THE REPUBLIC OF TURKEY

BAHCESEHIR UNIVERSITY

REINFORCE CYBER SECURITY IN TURKEY

Master's Thesis

MERT SEFA TAŞ

ISTANBUL, 2019

THE REPUBLIC OF TURKEY

BAHCESEHIR UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

CYBER SECURITY

REINFORCE CYBER SECURITY IN TURKEY

Master's Thesis

MERT SEFA TAŞ

Supervisor: ASSIST. PROF. DR. BETÜL ERDOĞDU ŞAKAR

ISTANBUL, 2019

THE REPUBLIC OF TURKEY
BAHCESEHIR UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
CYBER SECURITY

Name of the thesis: Reinforce Cyber Security in Turkey
Name/Last Name of the Student: Mert Sefa TAŞ
Date of the Defense of Thesis: 27/05/2019

The thesis has been approved by the Graduate School of Natural and Applied Sciences.

Asst.Prof.Yücel Batu SALMAN
Graduate School Director

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

Asst.Prof.Ahmet Naci ÜNAL
Program Coordinator

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

Examining Committee Members	Signature
Thesis Supervisor Asst.Prof.Betül ERDOĞDU ŞAKAR	----------
Member Asst.Prof.Ahmet Naci ÜNAL	----------
Member Asst.Prof.İnci Zaim GÖKBAY	----------

ABSTRACT

REINFORCE CYBER SECURITY IN TURKEY

Mert Sefa TAŞ

Cyber Security

Thesis Supervisor: Assist. Prof. Dr. Betül ERDOĞDU ŞAKAR

May 2018, 27 pages

In this era that we can describe it as digital age, people are connected to the world through the devices that they have. There are approximately 20 billion of devices connected to the internet that people use for it. With the development of the digital ecosystem so fast, it brings many conveniences that are essential for our lives. However, digitalization brings serious and new cyber threats that a few people can understand or can predict although many remarkable opportunities that happened or may happen to people through digitalization.

In order to deal with the cyber threats, nations must predispose the competence in cyber security field to the world that has been digitalized. Turkey is behind the other European countries in the cyber security competence. While Turkey ranks forty-third in the Global Cyber Security Index (2017) ranking that has been made by Internet and Telecommunication agent ITU and according to the study that has been made by Eurostat, the corporates in Turkey have digital security policy, only 20% identified as official / correct. Turkey is behind the European countries in the cyber competence and in addition to this, it may be said that Turkey is one of the focus targets of the cyber incidents / attacks. In the datum of the security report that has been published by Trend Micro that belong to the first part of 2016, states that all ransomware attacks have been increased in the rate of 172, that our country is the one that experiences ransomware attacks the most in Europe, as to world, Turkey takes part as third after USA and Brazil.

This study aims that to plan the necessary steps in order to Turkey can grow strong in cyber security field, to perform it and to manage it.

Keywords: Cyber Threat, Digital Ecosystem, Digitalization, Cyber Security, Ransomware

ÖZET

TÜRKİYE'DE SİBER GÜVENLİĞİ GÜÇLENDİRMEK

Mert Sefa TAŞ

Siber Güvenlik Yüksek Lisans Programı

Tez Danışmanı: Dr. Öğr. Üyesi Betül ERDOĞDU

Mayıs 2018, 27 sayfa

Dijital çağ olarak tanımlayabileceğimiz bu dönemde, insanlar ellerinin altındaki cihazlar sayesinde dünya ile etkileşim halindedir. Günümüzde insanların bu amaçla kullandığı internete bağlı olarak çalışan yaklaşık 20 milyar cihaz bulunmaktadır. Dijital ekosistemin bu hızla gelişmesi hayatımızın vazgeçilmezleri haline gelen birçok kolaylığı da beraberinde getirir. Ancak dijitalleşme ile birlikte insanların hayatına giren veya girebilecek kayda değer birçok fırsat olmasına rağmen dijitalleşme, çok az kişinin anlayabileceği ya da öngörebileceği yeni ve ciddi siber tehditleri de beraberinde getiriyor.

Siber tehditler ile başa çıkabilmek amacıyla ülkelerin siber güvenlik alanındaki yetkinliklerini dijitalleşen dünyaya uygun hale getirmeleri gerekmektedir. Türkiye siber güvenlik yetkinliği konusunda diğer Avrupa ülkelerinin gerisinde yer almaktadır. Internet ve Telekomünikasyon ajansı ITU'nun yaptığı Global Cyber Security Index (2017) sıralamasında Türkiye kırk üçüncü sırada yer alırken, Eurostat tarafından yapılan araştırmaya göre ise Avrupa'da ortalama %30 iken Türkiye'de kurumların sadece %20'si resmi / düzgün bir şekilde tanımlanmış dijital güvenlik politikasına sahiptir.
Siber yetkinliklerin Türkiye'de Avrupa ortalamasının gerisinde olmasına ek olarak, Türkiye yaşanan siber olaylar / saldırıların odak noktasında olan ülkelerden bir tanesi olduğu söylenebilir. Trend Micro tarafından yayımlanan 2016 yılının ilk yarısına ait bir diğer güvenlik raporundaki veriler, tüm dünyada fidye yazılım saldırılarının yüzde 172 oranında arttığını, ülkemizin Avrupa bölgesinde fidye yazılım saldırılarını en fazla yaşayan ülke olduğunu, dünyada ise ABD ve Brezilya'dan sonra üçüncü sırada yer aldığı ifade edilmektedir.

Bu çalışma, Türkiye'nin siber güvenlik alanında güçlenmesini sağlayacak adımların tasarlanması, uygulanması ve yönetilmesi için gerekli olan adımları belirlemeyi hedeflemektedir.

Anahtar Kelimeler: Siber Tehdit, Dijital Ekosistem, Dijitalleşme, Siber Güvenlik, Fidye Yazılım

CONTENTS

ABBREVIATIONS

ADSL	:	Asymmetric Digital Subscriber Line
CIA	:	Confidentiality, Integrity, Availability
CIRT (SOME)	:	Cyber Incidents Response Team
CSIS	:	Center for Strategic and International Research
DDOS	:	Distributed Denial of Service
EC	:	European Commission
EEC	:	European Economic Community
EU (AB)	:	European Union
EUCTF	:	European Cybercrime Task Force
ICS	:	Industrial Control System
ICTA (BTK)	:	Information and Communication Technologies Authority
IP	:	Internet Protocol
ISO	:	International Standards Organization
IT	:	Information Technologies
ITU	:	International Telecommunication Union
MACM (UDHB)	:	Maritime Affairs and Communications Ministry
METU(ODTÜ)	:	Middle East Technical University
NATO	:	North Atlantic Treaty Organisation
NCERC (USOM)	:	National Computer Emergency Response Center
NIO (MIT)	:	National Intelligence Organization
OAS	:	Organization of American States
OECD	:	Organization for Economic Co-operation and Development
TÜBİTAK	:	The Scientific and Technological Research Council of Turkey
UN	:	United Nations
US	:	United States

1. INTRODUCTION

1.1 CYBER SECURITY IN THE DIGITALIZED WORLD

In the statements given to individuals in the information age societies, it is stated that individuals who can access to electronic tools and understand the technology will be information rich. In this structure, individuals need to access information and use information. The individuals who know, understand and use technology are information age individuals. Individuals who are distant from technology in the information age will not be able to adapt to the social life since they will be deprived of knowledge. The individual-technology convergence required by social life requires increased communication efficiency for the use, dissemination and access of information (Folkerts, Lacy, 2004: 319).

The word "cybernetic" comes from the root of "cybernetic". Cybernetics means controlling and managing self-balance. The term "cyber" can be defined as the exchange of information with each other in the form of governance of human life and machinery. Nowadays, it is mostly used as virtual access or virtual life. Depending on the advancement of technology, the activities are carried out to ensure the security of cyber life. It covers the virtual world including policies, guidelines, risk management activities, trainings, software and hardware security systems implemented for the protection of valuable information and system assets that are open to cyber environment. As a result of digitization and digitalization, the information became independent of the physical environment on which it was kept. Data is sent to data servers in different areas via network systems in seconds. Cyber security vulnerabilities can cause irreparable losses on an individual, institutional and country scale. For this reason, cyber security measures should be established in all relevant critical information and infrastructure systems, especially military, public, private and private enterprises (Hekim, Hakan, 2015: 58).

Any cyber-attack attempt that could harm or damage the security of personal or corporate data is called a "cyber threat". For example; stopping server and web service (DDOS), enterprise and personal identity, such as attempts to damage, viruses, trojans, social media data theft and online fraud (Jeffrey, Carr, 2011: 23).

2. LITERATURE REVIEW OF DIGITALIZATION & CYBER SECURITY

2.1 WHAT IS DIGITALIZATION?

Communication, an inseparable part of human nature, was born with the need to transfer individuals' feelings, thoughts, accumulations to each other, and through this way, people continued to develop and develop their relations while also developing the phenomenon of communication. Communication, which has been in the right direction from oral to written, has brought a different impetus to technology communication developed in the last years by the effect of electrical system. The period from the development of language and vocabulary in the history of mankind to the development of today's complex electronic and digital mass communication systems is not as straight and linear as the evolutionist approach claims. The history of humanity is a complex and dialectical process of quantitative developments, which at certain points is caused by the jumps that lead to qualitative transformations through social revolutions. People have found the word, the official, the article with the effect of production (Cavelty, 2008: 93).

In time, they have developed printing techniques, photograph, telegraph, telephone, radio, cinema, television and computer systems. Thus, the change and development in communication did not progress in a parallel line, and the longer process started to shorten as it reached the present day. The internet, which developed especially with computer technology, transformed communication and change according to previous periods. The Internet is an international communication network system where many computers can be connected. The term internet is composed of the words "international" and "network". This international network consists of computers with high-speed communications that are permanently connected to each other. It is the last revolution of developing technology very rapidly in recent years (Sevda, 2015: 142).

At first, the Internet addressed military purposes. Then spread to the academic environment. Thus, a very important technology was created in the academic environment to exchange information. Over time, the Internet has spread to a wider community and the public has begun to use it. First academics and universities are adopting the Internet. And the first computers that speak between them are computers of universities in different cities. Then universities of different countries participate in this

structure. In 1972, the most popular application of the Internet, e-mail application is being used. In those years, the Internet is introduced to the public and the process of civilization is accelerated (Yeding, Akman, 2002: 13).

New media is one of the most important actors on the Internet began to develop in the early 1990s in Turkey. Scientific and academic institutions such as TÜBİTAK, METU and Boğaziçi University have developed and expanded the Internet. Internet access in Turkey began in 1994. The fact that the internet was of US origin naturally caused content to be in English. In this context, the shortage of Turkish content has been raised. The first Turkish publication on the Internet is the publication of Aktüel magazine in 1996 (Yengin, 2012: 349).

Briefly, the technology advancing rapidly has reduced both the distance between people and time, so there have been changes and developments in every field-especially communication. Due to the narrowing of the distance, the developments spread more widely due to the narrowing of time. Especially, it has started a new revolution in computer technology and internet communication. Because of time, data such as audio, video and video can be transferred to the internet so that a system that contains all kinds of communication has occurred. Also, if we look at the previous forms of communication, telegram, letter or telephone are one-to-one communication, radio and television is the way of communication with many people. However, when we look at the internet, we see a form that includes all kinds of communication that allows both individual and multi-person communication (Singer, Friedman, 2015: 58).

2.2 CYBER SECURITY

As a result of the rapid development in information and communication technologies and the spread of services provided by these systems and technologies in all areas, the role of information and communication technologies in political, social, economic and military fields has increased. In the light of all these developments, many people, institutions and organizations have started to use information and communication technologies at the highest level and have become an integral part of all activities. As a result, information and communication technologies have become vital for countries' critical infrastructure sectors (Albrechts, 2007: 56).

Recently, organized crime and terrorist organizations have been using their information and communication technologies in planning their activities, training, sharing information and propaganda activities in cyberspace. Cyber security and defense activities have increased the importance of individuals, institutions, organizations and states due to the attacks and threats. The target of cyber attacks and threats, if damaged and / or destroyed, has vital facilities, networks, services and assets that will have a negative impact on the safety and health of the citizens, their economic well-being or the provision of public services. Although these vary from country to country, they are mostly infrastructures for defense, finance, energy, transportation, electronic communication, health, education, nuclear facilities and basic public services and all these elements are defined as critical infrastructure (Cavelty, 2008: 111).

In recent years, institutions, organizations, international organizations and states in the world have accelerated their cyber security and defense activities in order to protect their critical infrastructure sectors and ICSs against these threats. In order to provide cyber security and defense, the development of administrative, technical and legal capacity on a national scale, the production of national software and equipment, and the use of national security products as important as possible in the critical infrastructure sectors have gained importance. In order to minimize the effects of cyber-space attacks, it has been necessary to identify critical infrastructure sectors, to ensure their security and to develop technological and legal measures (Çeliktaş, 2016: 42).

The concept of cyber security, which is of obvious importance nowadays, is one of the most popular issues in the future. As our dependence on information and communication technologies continues and continues to increase, cyber security will continue to remain one of the priority security areas of individuals, institutions, international organizations and states. Cyber security by the World Telecommunication Union (ITU), the United Nations (UN) body for communication, information and communication technologies; actions, trainings, applications and technologies. In the cyber space, organization and users' assets, individuals, computing equipment, infrastructures, applications, services, communication systems and cyber space is transmitted and / or stored information (ITU, 2008: 2).

It is called cyber security to protect the virtual systems against all kinds of threats, attacks and dangers that prevent the operation of information systems and networks or prevent them from functioning (Akleylek, Tok, 2011: 69).

Cyber security is also to determine the security risks and weaknesses of cyber space and to take necessary measures for security measures to protect the assets of institutions, organizations and users from unwanted threats and dangers. According to 2016-2019 National Cyber Security Strategy (2016: 7), cyber security, protecting cyber space-forming information and communication technologies from cyber attacks, ensuring the confidentiality, integrity and accessibility of the information processed in this digital environment, identifying attacks and cyber security incidents, the reaction mechanisms against the determinations and then the return of the systems to their previous state.

Protecting the confidentiality and privacy of information processed, stored and transferred within the information systems, maintaining and maintaining data integrity and access to information, access speed and quality, and ensuring the continuity and continuity of the system are the main objectives of information security and they are accepted as the basic principles of cyber security (Sağıroğlu, 2011; Atalay, 2012: 43). The concepts of confidentiality, accessibility and integrity are also referred to as the "CIA triad" (Singer, Friedman, 2015: 57).

Cyber security aims at minimizing the vulnerabilities and vulnerabilities caused by system administrators, user or manufacturer errors, as well as combating all kinds of cyber threats or cyber attacks coming from inside or outside the organization, as well as security risks (BTK, 2009 3).

Cyber defense is defined as the whole of the measures that should be taken to prevent the negative effects of attacks and threats in cyber space on communication, electronic and information systems during any attack of the enemy and to ensure the survival of the systems (Keleştemur, 2015: 315,316).

2.3 DIGITALIZATION AND CYBER SECURITY

Computer technologies and systems, which are information systems, have become one of the important tools of daily life. Situations such as access to information from the Internet through direct computer use, the realization of professional or daily tasks through

computers, and even the use of state-of-the-art computers are examples of common use. The reflection of information and communication technologies in public administration can be seen as "e-government" studies. In central government and local governments, legislative, executive and judicial organs, projects are underway to benefit from these technologies rapidly. Developed countries are prepared to provide almost all information and services offered by the public sector through these technologies. The reflection of information and communication technologies in public administration can be seen as "e-government" studies. The provision of state services by cyber systems, the storing and processing of state and citizen information and documents in these systems, brings with them cyber risks and threats and raises the problem of ensuring the security of these information and documents. These virtual archives where systematic information and documents of state and citizen are stored and used may be considered as a critical infrastructure. In this respect, these systems should be protected in the context of cyber security (Sadioğlu, Yıldız, 2007: 348).

Controlling the risks of information and communication technologies within the limits of cyber security and improving the resistance of these infrastructures against cyber attacks are among the main targets of cyber security strategies of countries (Klimburg, 2012: 56). As in the current period, the society will increasingly have industrial control systems that operate with critical infrastructures that depend heavily on systems connected to computers and networks. These industrial control systems include chemical industry, intelligent systems, energy networks, cities, household systems, agriculture, medicine, automotive, etc. widely used in the fields. On the other hand, power plants, plant irrigation systems and smart grids are among the other critical infrastructures based on information and communication systems (Genge, 2012: 1146). These critical infrastructures are among the first regions to be targeted in the traditional warfare method to make countries weaker.

Cyber attacks and cyber threats also target these critical infrastructures. Furthermore, cyber attacks can cause not only cyber problems (programs collapse, closure of computers, etc.) but also physical problems, as they were in previous periods, because of their damage to these critical infrastructures. Locking of transportation, gas and water network stops and then people deprived of them can lead to illness or death. More serious

and critical than these, nuclear program infrastructures can also be the target of cyber attacks as infrastructures that operate with industrial control systems (Genge, 2015: 1).

2.4 CURRENT STATUS OF CYBER SECURITY IN TURKEY

2.4.1 Qualifications

Have information about the state of cybersecurity efforts in Turkey as the first to be, which is the first strategy document related to cyber security, "National Cyber Security Strategy and the 2013-2014 Action Plan" studies on cyber security held until the approval of the will be announced shortly, followed by Within the framework of strategic action headings of the plan, the distribution of cyber security duties and responsibilities, public institutions and organizations, universities and civil enterprises, activities and studies carried out to date will be examined (ITU, 2008: 11).

After the announcement of the activities and operation of Turkey, which is the most current strategy documents related to cyber security, transportation in April 2016, Maritime Affairs and Communications Ministry (UDHB) issued by, 2013-2014 The degree of activity in the Action Plan, and considering the difficulties created for the future evaluations, which contain important on behalf of Turkey, 2016-2019 National Cyber Security Strategy will be examined (Kobara, 2016: 787).

The number and impact of cyber attacks and threats increase with the diameter of the world's countries and international organizations in the power and capacity to increase cyber security efforts, Turkey is also caused to accelerate its efforts in this regard. Therefore 2009 in the first official document about the nature of cyber security in Turkey "National Cyberspace Security Policy" was established. While the main headings of this policy are threats, openings, basic principles and virtual environment security steps, there is no strategy or action plan that determines the implementation steps of the issues in the policy document (Kırdı, 2015).

The execution of works made cyber security in Turkey and is responsible for the execution UDHB, while the approval of the decision on whether to run Cyber Security Board is responsible (Uslu, 2015). Cyber Security Council decision on the establishment of Turkey's most important strategic steps taken so far on cyber security and to this day is collected up to 4 times, a number of decisions were taken. The most important among these decisions are listed below.

i. The first National Cyber Security Strategy of Turkey and the creation of the 2013-2014 Action Plan,
ii. Determining the critical infrastructure sectors and conducting the studies on this by UDHB within the framework of "National Cyber Security Strategy Document and 2013-2014 Action Plan",
iii. Implementation of the Public Net project for the transmission of data over a secure network between the public institutions,
iv. Adoption of the Duties, Working Procedures and Principles of the Cyber Security Council.

Following the first Cyber Security Council meeting held on 21 December 2012, the National Cyber Security Strategy and 2013-2014 Action Plan were published in the Official Newspaper on 20 June 2013 under the coordination of UDHB with the contributions of institutions, organizations and NGOs (Çakmak, Demir, 2009: 30).

The National Cyber Security Strategy and the 2013-2014 Action Plan aim to ensure the security of the information and communication technologies of the critical infrastructure sectors operated by the public or private sector with information and systems that store or produce services and data of institutions and organizations, and to minimize the impact of cyber security incident assigns tasks to different institutions and organizations.

The Action Plan encompasses 29 action items, 86 sub-action items and 31 responsible, relevant institutions, organizations and organizations under 7 main headings. The plan includes 7 main strategic action topics.

a) Legal Regulations,
b) Carrying out studies that will help the process,
c) Establishment of National Cyber Incidents Response Organization,
d) Strengthening of National Cyber Security Infrastructure,
e) Training Human Resources in Social Security Area,
f) Developing Domestic Technologies in Cyber Security,
g) Extending the Scope of National Security Mechanisms

(National Cyber Security Strategy and 2013-2014 Action Plan, 2013: 4890).

While the Action Plan defines the works planned to be carried out in 2013-2014 period, it also includes training and awareness-raising activities which should be carried out continuously. In the Action Plan, it is stated that the need to update according to the

changing requirements, the developing technology and needs and the demands coming from the public and private sector. Indeed, in April 2016 2016-2019 National Cyber Security Strategy Document published by UDHB Turkey's new National Cyber Security Strategy was formed.

2.4.2 Cyber Attacks

Attacking, decommissioning, feeding, malware damage, social engineering, communication network listening, data playback and modification of critical infrastructure sectors, disrupting the internet pages of government or business organizations, stealing, deleting, disclosing or changing confidential information in the system often planned and coordinated attacks in cyber space into the communication infrastructure or information systems of the target person, company or organization are called cyber attacks (Çakmak & Demir, 2009: 29-30).

According to the 2016-2019 National Cyber Security Strategy (2016: 7), cyber attack is a deliberate attempt by persons or systems in any part of the cyber space to eliminate the privacy, integrity or accessibility of information and communication technologies in national cyber space. Cyber attacks can be carried out by individual hackers, organized crime groups, espionage activists, terrorists, foreign intelligence organizations or the hostile country in a coordinated and coordinated way, and unaware of the system by unconscious users.

Nowadays, the information is spreading rapidly, the use of the elements of the cyber space is spreading rapidly, as a result of which information, information and communication technologies, the critical infrastructure sectors are increasing attacks. In addition, recently, the technical knowledge required by the attackers is decreasing day by day, while the complexity and harms of cyber attack techniques are increasing.

2.4.3 Cyber Security Institutions

Cyberspace as a regulation, which focused on the security Cabinet's 11/06/2012 dated 2012/3842 numbered National Cyber Implementation of Security Studies, Management and Decision Regarding the Coordination 10.20.2012 dated 28447 numbered Official

Newspaper published enactment, Turkey ' is the updating of the Electronic Communication Law numbered 5809, which is the basic law for electronic communication, in cyber security focus. One of the important benefits of the decision is the determination of the measures to be taken regarding cyber security, prepared plans, programs, reports, procedures, principles and standards to approve and their implementation, to ensure the coordination (Decision 3842, art.4) is established Cyber Security Council (Akin, 2015: 99).

The Cyber Security Council is an important board in terms of high-level representation as required by the members' position and authority. The Council, Undersecretary of the Ministry of Foreign Affairs, Interior, National Defense, Transport, Maritime Affairs and Communications, under the chairmanship of the Minister of Transport, Maritime Affairs and Communications, Undersecretary of Public Order and Security, Undersecretary of National Intelligence Organization, Chief of Communication Electronics and Information Systems, Information Technologies and Communication Chairman of the Authority, Turkey Scientific and Technological Research Council President, Financial Crimes Investigation Board Chairman, Telecommunications Transport and Communications Vice President, consists of Maritime Affairs and Communications minister of ministries and senior managers of public institutions to be determined.

With the Decree No. 2012/3842 of the Council of Ministers, the Ministry of Transport, Maritime Affairs and Communications has the following duties related to cyber security (Decision 3842, art.5):

i. To prepare policies, strategies and action plans for the national cyber security.
ii. To prepare procedures and principles for ensuring the security and confidentiality of information and data of public institutions and organizations.
iii. To monitor the establishment of technical infrastructure in public institutions and establishments in ensuring the national cyber security, to ensure that the effectiveness of the applications are verified and tested.
iv. Promote the use and use of all national solutions and cyber-attack intervention tools in the provision of National Cyber Security.
v. Providing security certificates by determining the procedures and principles of real and legal persons working in the field of information security training, testing and solution production.

vi. To carry out the secretarial service of the Cyber Security Council.

As it is seen, the decree, as well as the establishment of a board to carry out concrete works on behalf of cyber security, also imposes specific duties on cyber security to the relevant ministry. In this regard the decree, an indication that occurs in the plane of the cyber security policy in terms of perception of Turkey would be counted. In fact, even though this perception does not include the formation of cyber security, ın information security iber has started to take place in the late 1990s and early 2000s. The biggest indicator of this is the National Information Security Organization, which is under the coordination of the Ministry of National Defense, but is not intended to be established with the Draft Law on the National Information Security Organization and Duties.

As stated by Bıçakçı et al., the Prime Minister, who is responsible for managing the country's information security policies under the Prime Minister's Office, is the Prime Minister, the Minister of Justice, National Defense, Interior, Foreign Affairs, Transport, Industry and Trade, and the Secretary General of the National Security Council. The Head of Electronic and Information Systems envisaged the establishment of a National Information Security Supreme Council to be formed by the Undersecretary of the National Intelligence Organization (MIT) and TÜBİTAK (2016: 32). The draft also designed the establishment of the National Information Security Authority. The Presidency was formed in the form of a Plan Program and Coordination, Information Security, Cryptology, Information Support, Supervision and Information Departments. It was envisaged that the draft law to be embodied in these proposals would be approved by the middle of 2003, but the bill was disbanded as a result of the failure to settle the bill. Considering the envisaged members of the Council, it is remarkable that the current ministries and state institutions have largely resembled the Cyber Security Council. In contrast to the cyber security board, the Telecommunication Communication Presidency, which was established in 2006 and closed in 2016, was not included in the National Information Security Organization, which was designed by the Information and Communication Technologies Authority established in 2000. On the other hand, considering the organization under the coordination of the Ministry of National Defense and under the chairmanship of the Prime Minister, it indicates that information security is directly perceived within the general defense function. The Cyber Security Council, which was established in 2012, was established under the coordination of the Ministry of

Transport, Maritime Affairs and Communications, and as the chairman, the Minister was appointed as the Minister. In this respect, it is possible to say that cyber security perception is positioned on a more specific platform in Cyber Security Council and the authority has been left to a more specific area of expertise (Ministry of Transport, Maritime Affairs and Communications) (Kılıç, Recep, 2014: 45).

2.5 CURRENT SITUATIONS OF CYBER SECURITY MEASURES OF OTHER COUNTRIES

The best sources of information security policies of EU countries are legal regulations. Legal arrangements mean that the agreed policies have been implemented. It is not possible to predict when and in what dimension the information is considered as a commodity. A complete prevention of the production and distribution of a malicious code is not possible, despite all legal or technical measures being taken. However, information security policies are determined under the umbrella of the EU on how to evaluate the act that occurs after the use of the code, and studies are underway to ensure that the legal regulations are not behind the social developments. Each country also harmonizes its domestic law with the directives and international conventions. A number of directives and recommendations have been prepared and published on the issue of ensuring information security, with a priority on the protection of personal data and cyber security by the EU. The main EU directives and recommendation decisions, including information security issues, are as follows;

i. Resolution 92/242 / EEC on Information Security
ii. Directive 95/46 / EC on the Protection of Personal Data and the Protection of Individuals on the Free Movement of Personal Data
iii. Directive 97/66 / EC on the Processing of Personal Data and the Protection of Privacy
iv. Electronic Trade Directive 2000/31 / EC
v. Directive 2002/58 / EC on the Protection of Personal Privacy in the Electronic Communication Sector
vi. 1151/2003 / EC Decision on Combating Unlawful and Harmful Content on Broad Network

vii. Decision to Switch to Secure Internet Usage No. 854/2005 / EC

viii. Directive 2006/24 / EC on the Preservation of Data Obtained on Public Communication Networks or during the Presentation of Public Electronic Communication Services, EC Directive 95/46 / EC of 24 October 1995; data protection law. Directive 97/66 / EC is complementary to the telecommunications field of Directive 95/46 / EC. The Directive 2002/58 / EC, which complements the Directive 95/46 / EC in the field of electronics, also provides stronger protection than the 2000/31 / EC electronic trade directive.

Apart from these, there are also recommendations made to improve user awareness. Illegal and harmful content on the internet in 1997 and 1999, the EU's approach to network and information security in 2003, attacks on information systems in 2005, the strategy of establishing a secure information society in 2007 and information and communication technologies in 2008 Recommendations for protecting children are some of the most important recommendations. Green Paper is one of the important documents that sheds light on EU information security policies in addition to directives, conventions and recommendations. The green paper is prepared by the EU Commission to discuss a specific issue across the EU and to ensure that the subject is matured through ideas. The green paper is not binding. However, due to its intention, it is an important step for the policies to be determined (European Union Information Security Policies). The green paper, published by the European Commission in November 2005, is one of the important documents for the creation of information security policies (European Commission, 2005).

In this document, the protection of critical information and communication infrastructure (information system network infrastructure, telecommunications, internet, satellite, computer, software, etc.) from the impact of any disaster that may occur measures have been allocated to minimize the damage. Information security policies in the EU are shaped by some basic issues. These are the interaction of information and communication technologies with society (e-commerce, etc.), activities carried out on the internet, data ownership rights and protection of personal data. Some of the EU directives are further debated and on the agenda due to the impact of these key issues on information and communication technologies and on the impact of the emerging information and communication technologies on the economy (King and Raja, 2012: 312).

The content of the data protection directive 95/46 / EC and the drafting of a new data protection directive, which is one of the most important elements of EU information security policies and regulations, provide important clues about the general approach to this issue. The EC directive 95/46 / EC of 24 October 1995 is an arrangement aimed at maximizing the privacy of persons and at the same time allowing the free movement of personal data. In the Directive, personal data is expressed as all information relating to specific or identifiable natural persons. In addition, the data that will be considered as personal data should contain a password on it, an identification number, the identification of the physical, mental, physiological, cultural, economic or social identity, and the distinctive information of a particular or identifiable person. The objective of the Directive is to ensure that personal privacy is protected by the member states in respect of the processing of personal data, the fundamental rights and freedoms of persons. States shall not interfere with the flow of personal data between Member States in the course of their conservation procedures (European Council, 1995).

It is aimed to provide security and access balance, which is one of the basic principles in providing information security with the article that prohibit the flow of data between the member countries. With directive 95/46 / EC, service providers are obliged to comply with certain rules, providing users with fundamental rights in protecting personal data. The Directive restricts the collection, recording, use and disclosure of personal information from companies and organizations without any legitimate or explicit justification. The data subject should be informed about how the data is processed, how it is stored and who is being accessed, and at least the personal information (health information etc.) should be recorded. In addition, it is necessary to ensure the security of the information and to protect it from unauthorized access. Article 25 of Directive 95/46 / EC prohibits the transfer of personal information of the user to countries outside the EU economic area that do not provide sufficient information security. It is stated that the evaluation of the adequacy of the protection level will be made by taking into consideration all the security conditions surrounding the data transfer activity. The factors that will be given special importance in the evaluation include the country where the data will be transferred, the legal arrangements, the structure of the data and the purpose of the activity. All member states are obliged to take the necessary measures against the third country, where the Commission has determined that it does not have adequate levels of

protection. Article 25 has some exceptions. These (item: 26) are exceptions that include special circumstances such as the fact that the data subject has explicit consent, requires the establishment of statutory rights or requires the public interest and is required to protect the vital interests of the data subject. In the European Commission decision 2000/520 / EC of 26 July 2000, in accordance with Directive 95/46 / EC, the Safe Harbor Agreement of the company to transfer the information from the European Economic Area to the United States is an exceptional case (European Commission, 2004). The Safe Port Agreement has made it necessary to inform the users about the personal data they collect and the purpose for which they will use this information and to take all necessary information security measures. In order to become a member of this agreement, the companies have to get approval from all EU member states separately, and they also support the increase of their dignity and reliability. For all companies operating within the EU, legal obligations are compulsory. Based on this, users are also entitled to data processing (including non-EU space) for information processing and information sharing with other companies (European Council, 1995).

Directive 95/46 / EC imposes new responsibilities on service providers to ensure that the data subject is informed about the data and to establish new servers within the EU. Companies that collect and process personal data through the services provided must fulfill these responsibilities. Existing data protection and consumer protection laws, which are valid within the EU, are insufficient to address concerns about secrecy, in particular (Filippi and Belli; 2012). Due to the advancement in information technologies and internet, the use of social networking sites and the change in information storage methods have made it necessary to make updates on the protection of information. Today, many transactions on the internet (online booking, purchase of products, various subscriptions etc.) require sharing with personal information such as first name, ID number, telephone, address, e-mail, date of birth. Therefore, there is a need for legal arrangements covering new areas. Directive 95/46 / EC on how to update the Personal Data on IP / 10/1462 (European Commission, 2010) and MEMO / 10/542 (European Commission, 2010b). In line with this need, the drafting of the protection of new personal data, which extensively regulates the EU Commission's online privacy rights, was submitted to the approval of the European Council and the Parliament on 25 January 2012 (European Commission, 2012).

The drafting of new personal data with reference number IP / 12/46 contains significant innovations such as the right to be forgotten which allows users to manage the risks of online data protection, easy access to data, transfer of personal data between service providers, how to obtain personal data more clearly and comprehensively (eg, over 13 years of age), informing the user and the relevant security units about the situation when a data breach occurs for any reason, take more responsibility for those who process personal data. Within the EU Agenda Digital Agenda (2010-2020), information security has been devoted to a wide area. The Digital Agenda is part of the EU's 2020 strategy. The purpose of the Digital Agenda in information security is to produce practical solutions to threats, including the protection of personal data and cyber attacks, and to develop information security policies (European Commission, 2012).

2.6 THE IMPORTANCE OF CYBER SECURITY

Cyber security was first used by computer engineers in the 1990s to describe security issues related to networked computers. However, there have been developments that later emerged that these security problems could have devastating social consequences. They were once considered a major threat to the Western world by politicians, private companies and the media, and were voiced as Electronic Pearl Harbor. The events of September 11 focused on information technologies, computers and security, especially in the protection of information technology infrastructures, electronic surveillance, terrorists' use of the Internet as a means of communication (Hansen, Nissenbaum, 2011: 1155).

Technological developments have a special importance in shaping international security studies. In particular, technological developments have been the decisive factor in the period of the Cold War in which the military balances were sought. Today, technology-based scenarios include cyber warfare, cyber attack and cyber security. These scenarios are that terrorists or malicious attackers can attack and destroy critical infrastructures and global networks by attacking physical or digital structures. The opposing forces and commercialization on the Internet have shown that the Internet is a space that is intertwined with our everyday reality, not an autonomous region above everyday life. As there is no definition of a common cyber area which the international system actors agree

on, the issue of how to apply international law to cyber space attacks is a problem. Yet another problem that arises in this issue is the understanding of whether the cyber attacks are carried out by the state or by the crime elements. This problem causes the states to be approached with suspicion about the source of cyber attacks. Due to the nature of the Internet that has difficulties to trace, it will be wrong to think that this situation will change as long as the fact that the source of cyber attacks cannot be determined clearly. Cyber security has created a serious economic sector beyond its means of political use. In the area of cyber security, large investments are made by states and private organizations. Considering the losses and the loss of reputation as a result of security vulnerabilities, it is considered that governments and institutions will not avoid cyber security investment costs. If we focus on the extent to which the attacks on the Internet can harm national security, we can mention four types of attacks against national security. Of these, cyber warfare and economic espionage are mostly threats associated with states, while cybercrime and cyber terrorism are more often associated with non-state actors. In an ideal case where we assume that the necessary legal arrangements have been made, the national cyber security structure should contain the following elements. First of all, an appropriate operational center where technical and operational transactions can be realized, a coordination center where strategies and concepts are developed and coordinated, legal approaches are established, communication with industry and international organizations is carried out, an administrative structure in which the strategic decisions are presented, discussed and approved for implementation. Considering the use of the Internet in every field today, it is seen that the role of cyber space in national security increases and how far this field will take place in national security in the future (Nye, 2012).

2.6.1 Financial Impact

The losses caused by cyber attacks started to bring serious financial burdens to the organizations. There are researches carried out by various companies to determine the financial burden and the severity of the incident. Some of them highlight the costs of data breach and cyber attack rates while others highlight data leakage and data loss. According to the 2015 Global State of Information Security survey, the number of reported cases in

the area of information security increased by 48% to 42.8 million. In the same report, there has been a 44% increase in attacks against the previous year for large-scale organizations with annual gross income of 1 billion or more. In mid-sized organizations with revenues of $ 100 million and $ 1 billion, an increase of 64% occurred (Pwc, 2014). For the IT security of Gartner's research company, it is estimated that the companies' expenditures in the amount of 71.1 billion dollars in 2014 will reach 76.9 billion dollars with an increase of 8.2% in 2015 (The Wall Street Journal, 2014).

According to the Visiongain survey, cyber security spending until July 2015 is estimated to reach $ 75 billion, while it is estimated to reach 101 billion in 2018 and $ 170 billion in 2020 (Siberbülten, 2015). According to the survey conducted by global market research company Vanson Bourne, companies around the world spend an average of € 4129 on a monthly basis to prevent data leakage, while Turkish companies spend 3220 Euros on average. In 2014, Kaspersky Lab. According to the Global Enterprise IT Security Risks survey conducted in collaboration with B2B International, it is known that the average cost of data breach in small or medium-sized enterprises in the world is $ 47 000. In Western Europe this figure is up to $ 55 000. Losses are not only financial and financial, but also damage to the image and reputation of the company. In the case of missing data cases, more than half of the events (56%) were reported to have a negative effect on the reputation or reliability of the company (Kaspersky, 2014).

According to a study by the Center for Strategic and International Research (CSIS) under the auspices of McAfee, the average annual cost of cybercrime in the world is estimated to be between $ 375 and $ 575 billion. In 2014, it is stated that the loss of cybercrime against the world economy is more than 400 billion dollars, 160 billion dollars on individual scale. In the same survey, the sectors most exposed to cyber attacks are automobiles with 68%, chemical and pharmaceutical sector with 66%, finance with 60%, and health sector with 58% (McAfee, 2014).

According to Norton 2013 report, the total costs arising from cyber attacks Turkey has reached 2 billion dollars and are per person experienced average cost has reached 309 dollars grew by 6 times compared to the previous year (Symantec, 2013). In a study conducted by NetDiligence (2014) on data breach events, 74% of the data loss caused by financial losses was reported by hackers and 23% by malware. The lowest of these losses was $ 1000 and the highest was $ 13.7 million. The average loss per incident decreased

by 23% compared to the previous year and was realized as $ 733.109 (NetDiligence, 2014).

2.6.2 Reputation Impact

The most serious cyber terror attacks can be directed towards economic targets. A cyber-terrorist attack that could lead to millions of people in the computer-dependent sectors, and even to become unemployed, attacks on population and land registers, attacks on health and energy institutions can create distrust against the authority and cause social crisis (Robinson, 2000). This negative impact of the attacks on these systems and the emergence of big economic losses as a result of the interconnection of the companies with the electronic network systems and the transfer of the activities of the new economy companies to the internet as well as the social lives of these countries cause serious losses in the global economies (Laudon, Laudon, 1996).

In general, cyberterors are attacking valuable targets. These targets are generally targets with economic returns or valuable information. Hence, most cyberterrorists set commercial computers, communication systems, or networks of large economic organizations as targets (Todaro, 1993). Thanks to computer technologies, a terrorist can overwhelm the information and communication of large banks, financial institutions and exchanges. In this case, thinking about the economic life of that country will be really mind-boggling (Özcan, 2004).

Cyberterrorists often leave the economies of the economy in a very difficult economic situation. For example, in 1999, it was reported that the company lost 2% of its market value within 5 days as a result of attacks on the American eBay company (Özcan, 2004).

2.6.3 Technological Effect

Under normal conditions, the benefits and effectiveness of security technologies can be measured by means of cost-benefit analysis. The benefits can be measured by the value of the information assets they maintain and the degree of risk they reduce, and their costs can be measured by the total cost of ownership, which includes the cost of installation, training, and maintenance of software / equipment. However, there are problems in measuring the effectiveness of selected safety technologies. In the laboratory tests, it is not possible to determine the percentage of total attacks and how many of the total attacks

can be prevented by the technologies. There is no formal methodology available to compare the safety technologies used with each other in terms of their effectiveness. The difficulties are due to the inability to measure the aggressive profile and the uncertainties in estimating the compliance status of the entity's security policy. The effectiveness of safety technologies is also measured by assessing how much that technology is reducing the relevant risk. Reducing the risk is to prevent the risk completely or reduce the likelihood of occurrence. In the evaluation of the effectiveness of safety technologies, if available, the results of the product trial conducted in the test environment and the statistical data of the past events can be used. In the absence of such historical data, experts in the information security may benefit from expert opinions to estimate the effectiveness of safety technologies. Butler stated that it is the right approach to conduct a sensitivity analysis in order to determine how sensitive the assumptions and predictions of the expert opinions are to the decisions taken. Another issue is that the safety technologies should not be measured independently due to the fact that they do not operate independently of each other; therefore, the measurement of the interaction in the case of using more than one safety technology. It should also be examined how much more than one technology will reduce the risk for the identified risk and whether the total benefit will be greater than the benefit to be taken when the technology is used individually. In order to evaluate the technical effectiveness of the security system infrastructure created by using security technologies, weakness screening, penetration tests and so on. A large number of products are available on the shelf. For this purpose, the enterprises also use the method of auditing the consultant companies with both internal audits and outsourcing, but this approach is the overall assessment of the system and cannot help in the evaluation of cyber security technologies on an individual basis. Gordon and others stated that cyber security audits have increased and that controls can reduce cyber security risks and make improvements in investment decisions (Şentürk et al., 2016: 44-45).

3. REINFORCEMENT FOR CYBER SECURITY

3.1 THE THREATS ARE GLOBAL – SO SHOULD BE THE SOLUTIONS

There are numerous attempts to combat cyber guilt, such as the European Union, the Council of Europe, the United Nations, the OECD (Organization for Economic Co-operation and Development), international organizations and organizations such as the Organization of American States (OAS), as well as numerous initiatives carried out with their support or participation. There are also numerous undertakings conducted by non-governmental organizations which are seen as international organizations. In the context of the United Nations Organization, from the mid-1980s onwards, the United Nations 'search for solutions in the fight against cyber crime has been raised in the Crimes Prevention and Criminals' Treatment Congresses. Resolution 45/121 (1990) of the UN General Assembly relates to computer crime legislation. Based on this decision, a manual was prepared by the UN in 1994 on the prevention and control of computer-related crimes (Gercke, 2009: 116).

In addition, in 2007, a document reveals the EU's policy on combating cybercrime. The entry into force of the Lisbon Treaty in December 2009 created a significant change. With the provisions of the Treaty 82-86, the EU is explicitly given the task of harmonizing the provisions of the substantive and procedural criminal law of the member states; The provision 83 provides for the provision of rules that establish minimum standards for the identification of criminal definitions and sanctions in respect of serious offenses involving transboundary crimes, in which computer crimes are also explicitly included. In this respect, the development of legislation on computer crimes is now within the scope of shared competence between the EU and the member states and the EU has the authority to make legally binding savings on the subject. As of December 1, 2012, the Draft Directive on attacks against information systems dated 30 September 2010 has not yet been adopted. Prior to the adoption of the Budapest Convention under the Council of Europe, an Expert Committee was appointed in 1985 to discuss the legal aspects of computer crime. A Recommendation was adopted in 1989, and in 1995 another Recommendation on problems arising from transboundary computer crimes was adopted. The Organization for Economic Co-operation and Development (OECD) has several

previous studies, but it should be noted in 2002 that the OECD Guidelines for Security of Information Systems and Networks: Towards Security Culture, adopted by the OECD Council. G-883, consisting of 8 major industrialized states (USA, Germany, France, England, Italy, Japan, Canada, and Russia), established in 1997 as the G-7, a subcommittee on high technology crime, fighting cybercrime subject to the subject. Later, the Ministers of Interior and Justice of these states adopted an action plan of ten principles to combat high-tech crimes. Perhaps one thing that should be emphasized is the "Contact Points Network", which is created within the G8 and constitutes a fundamental reference for international cooperation and reflected in Article 35 of the Budapest Convention. The work of INTERPOL, EUROPOL and EUROJUST in combating cybercrime is important. An important effort in this regard, as well as the establishment of the High Tech Crime Center by EUROPOL, is the aim of this center to co-ordinate the investigation of transnational cybercrime across Europe. Likewise, in 2010, a platform called European Cybercrime Task Force (EUCTF) was established within the EUROPOL, composed of persons headed by the European Commission, EUROJUST and the head of the cyber-guilt units of the EU countries. The aim is to assist in the development and promotion of a coherent approach within the EU in the fight against cybercrime and to respond to problems arising from the use of cyber technology in criminal offense (European Police Office, 2011: 48).

3.2 MORE FOCUS ON DIGITAL CYBER SKILLS

In fact, there are many technological or process solutions, methods, standards, laws and regulations in the world in terms of information security in our country (Tipton and Krause, 2007; T.S.E., 2006; Scholtz et al., 2006; ISO, 2005). However, as demonstrated by the numbers in the previous section, losses, deficits, and problems of information security continue to increase and information security risks cannot be adequately reduced or controlled. Because the basic problem is the view of individuals and society, errors and inadequacies in the way of perception and approach. The point of view of individuals, societies and institutions in information security has to be changed first. The top executives in the institutions, the written and visual media, the authorities regulating the laws and regulations have serious duties in this regard. It should be kept in mind that security is a process to be sustained and managed by informing people before the

technology, by raising awareness, starting from the top, informing, supporting and caring about such issues (Eminağaoğlu, 2008).

In organizations, groups that need to comply with the principles such as group as much as they should know, minimum authorization, as much as they need to reach are managers and informatics. On the contrary, in these two groups, these principles are the least applied and most risky actions (mandatory or arbitrary, conscious or unconscious). It is known that those who carry and use the most valuable and most confidential information in institutions are mostly employees in these two groups. In addition, the units that are the most frequently sampled and more conspicuous in terms of the nature of their work are also the two units (Tipton and Krause, 2007).

Considering the use of wireless ADSL, Internet, mobile phone, etc. in the daily lives of individuals and society, information security solutions need to be rapidly expanded not only for business purposes but also for individual use (Swaminatha and Elden, 2003).

3.3 AGILE ANSWERS

Turkey's Action Plan 2013-2014 and 2016-2019 Certificate in Cyber Security Strategy document is located. However, in the event of a possible attack, the National Computer Emergency Response Center (USOM), which is responsible for supporting the attacked organization and coordinating the intervention, and the Cyber Incident Response Teams (SOME) established by the companies providing electronic communication services. USOM has responsibilities such as conducting malware analysis, traffic monitoring, reporting malware, informing the public, and cooperating with public and private institutions. Cyber exercises have been conducted with the participation of many institutions to date. For example, in 2012, the Cyber-Shield Exercise under the leadership of BTK was aimed to develop technical aspects in order to eliminate cyber attacks. However, no drills have been carried out for 3 years since these drills were not followed (Sanalp, 2016: 40).

Turkey is a country that is not at the point when it should be assessed according to the potential to have but not in a bad location on cyber security. This is the period where the work occurred and lived with DDoS attacks against Turkey an extension inaccessibility of sites, events such as becoming unable to process the banking system of our country

should be seen as a great opportunity for the elimination of self-criticism made and shortcomings of the position in the cyber security field. As a matter of fact, all of the countries which are developed in cyber security today are the countries which are frequently cyber attacked. In cyber attacks, the identity of the attacker is often undetectable due to the use of zombie computers; The reason why the attackers should concentrate on a single gap of a system is that the fight against the attackers is a difficult process, as it is necessary to identify all vulnerable parts in the system for the protection of the system, and should not intimidate the fighters in cyber space. Because the fact that the attackers are often one step ahead of countries or companies brings about a technical improvement (Sanalp, 2016: 49-50).

3.4 CREATING TRUST

Many of the OECD and NATO member countries have a program for the protection of critical infrastructures defined at the government level. In these countries, the protection of critical infrastructures has entered into the country's legislation. An OECD document prepared in 2007 compared Australia, Canada, Japan, South Korea, the Netherlands, the United Kingdom and the United States to the studies of the protection of critical infrastructure (OECD, 2007).

In the first phase, all countries working on critical infrastructures identify basic countermeasures that concern all infrastructures. In order to protect the critical infrastructures in Turkey, the most important four steps are as follows:

a) Support and participation from the top level executive (eg. Prime Ministry)
b) Preparation and implementation of supporting legislation
c) Preparation of policy documents for the protection of critical infrastructures
d) Adequate budget allocation for studies

It is inevitable that the steps taken in order to protect the critical infrastructures without failing in these four steps will fail (Karabacak and Özkan, 2009).

4. CONCLUSION

Turkey runs a serious risk of losing trust, incurring additional costs and inadequately responding to a major cyber attack:

a) Cyber attacks against critical EU infrastructure can severely damage the Europe economy far beyond the national borders of the targeted country.
b) EU countries will not be able to securely provide trusted cross-border platforms and infrastructures.
c) Diminished trust in current or future digital platforms can severely undermine the European economy.

Under the light of these information, the suggestions mentioned in section 3 can be used to help Turkey take little steps to make big differences in order to attain a sufficient level of cyber security condition.

Firstly, threats in cyberspace do not respect borders governments cannot retreat into national responses to them. Cyber authorities should ensure security measures under the NIS Directive align to global standards and that schemes under the forthcoming Cybersecurity Certification Framework are compatible with international approaches. In order to gain competence advantage Turkey must acknowledge global solutions for global threats.

Secondly, the pace of digitalization brings new threats that many are not aware of or ready to respond to. There must be a strong focus on improving digital skills
across all levels of society, business and the public sector.
Thirdly, as digitalization drives innovation across ever expanding aspects of Turkey's economic and social lives, malicious actors are quickly looking for new exploitation paths. Turkey needs the flexibility to keep pace. Making space for fast-track, light-touch certifications under the proposed EU Framework is one way to help industry do so.

Lastly, cooperation between the public and private sector is essential not only to cybersecurity but to citizens' trust in technology. Sharing information should be a two-

way street and public authorities should take care to avoid an overzealous approach to data access for law enforcement and national security.

It is quite obvious that, Turkey Government, private sectors, schools, and individuals need more focus on reinforcing cyber security than world's average countries, on the occasion of increasing threats, complicated security solutions, lack of competence, and limited resources. It is crucial to remember that cyber risks keep progressing day by day, as well as digitalization. This research about cyber security measures should be updated periodically to take quick actions.

REFERENCES

Periodicals

Aslıyüksek, M. K. (2016). Bilgi teknolojileri ve dijitalleşmenin Türkiye'de bilgibilim literatürüne yansıması: Bilgi dünyası dergisi örneği (2000-2014). Bilgi Dünyası, 17(1).

Bayraktar, G. (2014). Harbin Beşinci Boyutunun Yeni Gereksinimi: Siber İstihbarat. Security StrategiesJournal, 10(20).

Bıçakcı, S., Ergun, D., &Çelikpala, M. (2015). Türkiye'de siber güvenlik. EDAM Siber Politika Kağıtları Serisi, (1).

Bulut, E., &Akçacı, T. (2017). Endüstri 4.0 Ve İnovasyon Göstergeleri Kapsamında Türkiye Analizi. Assam Uluslararası Hakemli Dergi, 4(7), 55-77.

Çakır, H., & Yaşar, H. (2015). Kurumsal Siber Güvenliğe Yönelik Tehditler Ve Önlemleri. Düzce Üniversitesi Bilim Ve Teknoloji Dergisi, 3(2).

Çetin, H., Gundak, İ., & Çetin, H. H. (2015). E-İşletme Güvenliği Ve Siber Saldırılar Üzerine Bir Araştırma. Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 6(2), 223-240.

Dalı, A. B. A. (2018). Nato Üyesi Ülkelerin Siber Güvenlik Stratejileri Açısından İncelenmesi.

Erol, O., Şahin, Y. L., Yılmaz, E., &Haseski, H. İ. (2015). PersonalCyber Security ProvisionScaledevelopmentstudy Kişisel Siber Güvenliği Sağlama Ölçeği geliştirme çalışması. Journal of Human Sciences, 12(2), 75-91.

Göçoğlu, V. (2018). Türkiye'nin Siber Güvenlik Politikalarının Kamu Politikası Analizi Çerçevesinde Değerlendirilmesi.

Gökce, K. G., Şahinaslan, E., & Dincel, S. (2014). Mobil Yaşamda Siber Güvenlik Yaklaşımı. Tablet, 195(270.7), 349-1.

Güngör, M. (2015). ULUSAL BİLGİ GÜVENLİĞİ: STRATEJİ VE KURUMSAL YAPILANMA.

Hekim, H., & BAŞIBÜYÜK, O. (2013). Sİber Suçlar ve TürkİYe'NİnSİberGüvenlİkPolİtİkalari. Uluslararası Güvenlik ve Terörizm Dergisi, 135-158.

Karaarslan, E., & Akbaş, M. F. (2017). Blokzinciri Tabanlı Siber Güvenlik Sistemleri. Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 3(2), 16-21.

Keser, H., & Güldüren, C. (2015). Bilgi Güvenliği Farkındalık Ölçeği (Bgfö) Geliştirme. Kastamonu Eğitim Dergisi, 23(3), 1167-1184.

Öğün, M. N., &Kaya, A. (2013). Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler. Security StrategiesJournal, 9(18).

Önaçan, M. B. K., & Atan, H. (2016). Siber Güvenlikte Lisansüstü Eğitim: Deniz Harp Okulu Örneği. Trakya Üniversitesi Mühendislik Bilimleri Dergisi, 17(1), 13-21.

Önok, M. (2013). Avrupa Konseyi siber suç sözleşmesi ışığında siber suçlarla mücadelede uluslararası işbirliği.

Şahinaslan, Ö. (2013). Siber saldırılara karşı kurumsal ağlarda oluşan güvenlik sorunu ve çözümü üzerine bir çalışma.

Şentürk, H., Çil, C. Z., & Sağıroğlu, Ş. (2016). Siber Güvenlik Yatırım Kararları Üzerine Literatür İncelemesi. Politeknik Dergisi, 19(1), 39-51.

Ünver, M., & Canbay, C. (2010). Ulusal ve uluslararasiboyutlariyla siber güvenlik. Elektrik Mühendisligi Dergisi, 438, 94-103.

VonSolms, R. ve Van Niekerk, J. (2013). Bilgi güvenliğinden siber güvenliğe. bilgisayar ve güvenlik , 38 , 97-102.

Wang, W. ve Lu, Z (2013). Akıllı şebekede siber güvenlik: Anket ve zorluklar. Bilgisayar Ağları , 57 (5), 1344-1371.

Yayla, M. (2013). Hukuki Bir Terim Olarak Siber Savaş. TBB Dergisi, 104, 194-198.

Yılmaz, E., Halil, U. L. U. S., & Gönen, S. (2015). Bilgi Toplumuna Geçiş Ve Siber Güvenlik. Bilişim Teknolojileri Dergisi, 8(3), 133.

Others Publications

Henkoğlu, T., & Yılmaz, B. (2013). Avrupa Birliği (AB) bilgi güvenliği politikaları. Türk Kütüphaneciliği, 27(3), 451-471.

Kara, M. (2013). Siber Saldırılar Siber Savaşlar ve Etkileri(Doctoraldissertation, İstanbul Bilgi Üniversitesi).

Kara, O., Aydın, Ü., & Oğuz, A. (2013). Ağ Ekonomisinin Karanlık Yüzü: Siber Terör.

Karabacak, B. (2011). Kritik Altyapılara Yönelik Siber Tehditler ve Türkiye İçin Siber Güvenlik Önerileri. Siber Güvenlik Çalıştayı, Bilgi Güvenliği Derneği, 29.

Sanalp, S. (2016). Çeşitli ülkelerde usom ve some yapılandırılması ve Türkiye modeli önerisi (Doctoraldissertation, İstanbul Bilgi Üniversitesi).

Türker, M. (2015). Finansal Güvenlik Sistemi rken Uyarı Modeli: Türk Bankacılık Sektörü Üzerine Bir Uygulama ve Politika Önerileri (Doctoraldissertation, Doktora Tezi, İstanbul).

Ünver, M., Canbay, C., & Mirzaoğlu, A. G. (2009). Siber güvenliğin sağlanması: Türkiye'deki mevcut durum ve alınması gereken tedbirler. Bilgi Teknolojileri ve İletişim Kurumu (BTK), Ankara, 8, 2018.

Yılmaz, S., & Sağıroğlu, Ş. (2013). Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri. 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı, 158-166.