost created a new structure with the cyber warrior staff, which has been increased to 5,000 by CYBERCOM (Pajurek, 2017:165). CYBERCOM has limited open source information regarding the current tasks and operations. The US cybersecurity regulations mainly operate in sectors defined within the scope of the US critical infrastructure, including the financial sector. It focuses on the goal of protecting private sector organizations and other organizations, including this, in accordance with the public authority, to protect their network technologies from cyber attacks and cyber espionage. On the other hand, there is a serious debate regarding the federal and state laws governing the cyber security regime in the USA. These discussions have different sides. The first of the parties supports these regulations by stating that the cyber security regulations are essential for the economic welfare and security of the USA. Within the scope of another view, cyber security laws are supported, but at this point, it is argued that the initiative should be in the private sector, which controls a significant part of critical infrastructures, rather than the public.

With the "Edward Snowden Incident" that broke out in June 2013, the tendencies in the US that support the revision of the federal laws, especially the Patriot Act, which have been harshly criticized for including anti-democratic practices and controlling the cyber security field, have increased. As a result, the US Freedom Act, which can be claimed to be relatively democratic, was adopted by the Obama administration in 2015 (Warner, 2020: 3). With this law, the monitoring, tracking and archiving of the communication on the internet was brought under a stricter regime. Also the United States is home to approximately 63% of the world’s privately-owned cybersecurity companies (Darıcılı, 2017:81). This data shows us new security investments by government work.

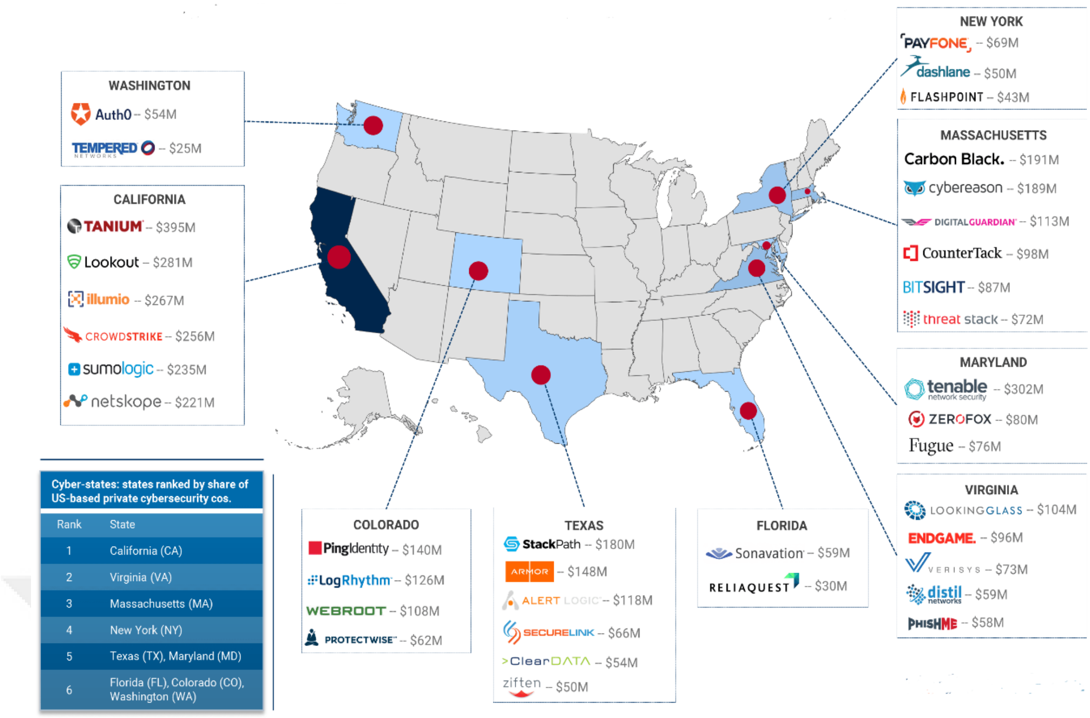

Figure 3. 2 The Country's Most Well-Funded Cyber Security Start-ups On One Map

Resource: CBInsights, 2017

If we sum this section according to cyber security of USA:

Global power states have begun to see cyber attacks and new generation information warfare techniques as an important method of strategic defense and damage to the opponent. The fact that cyber activities can be done easily and without a trace is one of the main factors that encourage this method.

In this context, developments in the cyber field have brought new security risks. While the importance of the states in eliminating these risks has increased even more, the states have had difficulties in developing strategies in this regard. It can be argued that with the cyber attacks originating from small groups and individuals, the structure of the international system has begun to turn into a more uncertain and anarchic state than before, in accordance with neo-realist paradigms (Pajurek, 2017:166). Depending on the expansion in the field of cyberspace, states react to threats from hostile states or non-state actors by establishing cyber armies and cyber security institutions as part of their cyber security strategies, as well as by training cyber experts and academics. The fact that it is not known for sure whether it is conducting a secret cyber activity against a state appears as the factors that cause the anarchic structure of the international system to deepen.

4.2. Cyber Security As A Critical Part Of The Turkey 's National Security Policy

In 2009, the framework of cyber defense and security principles was drawn with the "National Virtual Environment Security Policy" prepared by the working group coordinated by TÜBİTAK UEKAE (National Electronics and Cryptology Research Institute). Important and beneficial developments in the context of cyber security started in 2010 when Turkey became a party to the Council of Europe Cyber Crimes Convention. With the definitions and provisions prepared in more detail than the Turkish Penal Code, the gaps in the legislation started to be filled (Kılcı, 2020: 114) . Framework drafts prepared by international organizations have started to affect the agendas of the countries. In addition to this study, SGE (Cyber Security Institute), which has been operating under BİLGEM (Information and Information Security Advanced Technologies Research Center) since 2012, contributes to the formation of the necessary knowledge in the field of cyber security (Bıçakçı et al., 2015:7). Some regulations have been made in the Turkish Penal Code No. 5237 in order to ensure cyber security as a legal infrastructure. Crimes committed through electronic networks are accepted as the aggravating factor of the incident, and crimes specific to electronic networks are mentioned under the title of Crimes in the Field of Informatics in the tenth section of the law (Bıçakçı et al., 2015:8). After 2012, the agency responsible for cyber security became the Ministry of Transport, Maritime Affairs and Communications. The Cyber Security Council has been established, and the duties and powers of the Cyber Security Council and the Ministry of Transport, Maritime Affairs and Communications have been determined.

With the 1st National Cyber Security Exercise conducted under the coordination of the Information and Communication Technologies Authority, the necessary statistical data were collected with the exercise with the participation of public, private and non-governmental organizations. With the 2nd National Cyber Security Exercise, which was carried out under the coordination of the Ministry of Transport, Maritime Affairs and Communications, which included more participants and was tested by real cyber attacks, deeper and detailed data were obtained and necessary solutions were started to be planned (Aslay, 2017:25).

With the Decree of the Council of Ministers, the following duties have been determined regarding cyber security (Kurnaz & Ören, 2019: 82-88):

- To ensure the security of national information technologies and communication infrastructure and systems and databases, to identify critical infrastructures and to establish cyber threat and attack monitoring, intervention and prevention systems for them, to establish relevant centers, to have them installed, to control, operate and continuously strengthen these systems.
- To prepare the procedures and principles to ensure the security and privacy of information and data belonging to public institutions and organizations.
- To encourage the development and production of all kinds of national solutions and intervention tools against cyber attacks in the provision of National Cyber Security.
- To follow the establishment of technical infrastructure in public institutions and organizations in the provision of National Cyber Security, to ensure that the effectiveness of applications is verified and tested.
- To issue security certificates by determining the procedures and principles to real and legal persons working in the field of training, testing and solution generation in the field of information security.

The enacted decree creates a committee where concrete studies will be carried out on behalf of cyber security, and at the same time, it imposes specific tasks on cyber security to the relevant ministry. The Cyber Security Cluster of Turkey, a project supported by the Presidency of Defence Industries in 2017, creates a collaborative and coordinated working environment in which companies that develop domestic and national cyber security products and services are members (Özbenli & Özlü, 2020:77). The International Cyber Security Federation, which was established to increase cyber security awareness in the public and to create a system based on advanced technology, also operates in the field of cyber security. The Informatics Association of Turkey, established in 1971 as the world's first association in the field of informatics, acts as the largest and well-established non-governmental organization in the informatics sector of Turkey. The primary work carried out in the military field is the Cyber Defense Command, which was established under the General Staff. This command works to make the cyber security of other commands effective.

4.2.1. Cyber Attacks Targeting Turkey

Unlike the United States, there is no single organization attack in Turkey, so this section provides information about cyber attacks. Although the number of attacks was large, they took place in groups at different times.

According to researchers, Turkey is the 5th country in the world where the most attacks are made by target-oriented threat groups (Çetin et al., 2015:225). The most targeted sectors are public, banking and finance, telecommunications, health, energy and infrastructure, and e-commerce. The Ministry of Transport and Infrastructure has reported that 325 thousand cyber attacks targeting Turkey have been prevented in the last 3 years with KASIRGA, AVCI and AZAD applications, which were developed with domestic and national facilities in order to improve the understanding of cyber security throughout the country and to prevent cyber threats. According to the report of the International Telecommunication Union's Global Cyber Security Index published in 2019, Turkey became one of the 20 safest countries in the world in this field. It ranked 11th in Europe (Sari, 2019:129).

In terms of information security, when the position of Turkey compared to other countries in the world is evaluated according to different criteria, different results emerge. For example, in the most up-to-date intelligence report prepared by the cyber security firm FireEye, it is emphasized that there is more "targeted malware" in Turkey than occurred in Europe in 2016 (Aslay, 2017:26). According to the fireye spokesperson, infiltrations in this category likely have the same characteristics as the activities of state-sponsored, advanced and known hackers 23. According to Symantec's Internet Security Threat Report, Turkey accounts for 3.4% of the total malware detections in Europe, the Middle East and Africa in 2016 (Aslay, 2017:26).

Ransomware (2000-now)

This type of attack, which is called ransomware or ransomware pests, is generally carried out against institutions, SMEs or companies. The aim here is to take advantage of the weaknesses of the target system and capture the data inside and make it unreadable by encrypting it. Achieving their goals, cyber attackers contact the institution they attacked and demand a ransom to unlock the data they rendered unreadable.

Phishing Attacks (2000-now)

Phishing attacks, which are called phishing, come across as a method based on completely deceiving the other person. The purpose of this attack is to capture the passwords and user accounts of the target person. When the cyber attack is successful, the passwords of the other party can be captured, the bank accounts can be emptied, and the necessary access to the corporate network can be obtained. Cyber attackers generally redirect users to fake sites prepared by using the name of these institutions with fake emails they prepare as if they were sent from a bank or an institution.

Russian Attacks(2015)

With the downing of the Russian plane in 2015, Russian Hackers aimed to wear down the critical infrastructures that constitute the banking and finance, public institutions, e-government system of Turkey. While the attacks continued, a video was broadcast by the Anonymous hacker group and the attacks were undertaken. Although there will never be any clear evidence regarding the identity of the real planner, the attack against Turkey has a capacity to affect at least 400,000 sites, and the targeting of these sites as e-government, university, military or local company sites has shown that the attacks are planned (Daricili & Özal, 2017:24). In response, Turkey cut off international internet traffic on the first day of the attacks and access to websites with ".tr" extensions from abroad was also blocked. In addition, during the attacks, Turkey tried to ensure the continuity of public service by taking the operators providing service around, almost evading the attacked operators. At this stage, Cyber Incidents Fight Teams (SOME) played a role.

Although the attacks show that Turkey has partially progressed in its cyber security strategy, it has also revealed that the cyber defense resistance is still extremely insufficient, scattered and unplanned (Daricilı, 2018: 5-7). For example, no official authority has made any statements about the nature of the attacks until almost a week has passed since the attacks. This has led to serious disinformation during cyber attacks.

In general, it seems quite difficult to make a clear assessment regarding the determination of the damage caused by the attacks. It is usual to make public statements by the authorized institutions about the cost of the damage caused in Western countries. However, there is not yet an institution in Turkey to do a study. Since the cyber attacks on Turkey are not shared with the public, it remains unclear whether a cyber espionage activity was carried out against state institutions during cyber attacks (Can et al., 2018:183). In this context, it will be seen whether the strategically important information of the state was leaked from Turkish official institutions and organizations during the cyber attack.

4.2.2. Fundamental Measures of the Turkey's Cyber Security Strategy

Many countries, especially Turkey, and international organizations such as NATO and the EU have produced cyber security strategies. As a result of the examination of national cyber security strategies, it is seen that the following common goals are mentioned in the strategy documents ((Daricili & Özal, 2017:26):

• Providing a secure, attack-resistant and reliable cyberspace.

• Promoting economic and social welfare, safe business environment and economic growth [through information systems].

• Keeping the risks of information and communication technologies under control.

• Making IT infrastructures resilient.

Cyber security strategy studies do not have a long history in Turkey. One of the most important activities that stand out in terms of establishing cyber security is the adoption of some laws regulating this area. Although the measures taken in the cyber space have increased in recent years, the agreements made are described in the previous section.

With the Decree of the Council of Ministers, the following duties have been given to the Ministry of Transport, Maritime Affairs and Communications regarding cyber security strategies (Kurnaz & Önen, 2019: 84):

- To prepare the procedures and principles to ensure the security and privacy of information and data belonging to public institutions and organizations.
- To ensure the security of national information technologies and communication infrastructure and systems and databases, to identify critical infrastructures and to establish cyber threat and attack monitoring, intervention and prevention systems for them, to establish relevant centers, to have them installed, to control, operate and continuously strengthen these systems.
- To follow the establishment of technical infrastructure in public institutions and organizations in the provision of National Cyber Security, to ensure that the effectiveness of applications is verified and tested.
- To carry out awareness-raising, training and awareness-raising activities on National Cyber Security.
- To issue security certificates by determining the procedures and principles to real and legal persons working in the field of training, testing and solution generation in the field of information security.
- To carry out the secretariat service of the Cyber Security Board.

As can be understood from the name of the cyber security board, its importance in cyber security policies is great. The decisions to be taken, the strategies and policies to be followed are approved and concluded by this institution.

On the other hand, decisions regarding the determination of critical infrastructures, one of the important elements of cyber security mentioned in the previous sections of the research, are also taken by this board. So, the Cyber Security Council can be shown as a central actor in determining cyber security policies for Turkey at the point reached. A National Cyber Incident Response Center has been established within the Information Technologies and Communication Institution in order to identify threats to cyber security in Turkey, to reduce or eliminate the effects of possible attacks and incidents, and to share them with the determined actors (Ünver, 2017:107). The lack of intervention in the defense made against the attacks of Anonymous and Redhack groups against Turkey in 2015 due to the lack of sufficient crisis management (Bıçakçı, et al., 2016:75) was criticized. Nevertheless, a perception towards the protection of critical infrastructures has started to emerge in Turkey recently. In this context, legal regulations regarding cyber security were made in the country, strategy documents were prepared, new government units were established, these units and institutions started to work on cyber security (workshops, training, publications, projects, etc.).

The USA's awareness of cyber security dates back to the early 2000s. On the other hand, looking at the point reached in the strategy document published in 2015 regarding the cyber security of the country, it is observed that, despite the other documents issued in this time period, concrete steps have been taken more recently and this awareness is still developing (Harrop & Matteson, 2015:164). Considering this situation in terms of Turkey, we can say that it is not too late for studies and developments regarding cyber security. We are of the opinion that it is possible to catch the shield train in establishing cyber security infrastructures in the medium and long term by implementing structural reforms such as the localization of critical infrastructures, training of local IT experts and appropriate policies. Although Turkey is not yet at the desired level in crisis management, it is still not a situation to be late. The fact that very few of the policy proposals in the development plans are related to cyber security and that similar to the development plans, there are no policy proposals regarding cyber security in government programs show that cyber security in Turkey is not seen as a macro policy yet (Göçoğlu, 2018:162).

Studies on cyber security in Turkey are at the beginning stage, it has been observed that the perception of the subject in the country has increased rapidly as in the world. In this direction, the legal infrastructure regarding cyber security has begun to be established in the country, although not included in the development plans, issue-oriented strategies and action plans have been created and units have been established in line with the policies. However, these need to be improved. The said development will be possible primarily by training and establishing human resources for cyber security, as well as technical infrastructure. Turkey needs strategies on cyber security, which have been created on the basis of a consensus, including individuals, private companies, state institutions as a party, binding for all parties, and designed specific to the country, taking into account the country's dynamics (Karabacak et al., 2016: 529). Although there are companies established in the states for cyber security in the USA, Turkey is far from this situation.

4.3. Comparative Work Of The U.S And Turkey

The rapid growth of the cyber security market ensures the proliferation and growth of new enterprises and technology companies in Turkey in the field of cyber security. In cyber attacks against Turkey, titles such as ransomware, DDoS attacks, attacks on cloud systems, malware for mobile applications, hacking of IoT tools come to the fore. The main problem of institutions in Turkey is to take measures against cyber attacks and the insufficient number of experts to be employed as cyber security experts. The proportion of companies prepared for a cyber attack in Turkey increased from 12 percent in 2018 to 48 percent in 2019 (Sari, 2019: 131). This shows us that the awareness in institutions is rapidly increasing, that the necessary infrastructures for cyber security have been established, necessary precautions have been taken and even cyber security strategies have been established. The Turkish Cyber Security Cluster, which has reached over hundred companies today, also carries out efforts to make Turkish entrepreneurs a global player (Göçoğlu, 2021:19). Since cyber security is a broad concept that covers not only internet security but all communication infrastructures, it is necessary to determine the national cyber security policy with a multi-sectoral approach. It would be wrong to consider that Turkey is not exposed to a serious cyber attack as terrorist organizations do not have this potential. For this reason, measures should be taken for active defense as well as what is done in the passive defense field. While developing measures in the field of cyber security, it should not be overlooked that security-democracy, benefit-cost balances should be considered.

In order to understand the cyber security measures of the USA, it is useful to first determine from which components and actors this policy was created and how to follow this policy in a holistic way. In this context, the USA's orientation on cyber security policy is realized with the effects of the National Security Policy and Strategy, other strategic documents, laws, directives and recommended regulations, institutions related to cyber security and finally third party organizations (Tirrell, 2012: 7). The first comprehensive document published in the USA on cyber security was in the early 2000s.

There are five important actions and measures to protect the US cyberspace (Pajurek, 2015: 175):

1. Continuous evaluation of the risks and vulnerabilities of federal cyberspace.

2. Authorizing federal cyber system approved users.

3. Ensuring the security of federal local wireless networks.

4. Ensuring the security of the systems from which the state provides input through outsourcing and procurement.

5. Encourage central and local government organizations to negotiate information technology security programs that they can develop with institutions in other similar countries.

The measures taken are about transforming cyber defense operations, developing an active cyber defense capacity, reducing cyber aggression, creating forces ready to maneuver, and developing unpredictable defense strategies. Other measures are as follows; To develop systems that can survive even against very large and comprehensive cyber attacks, to identify high priority areas of duty, to succeed against comprehensive cyber attacks, to create a renewable cyber capacity. With these measures, it is ready to protect the interests of the country from devastating cyber attacks. An intelligence structure has been established to receive emergency alerts and threats in advance, and both human resources and cyber facilities have been mobilized for this. In line with all these issues examined, it is seen that the USA is a leading country in developing cyber security policy. While the nationality of the cyber infrastructures it creates keeps the country's dependence on cyber at a minimum, the dependence of critical infrastructures on cyber infrastructures weakens the cyber defense function of the country.

Considering this situation from the perspective of Turkey, it can be said that it is not too late for the studies and developments regarding cyber security, and importance is given to the establishment of cyber security infrastructure with rapid structural reforms and appropriate policies.

CONCLUSION

The technology age we are in also highlights cyber risks and cyber threats. Black hat hackers or hacker groups, which we define as malicious hackers, can harm many institutions or organizations such as governments, institutions, SMEs, hospitals or cafes. When we examine cyber attacks, we can see that they are carried out for many purposes, from hacktivism attacks for money, blackmail or political reasons, to theft. While cyber attacks can have a purpose, we witness that attacks are carried out without any purpose, the reason is only to cause harm or ego satisfaction.

When cyber attacks occur between states, it is defined as "Cyber Warfare". Cyber attacks in many areas such as interstate espionage, theft of secret documents, and spying have increased in recent years and have caused great financial and moral problems for states. Especially when examining the confidential information leaked over Wikileaks, we can foresee that these wars will be confirmed with bigger and worse results in the coming years. In this study on Inter-State cyber attack, examples of cyber attacks in the United States and Turkey are examined. Cyber wars occur when cyber attacks happen between states. In cyber wars, it can be done for purposes such as information leakage, vulnerability finding, intimidation, political and economic reasons, as well as cyber attacks for military purposes and cyber espionage. Cyber attacks are not only done to states, institutions or organizations. We also observe that almost all kinds of attacks can be made against SMEs and even individuals. The fact that cyber hackers can pursue different purposes in a way that can cause material and moral damages without targeting or can only harm for ego satisfaction shows that today's technology world is an inevitable security problem. In cyber attacks against Turkey is denial of service, which is called DDOS. These attacks cut all servers and internet access of your institution or company, causing you to be disconnected from the outside world and become incapable of doing business. In today's internet world, DDOS attacks are very dangerous and serious enough to cause financial damages for companies that provide customers in a completely virtual space such as e-commerce and generate their revenues. Turkey is among the top 5 countries where cyber attacks are made the most. The USA is in the first place. "Snowden Incident" and "WikiLeaks Documents" and "Democrat Party Hacking

Scandal" are among the most prominent cyber attacks in the USA. The USA has accelerated its planning to develop an effective cyber attack and defense capacity by using developments based on network technologies. Almost all of the official cyber security documents and presidential orders put forward by the USA in the 1990s have been prepared with a focus on developing and protecting the commercial capacity of the internet and its global dissemination in order to maintain the cultural hegemony of the USA. The US Department of Defense Cyber Strategy implemented since 2015 strengthened its security capacity. The USA has managed to have an advanced cyber attack capacity today with the cyber security documents it has published continuously. The fight against cybercrime in Turkey was carried out by the Information Technologies and Communication Authority (BTK) together with non-governmental organizations and institutions until 2012 under the coordination of the Ministry of Science, Industry and Technology. Later, the "National Cyber Security Strategy and 2013-2014 Action Plan" was prepared and put into effect. Turkey's National Cyber Security Strategy and 2013-2014 Action Plan aimed to protect information systems from attacks and to ensure the confidentiality, integrity and accessibility of the information processed in this environment. At the point we have reached today, we see that another important step is taken with the Personal Data Protection Authority law and that the privacy and security of institutions, companies, SMEs and even individuals are given serious importance. In terms of information security, when Turkey's position with respect to America is evaluated, a negative result emerges. Although Turkey started taking measures later, it is not too late yet. In recent years, more investments have been made in cyberspace to close this gap. Turkey does not openly and regularly publicize the cyber attacks. Therefore, unlike America, there is disorder.

REFERENCES

Akbulut, B. (2017). Criminal Law Responsibility Of Legal Entities In Turkey. *Perspectives of Business Law Journal*, (06), 154-158. http://businesslawconference.ro/revista/articole/an6nr1/23.%20Berrin%20AKBULUT.pdf

Al-Tae, A. K. J., Al, A. P. H. A. H., Dhalimi, P., & Al-Shaibani, A. K. J. (2020). Relationship of Cybersecurity and the National Security of the Country: Iraq Case Study. *Systematic Reviews in Pharmacy*, *11*(12), 469-476. https://www.sysrevpharm.org/articles/relationship-of-cybersecurity-and-the-national-security-of-the-country-iraq-case-study.pdf

Andress, J., & Winterfeld, S. (2013). *Cyber warfare: techniques, tactics and tools for security practitioners*. Elsevier.
https://books.google.com.tr/books?hl=tr&lr=&id=Udpb2PRRuWwC&oi=fnd&pg=PP1&dq=The+threats+that+cyber+security+deals+with+can+be+examined+under+five+headings:+Hacktivism,+Cyber+Crime,+Cyber+Sabotage,+Cyber+Terrorism,+Cyber+Warfare.+Each+threat+type+has+a+motivation,+actors,+and+goals.&ots=GlgN4xK9UY&sig=YeoDGGcr24tJkUzIowuUpTLaAvM&redir_esc=y#v=onepage&q&f=false

Arı, T. (2013). International Relations Theories (8th Edition). Ankara: MKM Publishing.

Aslay, F. (2017). Siber saldırı yöntemleri ve Türkiye'nin siber güvenlik mevcut durum analizi. *International Journal of Multidisciplinary Studies and Innovative Technologies*, *1*(1), 24-28. https://dergipark.org.tr/en/download/article-file/375131

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour?. *arXiv preprint arXiv:1901.02672*. https://arxiv.org/ftp/arxiv/papers/1901/1901.02672.pdf

Bagby, L. M., (2002), Political Thought, Toronto, Wadsworth/Thomson Learning Publication.

Bansal, C., Deligiannis, P., Maddila, C., & Rao, N. (2020, July). Studying ransomware attacks using web search logs. In *Proceedings of the 43rd International*

ACM SIGIR Conference on Research and Development in Information Retrieval (pp. 1517-1520). https://arxiv.org/pdf/2005.00517.pdf

Bashir, M., Wee, C., Memon, N., & Guo, B. (2017). Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool. *Computers & Security*, *65*, 153-165.

BBC News.(2012). Profile: Garry Mckinnon, https://www.bbc.com/news/uk-19946902 (Retrived:21.04.2021)

Beriş, H. E. (2010, December). State and Security Problem in Liberalism. 21. Century Magazine, 24, 91-95. Retrived from 24 March 2021 from http://www.21yuzyildergisi.com/assets/uploads/files/14.pdf

Berghel, H. (2017). Equifax and the latest round of identity theft roulette. *Computer*, *50*(12), 72-76. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8220474

Best, J. (2017). Security, economy, population: The political economic logic of liberal exceptionalism. *Security Dialogue*, *48*(5), 375-392. https://d1wqtxts1xzle7.cloudfront.net/53410611/Security__Economy__Population-JBest.pdf?1496773432=&response-content-disposition=inline%3B+filename%3DSecurity_Economy_Population_The_Politica.pdf&Expires=1618330320&Signature=Y2m1Lp-KG7myoVxY5xJDJmGAl3DOU3zJHoJdy7pmj7WouU-7QYUmuGyibJE0CRrLkkY8365pReyiFt-A42rU74ke7xO7qRAK2yg0AdV~Mr2Y652xNwz5B41J~VTPP2TtSHWbXWxpqYX2luczOC173qi1x48DxhKYNahvxiiwaEAgcBnvenjc9nTy7H4UoREOv9Q3WBg4VoQH5Hlt95UzcR8VJTGvnllH2EWiQJBEnLcetNrr4NjEB53vaY3Xgw5sMQs3AlUbZ7ZAYarZLcPcpZgJYjqf~UbB4fwTAYA-uWBb23TA5XEDhs4TLaUbSE-3E3Yh8aqAq5vRiSC6dBubYg__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

Bıçakcı, S., Ergun, D., & Çelikpala, M. (2015). Türkiye'de siber güvenlik. *Ekonomi ve Dış Politika Araştırma Merkezi (EDAM) Siber Politika Kağıtları Serisi*, *1*, 1-35. https://www.edam.org.tr/document/CyberNuclear/SiberKitapTR/edam_siber_guvenlik_b2.pdf

Birdişli, F. (2011). "Historical and Intellectual Basis of National Security Concept". Erciyes University Journal of Social Sciences Institute, 31. p. 149-169.

Borum, R., Felker, J., Kern, S., Dennesen, K., & Feyes, T. (2015). Strategic cyber intelligence. *Information & Computer Security*.

Bozdağlıoğlu, Y. (2007), "Constructivism Approach (Constructivism)", International Relations, Introduction, Concepts and Theories (Ed .: Haydar Çakmak), Ankara: Platin Publications.

Browning, C. S., & McDonald, M. (2013). The future of critical security studies: Ethics and the politics of security. *European Journal of International Relations*, *19*(2), 235-255. https://d1wqtxts1xzle7.cloudfront.net/31439879/Browning_and_McDonald__The_Future_of_CSS__EJIR_2013.pdf?1372043444=&response-content-disposition=inline%3B+filename%3Dwith_Christopher_S_Browning_The_Future_o.pdf&Expires=1618331266&Signature=FENEjVxSqmyAuhTnGjrCu-mqeHHlzheXap8EjHfvYvu~Y10m6TLPpjDuSI1XinrwKyod6hlqvof02ZAWfQewLzQbTvb5bIoqhfQr6MpyFsi6SXRNPmcMLJMjtl0sOhLDYrmAt23-AEUF9Dm42H~uYF84lqU--dGfbBB1g3JUKhNgcCzyqbmK8egOMy9Ny7hzsjropuVlUY7xkTIJy7UDphnoaZnr5tMEq0vW1LktNTjLQ72Wo68cZk~9bec7abJbYXYMuXThFfF3fxuTUd7m1GjWqy5EWs~2~5URG2jfPwxZwX1u6CI8oq~MehMv~tybRG5tt5epsKIZkm5sXxcHFQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

Bruner, J. (1987). Life as narrative. *Social research*, 11-32.

Buzan, B. (2008). "Askeri Güvenliğin Değişen Gündemi", Uluslararası İlişkiler, 5(18), 107-123. https://lonang.com/wp-content/download/Grotius-LawOfWarAndPeace.pdf

Buzai, G. D. (2014). Fronteras en el ciberespacio: el nuevo mapa mundial visto desde Buenos Aires (Argentina). *Cuadernos de Geografía: Revista Colombiana de Geografía*, *23*(2), 85-92.

Can, S. H., Ikitemur, G., & Hendy, H. M. (2018). Measurement of organisational variables associated with cyber security preparedness in Turkey. *Cyber Security: A Peer-Reviewed Journal*, *2*(2), 181-192.

Canbolat S. İbrahim (2006), Marxism and International Relations, International Relations in a Changing World, Lalezar, Ankara.

Carr, E. H. (1994). Realism and Idealism. *Conflict after the Cold War, Boston, Simon & Schuster*, 72-87.

Carr, M. (2016). Public–private partnerships in national cyber-security strategies. *International Affairs*, *92*(1), 43-62. https://www.chathamhouse.org/sites/default/files/publications/ia/INTA92_1_03_Carr.pdf

Catota, F. E., Morgan, M. G., & Sicker, D. C. (2019). Cybersecurity education in a developing nation: the Ecuadorian environment. *Journal of Cybersecurity*, *5*(1), tyz001. https://watermark.silverchair.com/tyz001.pdf?token=AQECAHi208BE49Ooan9kkhW_Ercy7Dm3ZL_9Cf3qfKAc485ysgAAAq4wggKqBgkqhkiG9w0BBwagggKbMIICIwIBADCCApAGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQMIo_9PqEbbqKUaP5lAgEQgIICYRME7XCcDiLZmYvHr4MjVpxiAfAY4TsQh7vBN5dI8XBFc1nMop3opk6ZFIlwbFQzu9zKCMQADxlu9LIH--0yc4Ei3wX9Tw4zEeobI1XC4P6x3eeRLkUZcjgJ29cGL-vmd-KE-95YXpcEWzKAtPnv6g_FlYOgJRVmgXOyhX9ywQnZUCWFApDgqk2epUSKgcsjdBSlwXBBNO9Ek9XRcVZC0TtbqDPSiFALNzG2QVxD-pRrJELax4606eYfe4JAyI0AfyxsN8yngbG8aCcb2T3yVbR1gr7RTkl8X6Z4MN9u8vJhuKabDHIBaiBcpkoxaunBVZ1mPzYv3DwaLgAWyCdAErKIfNP26NfniGoaHA4W2F6NlOqvzp1_Ymm7efkk2dQwddvhq7qKmRwev0Qw7ojrV3smqPFcEJHMpVXXtfwLwIfCIQ5d_lapvINHMZpYUqiA51_jf-5E7tmVabLYxaGlESipamnYJnSo5WsZ_HAcl1_gY1CrKAZ853xvcmyZLE6xu6-iqq61N7smmWnYUH7tvPGI3ou4AU68Mvho849bDxfUezuO5fJhmDNbr9IbUnN972QasNQ3NAkXOiX3tJoSHFsaCeE0bjVZQ_-ZApxS2sOW4JcFLTTGmXcoglD15zcNGG4QTjXE4q_Pk8AXUC2DJT4O2MS1F11zosXPRaGJGjdEe_BCjRsZouWVQMd90DFMUnJuZ1WpCOUkQbVDvK_O9zFPS2M_7p2hlOaCFhQ3ROVpsFwh7Qh64ycYc2mK2QItA56glQkr7DMurjLiZnwDmMIxe0CeD02T8dXrKLIKiD_qw

Cavelty, M. D. (2014). Breaking the Cyber-security Dilemma: Aligning Security Needs and Removing Vulnerabilities. Science and Engineering Ethics, 20(3), 701-715.

Chapper, J. R. (2011). *Worldwide threat assessment of the US intelligence community*. OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE WASHINGTON DC. https://apps.dtic.mil/sti/citations/ADA539742

Chou, T. S. (2013). Security threats on cloud computing vulnerabilities. *International Journal of Computer Science & Information Technology*, *5*(3), 79. https://d1wqtxts1xzle7.cloudfront.net/54805153/5313ijcsit06.pdf?1508848706=&response-content-disposition=inline%3B+filename%3DSECURITY_THREATS_ON_CLOUD_COMPUTING_VULN.pdf&Expires=1620312917&Signature=CEls3iSrovD~s8zG4SWvVyM80R9NHQE-5fbObKcf~imPWvkoe~-zwmuANqm-yte9j8fCBGOIXgVC79zB2rN73KgL3n9OSi3UcQzojyZpy953kUEy8K67CFveawQGPTr4l0Y2FLYAk4BSfF~FVHBbKU7zZjB7yxqkCF6V5Qe3MzMFAKmtwQITnndkp-Vh3JUfTmJGk0Of2~kNeTFyalQ46VaTloGxkj59C51TbDfw4vNcqbctdpfmCRLEKQZ84VlokRWG5-ZE3fwQeVo3bA69IooroYjPF3NVXg6CG4Mw4uBngTUb5yjl-dBDZ~qHs6FApIvGcDgmTYLJLChHCbgqqA__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

Collins, S., & McCombie, S. (2012). Stuxnet: the emergence of a new cyber weapon and its implications. *Journal of Policing, Intelligence and Counter Terrorism*, *7*(1), 80-91.

Crocker, S. D. (2019). The Arpanet and Its Impact on the State of Networking. *IEEE Computer Architecture Letters*, *52*(10), 14-23. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8848151

Çetin, H., Gundak, İ., & Çetin, H. H. (2015). E-işletme güvenliği ve siber saldırılar üzerine bir araştırma. *Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *6*(2), 223-240. https://dergipark.org.tr/en/download/article-file/253880

Danyk, Y., Maliarchuk, T., & Briggs, C. (2017). Hybrid war: High-tech, information and cyber conflicts. *Connections*, *16*(2), 5-24. https://www.jstor.org/stable/pdf/26326478.pdf?acceptTC=true&coverpage=false

Darıcılı, A. B. (2017). Comparative analysis of cybersecurity strategies of the United States and the Russian Federation.

Daricili, A. B., & Özdal, B. (2017). Enformasyon Savaşı Bağlamında Rusya Federasyonu-Türkiye İlişkilerinin Analizi. *İstanbul Gelişim Üniversitesi Sosyal Bilimler Dergisi*, *4*(1), 19-40.

de Miranda Rios, V., Inácio, P. R., Magoni, D., & Freire, M. M. (2021). Detection of reduction-of-quality DDoS attacks using Fuzzy Logic and machine learning algorithms. *Computer Networks*, *186*, 107792. https://hal.archives-ouvertes.fr/hal-03182934/document

Dogrul, M., Aslan, A., & Celik, E. (2011, June). Developing an international cooperation on cyber defense and deterrence against cyber terrorism. In *2011 3rd International Conference on Cyber Conflict* (pp. 1-15). IEEE. https://ccdcoe.org/uploads/2018/10/DevelopingAnInternationalCooperation-Dogrul-Aslan-Celik.pdf

Giri, S. (2019). Cyber Crime, Cyber threat, Cyber Security Strategies and Cyber Law in Nepal. *Pramana Research Journal*, *9*(3), 662-672. https://www.pramanaresearch.org/gallery/prj-p576.pdf

Göçoğlu, V. (2018). Türkiye'nin siber güvenlik politikalarının kamu politikası analizi çerçevesinde değerlendirilmesi.

Goztepe, K., Kilic, R., & Kayaalp, A. (2014). Cyber defense in depth: Designing cyber security agency organization for Turkey. *Journal of Naval Science and Engineering*, *10*(1), 1-24. https://www.researchgate.net/profile/Kerim-Goztepe/publication/274733863_Cyber_Defense_In_Depth_Designing_Cyber_Security_Agency_Organization_For_Turkey/links/55290b710cf2779ab78e45a4/Cyber-Defense-In-Depth-Designing-Cyber-Security-Agency-Organization-For-Turkey.pdf

Grotius, H. (2012). *Hugo Grotius on the law of war and peace*. Cambridge University Press.

Gürkaynak M. ve İren,A.A.(2011).Reel Dünyada Sanal Açmaz: SiberAlanda Uluslararası İlişkiler, Süleyman Demirel Üniversitesi İktisadi ve İdariBilimler Fakültesi Dergisi,16 ,265

Hama, H. H. (2017). State security, societal security, and human security. *Jadavpur Journal of International Relations*, *21*(1), 1-19.

Hamdy, N., & Mobarak, R. (2010). Iraq War ushers in Web-based era. *Media*, *3*(1-4), 245.

Harrop, W., & Matteson, A. (2015). Cyber resilience: A review of critical national infrastructure and cyber-security protection measures applied in the uk and usa. *Current and emerging trends in cyber operations*, 149-166.

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The law of cyber-attack. *California Law Review*, 817-885. https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com.tr/&httpsredir=1&article=4844&context=fss_papers

Herrera, A. V., Ron, M., & Rabadão, C. (2017, June). National cyber-security policies oriented to BYOD (bring your own device): Systematic review. In *2017 12th Iberian Conference on Information Systems and Technologies (CISTI)* (pp. 1-4). IEEE. https://d1wqtxts1xzle7.cloudfront.net/53542446/Paper_CISTI_2017-Mario_Ron.pdf?1497621534=&response-content-disposition=inline%3B+filename%3DNational_Cyber_security_Policies_oriente.pdf&Expires=1621872880&Signature=KuiYMYSTe-r2BlBv1-fcSaHWnLPNfrg1i0z3kYLiS~ds8EznYt0hamQtcpMzYmaZWfvvnNrtPH8mYAM3vh79daU-IsyBh3F6iZnU-g6xUBiDcadHO4rOyBu5JRuOtQxDAOy4SB1k7zFNOntSv5RCQ2zZU4vBcekt~PRoF0m03gfAKZeqy27EmZxcs8tfpJQ8gfaooOlk3hEHV1YXORdYF0O1ehJM9YcN8J83cxiUryKEunmUw5icHro0TtzFAqaouWHH8a0fXVGIof10AIEJd50AoibQbE8HoiNuCrM3kTMVb~lt47N9AscXYWZ9saMfqvkOArdBgEO~5nWDUQ5m6w__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

Hekim, H., & Başıbüyük, O. (2013). Siber Suçlar Ve Türkiye’nin Siber Güvenlik Politikalari. *Uluslararası Güvenlik Ve Terörizm Dergisi*, *4*(2), 135-158. https://www.researchgate.net/profile/Hakan-Hekim/publication/348241799_Siber_Suclar_ve_Turkiye%27nin_Siber_Guvenlik_Politikalari/links/5ff4b08ea6fdccdcb83388ca/Siber-Suclar-ve-Tuerkiyenin-Siber-Guevenlik-Politikalari.pdf

Hintz, A. (2013). Dimensions of modern freedom of expression: Wikileaks, policy hacking, and digital freedoms. In *Beyond WikiLeaks* (pp. 146-165). Palgrave Macmillan, London. https://link.springer.com/chapter/10.1057/9781137275745_9

Hobbes, T. (1967). *Hobbes's Leviathan*. Рипол Классик.

Howard, M., & Lipner, S. (2006). *The security development lifecycle* (Vol. 8). Redmond: Microsoft Press.

Hu, F., Lu, Y., Vasilakos, A. V., Hao, Q., Ma, R., Patil, Y., ... & Xiong, N. N. (2016). Robust cyber–physical systems: Concept, models, and implementation. *Future generation computer systems*, *56*, 449-475. https://www.sciencedirect.com/science/article/am/pii/S0167739X15002071

Inkster, N. (2016). Information warfare and the US presidential election. *Survival*, *58*(5), 23-32. https://www.tandfonline.com/doi/abs/10.1080/00396338.2016.1231527?journalCode=tsur20

Ismailova, R. (2017). Web site accessibility, usability and security: a survey of government web sites in Kyrgyz Republic. *Universal Access in the Information Society*, *16*(1), 257-264.

Javaid, A. Y., Sun, W., Devabhaktuni, V. K., & Alam, M. (2012, November). Cyber security threat analysis and modeling of an unmanned aerial vehicle system. In *2012 IEEE Conference on Technologies for Homeland Security (HST)* (pp. 585-590). IEEE. https://ieeexplore.ieee.org/abstract/document/6459914/

Kadivar, M. (2014). Cyber-attack attributes. *Technology Innovation Management Review*, *4*(11).

Kalkan Küçüksolak, Ö. (2012). Güvenlik Kavramının Realizm, Neorealizm ve Kopenhag Okulu Çerçevesinde Tartışılması, Turan Strateji Araştırmalar Merkezi (TURAN-SAM), 4(14), 202-208.

Kane,R.K.(2010).Internet Governance in an Age of Cyber Insecurity, E-kitap: Council Special Report No. 56

Karabacak, B., Yildirim, S. O., & Baykal, N. (2016). Regulatory approaches for cyber security of critical infrastructures: The case of Turkey. *Computer law & security review*, *32*(3), 526-539.

Kay, S. (2004). Globalization, Power, and Security. **Security Dialogue,** 35(1), 9– 25.

Kaygusuz, K. (2007). Energy for sustainable development: key issues and challenges. *Energy Sources, Part B: Economics, Planning, and Policy*, *2*(1), 73-83.

Kenney, M. (2015). Cyber-terrorism in a post-stuxnet world. *Orbis*, *59*(1), 111-128.

Kılcı, H. B. (2020). Türkiye'nin Siber Güvenlik Politikaları. *Cyberpolitik Journal*, *5*(9), 113-140. http://www.cyberpolitikjournal.org/index.php/main/article/view/7

Kirshner, J. (2006). **Globalization and National Security.** NY: Routledge.

Klimburg, A. (2012). ***National cyber security framework manual.*** NATO CCD COE Publication,Tallinn. Erişim tarihi: 24.03.2020, http://www.ccdcoe.org/369.html

Kostyuk, N., & Zhukov, Y. M. (2019). Invisible digital front: Can cyber attacks shape battlefield events?. *Journal of Conflict Resolution*, *63*(2), 317-347. https://sites.lsa.umich.edu/zhukov/wp-content/uploads/sites/140/2017/07/KZ_IDF_v25.pdf

Kott, A. (2014). Towards fundamental science of cyber security. In *Network science and cybersecurity* (pp. 1-13). Springer, New York, NY. https://link.springer.com/chapter/10.1007/978-1-4614-7597-2_1

Kurnaz, S., & Önen, S. M. (2019). Avrupa Birliğine Uyum Sürecinde Türkiye'nin Siber Güvenlik Stratejileri. *International Journal of Politics and Security*, *1*(2), 82-103.

Lam, C. (2018). A slap on the wrist: Combatting Russia's cyber attack on the 2016 US presidential election. *BCL Rev.*, *59*, 2167. https://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=3696&context=bclr

Lawson, S., & Middleton, M. K. (2019). Cyber Pearl Harbor: Analogy, fear, and the framing of cyber security threats in the United States, 1991-2016. *First Monday*. https://journals.uic.edu/ojs/index.php/fm/article/view/9623

Levin, D. A. (2021). The State of K-12 Cybersecurity: 2020 Year in Review. *K-12 Cybersecurity Resource Center*. https://k12cybersecure.com/wp-content/uploads/2021/03/StateofK12Cybersecurity-2020.pdf

Lewis, J. A. (2005). Computer Espionage, Titan Rain and China. *Center for Strategic and International Studies-Technology and Public Policy Program, 1*.

Lin,H.S.(2010). Offensive Cyber Operations and the Use of Force, Journal of National Security Law and Policy, 4(63).

Liu, S., You, S., Yin, H., Lin, Z., Liu, Y., Yao, W., & Sundaresh, L. (2020). Model-free data authentication for cyber security in power systems. *IEEE Transactions on Smart Grid*, *11*(5), 4565-4568. https://par.nsf.gov/servlets/purl/10168664

Locke, J. (1997). *Locke: Political Essays*. Cambridge University Press.

Maschmeyer, L., Deibert, R. J., & Lindsay, J. R. (2021). A tale of two cybers-how threat reporting by cybersecurity firms systematically underrepresents threats to civil society. *Journal of Information Technology & Politics*, *18*(1), 1-20. https://www.tandfonline.com/doi/pdf/10.1080/19331681.2020.1776658

Maurer, T. (2011). Wikileaks 2010: A glimpse of the future. *Harvard Belfer Center*. https://www.belfercenter.org/sites/default/files/files/publication/maurer-dp-2011-10-wikileaks-final.pdf

Maynard, D. C. (2019). An Introduction to the History of the Internet: A Brazilian Perspective. In *The Internet and Health in Brazil* (pp. 15-26). Springer, Cham. https://link.springer.com/chapter/10.1007/978-3-319-99289-1_2

McKelvey, F., & Driscoll, K. (2019). ARPANET and its boundary devices: modems, IMPs, and the inter-structuralism of infrastructures. *Internet Histories*, *3*(1), 31-50. https://kevindriscoll.info/docs/mckelvey_and_driscoll-2018-ARPANET_and_boundary_devices.pdf

Miller, S., & Walsh, P. (2016). The NSA leaks, Edward Snowden, and the ethics and accountability of intelligence collection. *Ethics and the Future of Spying: Technology, National Security and Intelligence Collection*, *193*.

Moretti, E., Steinwender, C., & Van Reenen, J. (2019). *The intellectual spoils of war? defense r&d, productivity and international spillovers* (No. w26483). National Bureau of Economic Research. https://www.nber.org/system/files/working_papers/w26483/w26483.pdf

Morgenthau, H. J., & Kennan, G. F. (1955). The impact of the loyalty-security measures on the state department. *Bulletin of the Atomic Scientists*, *11*(4), 134-140.

Newman, R.E. (2000), "Computer and Network Security", http://www.cise.ufl.edu/~nemo/security/notes/network_security_standards.pdf (15.03.2021).

Newmeyer, K. P. (2015). Elements of national cybersecurity strategy for developing nations. *National Cybersecurity Institute Journal*, *1*(3), 9-19. http://publications.excelsior.edu/publications/NCI_Journal/1-3/offline/download.pdf#page=11

Okoro, C. B., Nebo, O. E., & Okoro, V. I. (2017). The Impact of Globalization on the World Economy in the Global Market and Production. *International Journal of Advanced Academic and Educational Research*, *13*(2), 105-115. http://eprints.gouni.edu.ng/1335/1/The%20Impact%20of%20Globalization%20on%20the%20World%20Economy.pdf

Oels, A. (2012). From 'securitization'of climate change to'climatization 'of the security field: comparing three theoretical perspectives. In *Climate change, human security and violent conflict* (pp. 185-205). Springer, Berlin, Heidelberg. https://is.muni.cz/el/fss/podzim2015/MEB401/um/Oels_2012.pdf

Özbenli, H. H., & Özlü, M., (2020). Siber Güvenlik Ekosisteminin Geliştirilmesi Modeli: Siber Güvenlik Kümelenmesi Model for cyber security Ecosystems: cyber security clusters.

Pajurek, M. (2017). Cybersecurity military entities of the United States of America. *Facta Simonidis, 10*(1), 163-178.

Pirinççi, F. (2010). Armament and War. Bursa: Dora Publications.

Reed, J. H., & Gonzalez, C. R. A. (2012). Enhancing smart grid cyber security using power fingerprinting: Integrity assessment and intrusion detection. In *2012 Future of Instrumentation International Workshop (FIIW) Proceedings* (pp. 1-3).

Robinson,p., (2008). Dictionary of International Security, Polity Press, ISBN-13: 978-07456-4027-3, ISBN-13: 978-07456-4028-0 (pb), p.1-4

Robinson, M., Jones, K., & Janicke, H. (2015). Cyber warfare: Issues and challenges. *Computers & security*, *49*, 70-94. http://www.tech.dmu.ac.uk/~rgs/ACECSR_publications/HelgeJanicke.pdf

Rosecrance, R., & Thompson, P. (2003). Trade, foreign investment, and security. *Annual Review of Political Science*, *6*(1), 377-398.

Sari, A. (2019). Turkish national cyber-firewall to mitigate countrywide cyber-attacks. *Computers & Electrical Engineering*, *73*, 128-144.

Senol, M., & Karacuha, E. (2020). Creating and Implementing an Effective and Deterrent National Cyber Security Strategy. *Journal of Engineering*, *2020*. https://www.hindawi.com/journals/je/2020/5267564/

Sheldon,J.(2012).Toward a Theory Of Cyber Power Strategic Purpose İn Peace and War, Cyberspace and National Security Threats, Opportunities and Power İn a Virtual

Singer, P.W. and Friedman, Allan (2015), Cyber Security and Cyber War, 1st Edition, Ankara: Buzdağı Publishing House, 57.

Sliwinski, K. F. (2014). Moving beyond the European Union's weakness as a cyber-security agent. *Contemporary Security Policy*, *35*(3), 468-486. https://repository.hkbu.edu.hk/cgi/viewcontent.cgi?referer=https://scholar.google.com.tr/&httpsredir=1&article=1007&context=gis_ja

Smith,C.S.(2012).The First World Hacker War, https://www.nytimes.com/2001/05/13/weekinreview/may-6-12-the-first-world-hackerwar.html ,adresinden (Retrived : 19.04.2021)

Stritzel, H. (2014). Securitization Theory and the Copenhagen School. In *Security in Translation* (pp. 11-37). Palgrave Macmillan, London. https://link.springer.com/chapter/10.1057/9781137307576_2

Szabó, Z. (2019). The effects of globalization and cyber security on smart cities. *Interdisciplinary Description of Complex Systems: INDECS*, *17*(3-A), 503-510.

Tatar, Ü., Çalik, O., Çelik, M., & Karabacak, B. (2014). A comparative analysis of the national cyber security strategies of leading nations. In *International Conference on Cyber Warfare and Security* (p. 211). Academic Conferences International Limited. https://www.proquest.com/openview/1fd94ace6d7f5c442fd1eb9f5764194d/1?pq-origsite=gscholar&cbl=396500

Terlizzi, M. A., Meirelles, F. D. S., & Viegas Cortez da Cunha, M. A. (2017). Behavior of Brazilian banks employees on Facebook and the cybersecurity governance. *Journal of Applied Security Research*, *12*(2), 224-252. https://www.researchgate.net/profile/Marco-Terlizzi/publication/320783357_Cybersecurity_governance_An_experiment_with_Brazilian_bank_employees_on_FacebookR/links/5a0aa25eaca272d40f414202/Cybersecurity-governance-An-experiment-with-Brazilian-bank-employees-on-FacebookR.pdf

Thomas, J. (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. *Thomas, JE (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. International Journal of Business Management*, *12*(3), 1-23.

Tirrell, W. K. (2012). United States Cybersecurity Strategy, Policy, and Organization: Poorly Postured to Cope with a Post-9/11 Security Environment. B.A. Thesis, Washington D.C: The George Washington University.

Tjalve, V. S., & Williams, M. C. (2015). Rethinking the logic of security: Liberal realism and the recovery of American political thought. *Telos*, *170*, 46-66. https://d1wqtxts1xzle7.cloudfront.net/46508393/Vibeke_Schou_Tjalve___MIchael_C_Williams-_Rethinking_the_Logic_of_Security__Telos__Spring_2015.pdf?1465996640=&response-content-disposition=inline%3B+filename%3DRethinking_the_Logic_of_Security_Liberal.pdf&Expires=1618330405&Signature=bYWMPOeSLteNx8GeEsqE8E-Y2GojHz-

l0c950ziHSDtfBfQGUPF1lfU9rt~wlzL9tkh8V~PKrRmX4t6K1N4CofuMIx7--LdcrOT8mw1KeA4PnBr1kcYJRzL~lHaqJXGg5Ae8-8VuIgdJmd-wscq3Nbl9DQR9r8ffVMPmk0JxEUlH5SSnradcB3X3Xw~DkVW4g1klnvmJ8~iaefzS-Wk1IQa9bawhgBIYFoUlboWAIlllCkfwr9VC0zGwk49otmJFMLbTNmlPxU5PQG7~oLM~K~lJQpcz3ulg4kdpsRuDOTjET7OEcGtIlm7Mu7L3Fl5bb0m3MSKmbTRdRqzeht71dQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

T.R. Ministry of Transport, Maritime Affairs and Communications, Information Security Association (2012, June) "National Cyber Security Strategy: A strong and leading bit for Turkey in the cyberspace of 2023"

Uğrasız, B. (2003). “Two Different Approaches in International Relations: Idealism and Realism ”, Dokuz Eylül University Institute of Social Sciences Journal, 5(2), 139-145.

Uğurlu G., (2014), International Relations Theories Basic Concepts, Kripto Publishing House, 1st Edition, January.

Ünver, G. N. (2017). Ulusal Siber Güvenlik Strateji Belgelerinde İnsan Hakları. *Cyberpolitik Journal*, *2*(3), 101-126.

Verble, J. (2014). The NSA and Edward Snowden: surveillance in the 21st century. *ACM SIGCAS Computers and Society*, *44*(3), 14-20. http://people.uncw.edu/guinnc/courses/Spring20/TheTwoCodes/Readings/SnowdenBackground.pdf

Vest, C. M. (2007). *The American research university from World War II to world wide web*. University of California Press.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97-102. https://www.profsandhu.com/cs6393_s19/Solms-Niekerk-2013.pdf

Waltz, K. N. (1988). The origins of war in neorealist theory. *The Journal of Interdisciplinary History*, *18*(4), 615-628.

Waltz, K. N. (1990). Realist thought and neorealist theory. *Journal of International Affairs*, 21-37.

Waltz, K. N. (2000). Structural realism after the Cold War. *International security*, *25*(1), 5-41.

Waltz, K. (2004). Neorealism: Confusions and criticisms. *Journal of Politics and Society*, *15*(1), 2-6.

Warner, M. (2020). US Cyber Command's First Decade. *A Hoover Institution Essay*. *Aegis Series Paper*, (2008). https://www.hoover.org/sites/default/files/research/docs/warner_webready.pdf

Watson, S. D. (2012). 'Framing'the Copenhagen School: Integrating the literature on threat construction. *Millennium*, *40*(2), 279-301. https://journals.sagepub.com/doi/abs/10.1177/0305829811425889

Wendt, A. (1995). Constructing international politics. *International security*, *20*(1), 71-81.

Wendt, A. (1999). *Social theory of international politics* (Vol. 67). Cambridge University Press.

Wirtz, J. J. (2017). The Cyber Pearl Harbor. *Intelligence and National Security*, *32*(6), 758-767. https://d1wqtxts1xzle7.cloudfront.net/54660138/The_Cyber_Pearl_Harbor.pdf?1507502095=&response-content-disposition=inline%3B+filename%3DThe_Cyber_Pearl_Harbor.pdf&Expires=1621877195&Signature=BfM4ocyx3fyJE3-XVTVb~7OKU6a8qvlw5H5rQo1OR2vU2~-B2dsEbpDtmNJ-cDWkM~gNGr~QB2fTltOQxnF1bmZn6BMEhZRAhgUh~YgMZHP8DR9E2sMBhIJ2FflBcwy3AGTsaycjjR4LoY1QCzmMU0AV1PJnZYj-xTmdMnuT8j9YEsT31DyVq2tHr5j3zQvELlcjlG09-hGwZC1he91eQ0J8qTymd9Vx4DHwCJUwou1b94PVmtfc3LoEYxfGKF-lYvdMTDUsAawnOwCtGrRxq63W~OxOO4MtLoZSzjRaZfAbDSgIjMzwNgrtReLfD7unrkjxqQ8Rvcucm6VIIEg1FA__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

WH (2003). The National Strategy to Secure Cyberspace. Washington: The White House. Accessed 17.04.2021, https://www.us-cert.gov/sites/default/files/ publications/cyberspace_strategy.pdf

Yeboah-Boateng, E. O. (2013). *Cyber-Security Challenges with SMEs in Developing Economies: Issues of Confidentiality, Integrity & Availability (CIA)*.

Institut for Elektroniske Systemer, Aalborg Universitet.
https://vbn.aau.dk/ws/files/316448052/PhD_Thesis_Boateng_Final_for_print.pdf