Journal of Social Sciences of Mus Alparslan University

anemon

Derginin ana sayfası: http://dergipark.gov.tr/anemon

Araştırma Makalesi ● Research Article

An Examination of the Historical Development of Cybersecurity in the Context of International Security Studies: The Case of Turkiye

Gürkan Gündüz*

Abstract: In the contemporary era, rapid technological advancements have created significant conveniences while simultaneously generating complex security challenges in the digital environment. Developments in information technologies have increased security risks for individuals, organizations, and states, particularly concerning the protection of information and digital documents. In this context, cybersecurity has emerged as a fundamental component of efforts to address threats arising in the digital domain. Owing to the transnational and borderless nature of cyber threats, cybersecurity has become a critical issue that directly affects global security and transcends national boundaries. Consequently, it has assumed a central role in the security agendas of both developed and developing countries. This article, entitled "An Examination of the Historical Development of Cybersecurity in the Context of International Security Studies: The Case of Turkey," aims to analyze the historical evolution of cybersecurity since the 1990s at both the global level and within the Turkish context. The study is based on a literature review and employs document analysis and comparative analysis methods within a theoretical framework grounded in international security approaches.

Keywords: Asymmetric Threat, Cyber Security, International Security, National Security, Security Technologies

Uluslararası Güvenlik Çalışmaları Bağlamında Siber Güvenliğin Tarihsel Gelişimi Üzerine Bir İnceleme: Türkiye Örneği

Öz: Günümüzde teknolojik gelişmelerin hız kazanması, hayatı kolaylaştıran imkânlar sunmakla birlikte dijital alanda yeni güvenlik sorunlarını da beraberinde getirmiştir. Özellikle bilişim teknolojilerinde kaydedilen ilerleme, bilgi ve belgelerin korunması başta olmak üzere bireyler, kurumlar ve devletler açısından ciddi güvenlik riskleri doğurmuştur. Bu bağlamda siber güvenlik, dijital ortamda ortaya çıkan tehditlere karşı alınan temel önlemlerden biri hâline gelmiş; söz konusu tehditlerin sınır aşan niteliği nedeniyle yalnızca ulusal değil, aynı zamanda küresel güvenliği de ilgilendiren bir alan olarak önem kazanmıştır. Bu durum, siber güvenliği gelişmiş ve gelişmekte olan ülkelerin güvenlik politikalarının merkezine yerleştirmiştir. Siber güvenliğin artan önemi, konuya yönelik akademik çalışmaların da yoğunlaşmasına yol açmıştır. "Uluslararası Güvenlik Çalışmaları Bağlamında Siber Güvenliğin Tarihsel Gelişimi Üzerine Bir İnceleme: Türkiye Örneği" başlıklı bu makale, siber güvenliğin 1990'lı yıllardan itibaren dünya genelinde ve Türkiye özelinde geçirdiği tarihsel gelişim sürecini ortaya koymayı amaçlamaktadır. Çalışma, literatür taramasına dayalı olarak hazırlanmış olup doküman analizi ve karşılaştırmalı analiz yöntemleri kullanılmıştır. Ayrıca uluslararası güvenlik yaklaşımlarına dayanan teorik bir çerçeve oluşturularak merkezi bir araştırma sorusu etrafında analiz gerçekleştirilmiştir.

Anahtar Kelimeler: Asimetrik Tehdit, Güvenlik Teknolojileri, Siber Güvenlik, Ulusal Güvenlik, Uluslararası Güvenlik

* Dr., Jandarma Genel Komutanlığı,
ORCID: 0000-0002-3067-6576, drgurkangunduz@gmail.com
Cite as/ Atıf: Gündüz, G. (2025). An examination of the historical development of cybersecurity in the context of ınternational security studies: The case of Turkiye. *Anemon Muş Alparslan Üniversitesi Sosyal Bilimler Dergisi*, *13*(3), 1988-2023.
http://dx.doi.org/10.18506/anemon.1776172
Received/Geliş: 02 September/Eylül 2025
Accepted/Kabul: 04 December/Aralık 2025
Published/Yayın: 30 December/Aralık 2025

e-ISSN: 2149-4622. © 2013-2025 Muş Alparslan Üniversitesi. TÜBİTAK ULAKBİM DergiPark ev sahipliğinde.

Introduction

The globalizing world is changing at an extremely rapid pace; developments in cyberspace are emerging as the most important reason for this process of change. In today's world, where both states and non-state actors are engaged in a race to gain advantages and establish superiority over each other, cyberattacks are at the forefront of asymmetric threats between states. Ensuring cybersecurity has attracted the attention of states and non-state actors, becoming an important agenda item in the international arena, particularly in national security policies. Cybersecurity, which has emerged as a serious factor in international relations, continues to be effective in many areas today (Güntay, 2018). For these reasons, cybersecurity has become a very serious scientific topic researched by scientists around the world.

Cybersecurity, which has become one of the most important structures in the cyber world in terms of security, is a phenomenon that ensures the digital security of modern life. For this reason, numerous definitions have been made in the scientific world regarding what cybersecurity is. However, a definitive definition of cybersecurity has not yet been established. The fact that the world of technology evolves day by day, like a living organism, makes it very difficult to establish a definition in this field. This is because when the boundaries of cybersecurity cannot be clearly defined, its definition cannot be established in a genuine manner. Nevertheless, cybersecurity has become a significant force in ensuring the security of humanity in the fields of information and technology (Tunca, 2019). Therefore, cybersecurity will be at the forefront of the issues that people will focus on and discuss the most, both today and in the future.

According to Karasoy, cybersecurity, which rapidly entered people's lives in the early 1990s, connects people internationally, primarily in the areas of economy and security. Today, cybersecurity plays a huge role in preserving and storing information in institutions and organizations that work with high volumes of digital data, such as security forces, judicial units, population offices, health institutions, banking operations, educational activities, state infrastructure and superstructure works, intelligence information, etc. This is because all of the aforementioned tasks are necessary for the security of states and the peace of mind of citizens; protecting them is of serious importance. Cybersecurity comes into play here and is in an effective position to take the necessary digital measures to protect this information. In addition to protecting the aforementioned information, it is also important to store and make this information available for use (Karasoy & Gezici, 2023). Therefore, it is essential that cybersecurity is effectively in place to ensure that this information is shared securely in the digital environment.

In today's world, where accessing information has become very easy, protecting sensitive information that constitutes state security is becoming increasingly difficult. Hackers, spyware, and other illegal means can easily access digital data through cyberattacks, exposing information that should remain confidential and leaking it outside. This situation poses a threat and danger to the security of states. It is imperative that decisive measures be taken against these threats, and for this, cybersecurity must be further developed and actively implemented.

As stated above, cybersecurity is crucial in today's world for ensuring genuine security worldwide. This is because in the 21st century, with its highly advanced technology, the security of both the world and Turkiye, which is the subject of our work, is under threat. For this reason, since the 1990s, cybersecurity measures have been implemented in all countries around the world, including Turkiye, against every threat to digital security.

Since the early 1990s, there have been rapid developments in the field of cybersecurity worldwide. This study, prepared through extensive research, is divided into two sections. The first section examines the historical process of cybersecurity development worldwide, while the second section attempts to explain in detail the developments in cybersecurity in Turkiye from the early 1990s to the present day. Prepared using scientific studies on the subject, this article employs document analysis and comparative analysis methods. This article, created by drawing on numerous sources, aims

to provide a valuable resource for those working in the field of cybersecurity. Overall, this study seeks to answer the question: "How has the concept of cybersecurity developed within the theoretical framework of international security studies in a historical context, and how has this development taken shape in Turkiye in light of certain dynamics?" Approaching the research from this perspective makes it possible to understand both the chronological historical change and the international security perspective together.

Objective

The objective of the study, entitled "An Examination of the Historical Development of Cybersecurity in the Context of International Security Studies: The Case of Turkiye," is to reveal the evolution of cybersecurity, a field that has played a significant role in people's lives since the 1990s.

In line with this objective, the study aims to reveal the stages through which cybersecurity has passed, both globally and in Turkiye, to reach its current state. The hypothesis of this study is based on the view that "the development of cybersecurity gains momentum when digital infrastructures are placed at the center of security policies as the fundamental subject of state security, and when considered in line with global trends, developments in Turkiye follow a similar pattern." In accordance with the study's hypothesis, advancements in the domain of cybersecurity in Turkiye are scrutinized from a historical standpoint, with the objective of contributing to the body of knowledge in this field.

Methodology

The present article was prepared by conducting a comprehensive literature review and drawing upon numerous scientific works. The document analysis technique, content analysis technique, and comparative analysis method were utilized.

The sources under scrutiny in this document analysis comprise a range of materials, including national strategy documents, reports from the Turkish Academy of Science and Technology (TÜBİTAK), development plans, academic articles, and official legislation texts. The selection of these sources was guided by predefined criteria, such as publication year, institutional reliability, and relevance to the domain of cybersecurity.

The comparative analysis technique was employed by means of a comparison between the global development of cybersecurity policies and the evolution of their implementation in Turkiye over time. In this process, developments subsequent to 1990 were specifically classified analytically (Bowen, 2009).

Findings

A comprehensive literature review was undertaken on the subject, and the topic was subjected to meticulous scrutiny. The subjects addressed were classified into two categories for analysis.

A consideration of the findings obtained in conjunction with the theoretical approaches identified in the extant literature leads to the following conclusions: The global development of cybersecurity since 1990 has gained momentum in the context of inter-state power struggles, as posited by the Realist approach (Baylis & Smith, 2017, 301).

• Following 2010, Turkiye experienced a significant acceleration in its historical development, which unfolded largely in accordance with the securitization model theorized by the Copenhagen School.

• Nevertheless, initiatives aimed at cultivating cybersecurity awareness among the Turkish populace remain constrained when assessed within the framework of the critical security perspective.

Theoretical Framework: International Security Approaches and Cybersecurity

The objective of this discourse is to ascertain the role of cybersecurity within the broader paradigm of international security studies.

A meticulous evaluation of the foundational theoretical approaches is imperative to achieve this objective. The realist approach, a perspective that perceives cyberspace as a novel dimension in the incessant power dynamics among states, construes cyberattacks as deliberate threats to national security (Walt, 1991).

The Copenhagen School, conversely, addresses the issue of cybersecurity within the framework of 'sectoral security,' emphasising the crucial necessity of ensuring the security of digital infrastructure (Buzan, Wæver & de Wilde, 1998, 27). Contrary to the aforementioned perspectives, Critical Security Studies propound the notion that cybersecurity is not solely state-centric but rather a multifaceted endeavor encompassing technological, social, and individual interactions (Booth, 2007, 145). The theoretical approaches delineated above offer an interpretive framework for the analyses to be undertaken in the course of the study.

The Development Process of Cybersecurity in the International Arena

Since the early 1990s, cybersecurity has become an integral part of people's lives, and its importance for defense has been recognized. To better understand this concept, serious research is being conducted worldwide, and it is essential that such research continues. Looking at the historical development of cybersecurity around the world, it is clear that many different concepts have emerged from 1990 to the present day. These concepts include "cyberwar," "cyber asset," "cyber incident," "cyberbullying," "cyber espionage," "cyber weapon," "cyber police," "cybercrime," "combating cybercrime," "cyberterrorism," "cyberterrorist," "cyberattack," "cyberthreat," "cyberdefense," "cyberpsychology," "cyberhealth," etc. (Sağıroğlu, 2018, 21). As can be seen, the word cyber has been added to the beginning of many terms used in everyday life, and these new word groups are frequently used today.

In the international arena, numerous countries, primarily the US and EU countries, along with international organizations, institutions, and organizations, are collaborating on the secure sharing of important information to establish cybersecurity. Plans and programs are being developed to establish cybersecurity in the international arena in a healthy manner, and serious steps are being taken for the future (Ünver et al., 2011, 1). This situation reveals that cybersecurity is extremely important in international security efforts.

So, how did cybersecurity, which is considered so important, emerge and become effective internationally? In essence, cybersecurity alone does not mean much. Cybersecurity encompasses all security measures aimed at protecting electronic devices connected to each other via internet networks, primarily information processing and digital systems. Therefore, in the rapidly evolving digital world, cybersecurity must be addressed as a whole (Solmaz, 2011). This is because today, very serious cyberattacks are taking place worldwide, and states must take measures against them. The historical development of this process is occurring rapidly, and measures to address it have been increasing since the 1990s. The same is true for Turkiye.

From the perspective of the historical development of cybersecurity, the invention and use of the first computers constitute the first phase. Developments during and after World War II revealed that military methods relying solely on humans and weapons were insufficient in security-related areas, ranging from ensuring national security to securing borders. This necessitated the adaptation of technology to the security domain. The first computers invented were also primarily used in the military field.

In this context, the scientist Alan Turing invented the "Turing Machine," a simple computing machine capable of performing 'algorithms' and "calculations," during World War II. At the same time, the United States was attempting to establish a technological system that would enable war vehicles such as aircraft, which were unable to reach their targets due to adverse weather conditions, to easily identify their targets. As a result of the scientific studies conducted for this purpose, in 1943, "John Mauchly" and "Presper Eckert" invented the computer called "Electronic Numerical Integrator and Computer (ENIAC)" in 1946, which is considered the first computer in the digital sense (Gündoğdu, 2023). In fact, only a few computers were produced worldwide between 1940 and 1950, and many people were unaware of the existence of computers. In terms of cybersecurity, technological developments have made significant progress since the 1950s.

Cybercrimes began to emerge in the 1950s, posing a threat to security. In this context, there is a very serious connection between the open-source programs that began to develop in the United States in the 1950s, known as the "Hippie Movement." According to Bıçakçı, "The Hippies' rebellious stance against accepted rules formed the core philosophy of computer-based technological developments. This philosophy, which originated in the laboratories of the Massachusetts Institute of Technology, involved programmers, or hackers as described by Steven Levy, writing programs and making their codes available to their friends. Other software developers would then develop these codes as needed and adapt them to their own purposes. Here, sharing was done entirely based on personal preferences and freely. The open-source philosophy behind this sharing was prominent. The fact that hippies shared a similar philosophy ensured that this movement was supported by hackers." (Bıçakçı, 2014). Thus, with the emergence of hackers in the US, the foundation was laid for cybercrime, which began to threaten security in many areas, primarily the military, around the world.

From a cybersecurity perspective, cybercrimes began to pose a threat to the world as computers developed significantly in the 1960s and cybercriminals sought to increase their influence. In this context, with advances in communication technologies, the world has given birth to a neosphere, a "world of minds" extending from one side of the globe to the other, a "thinking cycle," a "wonderful thinking machine," a "thinking shell" filled with fiber and networks, and a planet-wide "consciousness." According to Özdemirci, at the core of every event and development seen around the world, there is another condition for living beings to survive in the layer where they exist, known as the "biosphere," where information begins to emerge. This is the new condition of life that has emerged as a result of the development of information and intelligence (Özdemirci & Torunlar, 2018). These new conditions of life naturally reveal how important cybersecurity has become.

From a cybersecurity perspective, the year 1969 is extremely important. This is because the first computer network, called ARPANET, was established and put into operation at the Stanford Research Institute, the University of California, Los Angeles, the University of California, Santa Barbara, and the University of Utah. Initially, the system was only open to institutions and organizations working with the US Department of Defense, but over time, scientists began to use it for scientific communication purposes as well. Originally developed primarily for research and investigation in military fields, this communication network began to be used intensively by scientists for personal conversations as well; subsequently, this communication network began to be used by all scientists (Sancakdar, 2021, 16). The use of computers for military purposes since 1969 has naturally made cybersecurity a priority in many developed countries, particularly the United States.

According to Ünver, in the context of cybersecurity, for the "Advanced Research Projects Agency" (ARPA), this meant finding ways to make the times when computers were not in use productive and to enable people doing different work to benefit from them, primarily at the Pentagon and other institutions across the United States. Efforts focused particularly on inter-university data transfer, with the first "electronic mail" sent in 1971 and the first network connection made from the University of Florida to Stanford in 1969, expanding in 1972 to connect more areas by adopting a forty-node logic. Shortly thereafter, many more research centers and universities around the world joined this first network or, alternatively, created their own networks (Ünver, 2023, 45). This situation is extremely important in terms of demonstrating the rapid pace of development in computers since 1969.

When it comes to cybersecurity on an international scale, the first concept that comes to mind is the foundation of the internet, namely the "ARPA" project that created the internet. With the inclusion of new computers over time, communication over the network has increased significantly. Consequently, many new systems, primarily electronic messaging and file transfers, which were considered useful and beneficial to many users, were invented and made available. After this, in 1973, efforts were made to create a common language and integrate existing networks so that networks with different characteristics could share information with each other. Developed for this purpose, "TCP/IP (Transmission Control Protocol/Internet Protocol)" was created and put into use as a common software language that enables network protocols and computers with different characteristics to communicate efficiently with each other (Altınbaşak & Karaca, 2009).

The year 1983 is very important in terms of the concept of cybersecurity. This is because in 1983, MCI pioneered efforts to launch the first commercial email service over the internet. The word "cyber" was first coined during these developments. William Gibson first used the word in his 1982 work as a combination of "cybernetic" and "space." Two years later, in his revolutionary novel Neuromancer, he described it as "an illusion based on consent experienced daily by billions of legitimate operators in every nation... Unthinkable complexity, lines of light, a metaphor found in the void of the mind, in data sets and constellations" (Ünver, 2023, 46). Thus, from this date onwards, the concept of cybersecurity began to be known and used seriously around the world.

In the context of the historical development of cybersecurity, it was determined in the late 1980s that managing the internet was not the responsibility of the research community. Commercial actors were able to provide the network services needed to develop and grow the internet, and at the same time, they became enthusiastic consumers of this development. Therefore, the White House Office of Science and Technology developed a plan to expand and commercialize its work. Planners anticipated a ten-year process, with the final stages of commercial transfer not being completed until the late 1990s.

In the context of the above statements, US Congressman Gore argued that high-speed telecommunications were the driving force behind both economic growth and the improvement of our education system. He was the first elected official to grasp that computer communications could have a broader impact beyond improving developments in science and academia. Work on the internet began in 1973 and reached its peak in 1983. However, the internet as we know it today was not made available for use until 1983. When the internet was still in its early stages of use, US Congressman Al Gore provided intellectual leadership by helping to shape the vision of the potential benefits of high-speed computing and communication (Wiggins, 2010). For example, sessions were held on how advanced technologies could be used in areas such as coordinated intervention by government agencies in response to natural disasters and other crises. These developments and advances in internet systems are gradually leading us toward the issue of cybersecurity.

According to Önal, systems known as DNS began to be created using structures that are easier to remember than numbers. By the end of the 1980s, the internet system had transitioned to being used for commercial purposes and was heavily utilized in the field of internet commerce. As a result of the active use of the internet in many areas, including commerce, the world's first search engine, called Archie, emerged. According to Önal, the development of this search engine and its widespread use across the internet led to major problems in the field of cybersecurity and, in subsequent periods, to a situation that became uncontrollable. Indeed, in an environment where internet usage had developed to such an extent, the first viruses appeared in 1982, and the virus called MORRIS, invented in 1988, damaged a large portion of devices connected to the internet network (Önal, 2021). Consequently, the concept of cybersecurity, which is now a crucial branch of global security, emerged.

According to Çeliktaş, starting in 1990, the serious development of computers and the internet and their significant growth worldwide resulted in a large amount of data, primarily security information, being transferred to cyberspace. This has made humanity dependent on information and technology. Initially thought to be highly beneficial and capable of significantly improving human life, this situation

has deteriorated over time. This is because the information transferred to computers has fallen into the hands of malicious individuals, endangering the security of people and states (Çeliktaş, 2016, 5). Cybersecurity has become vulnerable to cyberattacks and threats that compromise security in such an environment, making it necessary to move away from traditional security approaches and develop new systems.

Another milestone in the development of cybersecurity was 1991. What made 1991 stand out was that it was the year of the Gulf Crisis, a significant development in the world. During this process, John A. Warden, an American who was seen as the architect of the air assault operations in the Gulf War, argued that all states and elements with a strategic structure should be analyzed using a systems approach. Based on this statement, Warden spoke of the existence of a total of five interlinked rings. These rings consist of the following: a) leadership, b) important structures, c) infrastructure, d) population, e) military forces. Since 1991, the internet network has also become extremely important. This is because, with the onset and increase of cyberattacks, defense systems based on technological superiority have become essential due to the inadequacy of countries' attack capabilities and the aforementioned five rings (Güneş, 2019). This has once again highlighted the importance of cyber security systems based on technological superiority.

In 1990, a researcher at the European Organization for Nuclear Research (CERN) in Switzerland created a new network interface using documents and files on a computer where many letters were vaguely related. This was the Hypertext Transfer Protocol (HTTP). Tim Berners-Lee invented the World Wide Web (www) with an accompanying system for creating computer-related documents (URLs). According to Singer and Friedman, when Berners-Lee attempted to present this at an academic symposium, his invention was not considered valuable enough (Ünver, 2023, 52). Instead, he was confined to holding a poster in a hallway.

The first website in the context of cybersecurity was created in 1991. According to Yılmaz, since that date, the system known as the “World Wide Web” has been defined as the interconnection of information, documents, and computer networks through “hypertext” and digital technology. However, it is important to remember that the web and the internet are not synonymous. This is because the internet refers to the combination of networks where all information, especially information belonging to official institutions and organizations, is made publicly available. The web, on the other hand, is a subcomponent of the internet that facilitates the flow of information via a browser over the network. In this context, emails, social media platforms such as Facebook and Instagram, blogs, and search engines are all part of the internet. Therefore, these are not the web (Yılmaz, 2021). As the use of web pages has increased, very serious problems have arisen in terms of cybersecurity based on the internet. In other words, as internet usage has increased and the number of web pages has grown, a serious security problem has emerged in the virtual world. This has increased the importance of cybersecurity.

In the history of cybersecurity, the emergence of viruses, which are malicious software, is as important as the development of the internet and web systems. The first known virus in the world is the “MORRIS VIRUS,” written by Robert Tappan Morris for fun. This malicious software program, referred to in Turkish as the “MORRIS WORM,” and created by the aforementioned individual as a result of an error, damaged approximately 10% of computers connected to the global internet network from the day it first appeared. Subsequently, macro viruses emerged in 1996 (Acarer, 2020). Cyberattacks began to be carried out through the virtual world immediately after these viruses, posing serious dangers. This has once again brought cybersecurity to the forefront as an important issue. Viruses pose a serious danger and threat to computers and information networks.

In the early 2000s, credit card fraud emerged worldwide, creating a serious security issue. Cybersecurity affects many areas, including economic systems. When looking at cybersecurity from the perspective of economic systems, banking transactions, credit cards, investment funds, and many other transactions conducted online involve financial institutions such as banks, credit card service providers, and fund management companies, which hold a large amount of information, primarily personal identity details and home addresses. This situation has attracted the attention of cybercriminals to a significant

degree (Akçakanat et al., 2021). Therefore, since the 2000s, credit card and other types of virtual fraud have increased, making it necessary to take serious measures in the field of cybersecurity.

The 'I LOVE YOU' virus, which emerged in 2000, infected approximately 50 million computers worldwide in just two days, making it one of the fastest-spreading malicious software programs in history. This virus, which spread via email, caused significant data loss, particularly in public institutions and large companies. It has become an important example in the literature for demonstrating the effectiveness of social engineering in cyberattacks (Reagan, 2001).

The large-scale DDoS attacks carried out against Estonia in 2007 are considered one of the first major state-sponsored cyber operations in the modern sense. These attacks disabled banking systems, government portals, media organizations, and the official websites of the parliament, directly impacting the country's administration. The Estonian example brought to the world's attention how destructive cyberattacks can be in terms of national sovereignty and critical infrastructure (Ottis, 2008, 24).

Similarly, in 2008, Georgia was subjected to simultaneous cyberattacks during the military tensions with Russia. These attacks were coordinated with physical conflict and led to the concept of 'hybrid warfare' becoming established in the cybersecurity literature (Shakarian, 2011). These two events caused states to reshape their cyber defense strategies and clearly revealed the connection between the cyber domain and the military dimension in international security studies.

Another significant development that fundamentally changed the concept of cyber warfare was the Stuxnet attack, discovered in 2010. Believed to be a joint US–Israel operation, Stuxnet targeted centrifuges at Iran's Natanz nuclear facility and caused physical damage. This attack is considered in the literature as the 'birth of digital weapons' because it was the first time in history that malware was used to directly sabotage physical infrastructure (Zetter, 2014, 58). Stuxnet fundamentally changed strategic thinking about the cyber operation capabilities of states.

Since the 2000s, the healthcare, e-commerce, and banking sectors have become the most frequently targeted areas globally. For example, in 2015, an attack on the systems of the US healthcare company Anthem resulted in the theft of approximately 80 million citizens' personal data. Similarly, the 2014 JPMorgan Chase attack highlighted the risks facing the financial sector on a global scale (Kshetri, 2016, 78). These incidents demonstrated that digitizing sectors creates critical security dimensions for the private sector as well as for government policies.

The rapid advancement in cyber technologies observed since the mid-2000s has led to the widespread adoption of cloud computing-based applications at both the corporate and individual levels. This development has necessitated the strengthening of security protocols aimed at protecting data and information integrity; it has also triggered comprehensive improvement processes related to increasing the resilience of information systems in the face of growing threat vectors and attack surfaces. Cybersecurity, which covers a wide range from data security to ensuring system continuity, has become a strategic area at the center of both public policies and daily life practices today. The dynamic and constantly changing nature of human life makes it imperative to establish effective cybersecurity architectures and information systems that minimize risks (Kestane & Kurt, 2024). Cisco, known for its network, cloud, and cybersecurity solutions, stated at the beginning of 2013 that 8.7 billion devices were connected to the internet and emphasized that this number reached forty billion at the beginning of the 2020s.

According to Kestane, with the advancement of technology today, it is possible to encounter new types of malware every day. The main types of malware that we frequently encounter today are viruses, worms, spyware, adware, Trojan horses, botnets, rootkits, ransomware, and backdoors. These enable cyberattacks (Kestane, 2025). Today, a serious fight is being waged against these attacks worldwide. It is believed that if serious cybersecurity policies are not followed against cyberattacks, this situation will pose a great threat to the existence and security of the world.

The Development Process of Cybersecurity in Turkiye

According to Bıçakçı, as was the case globally, cyberattacks were primarily regarded as legal issues in Turkiye before becoming a serious security concern. However, as it became evident that cyberattacks posed significant threats to air, naval, and ground forces, the military began to prioritize this issue. This is because warfare has now shifted from the traditional understanding to cyberattack-based warfare. These attacks occurred both externally and internally. Therefore, measures needed to be taken against cyberattacks. In this context, cybercrimes were first included in Turkiye as a result of the amendment made to the Turkish Penal Code No. 3756 on June 16, 1991. This law listed what constitutes digital crimes and specified the criminal penalties for them (Bıçakçı et al., 2015, 4). Since then, serious measures have been taken in Turkiye's domestic legal system against cyber threats, and serious measures have also been taken through international agreements.

The situation described above began to change positively in 1997 with the implementation of certain studies within TÜBİTAK. In this context, the "TÜBİTAK National Institute of Electronics and Cryptology (UEKAE)" was established in 1997 under the name "Information Systems Security Unit" and began its work. Later, UEKAE separated from the Information Systems Security Unit and continued its work as a separate institute within TÜBİTAK BİLGEM. This structure, named the Cyber Security Institute, has prepared a great deal of information, documentation, legislation, and documents related to information technology security and cybersecurity, among other areas, in Turkiye. In other words, it has carried out serious work in this field (Fidancıoğlu, 2023: 5). This is particularly important as it demonstrates the positive development of cybersecurity efforts and policies against cyber threats in Turkiye.

Cybersecurity policies initiated within TÜBİTAK in Turkiye in 1997 and intensified in the 2000s are extremely important for the country's security. Cybersecurity is one of the essential issues that must be addressed to ensure national security, given Turkiye's current situation. In particular, the threats posed by cyber spies to Turkish companies and certain government institutions since the late 1990s have necessitated investment and efforts in the field of cybersecurity (Yıldırım, 2024). For this reason, since the early 2000s, serious efforts have been made under the leadership of TÜBİTAK within both the General Directorate of Security and the General Command of Gendarmerie.

In 1998, a highly significant step was taken in the field of cybersecurity in Turkiye. During this year, two committees were established to resolve, evaluate, and analyze issues arising in public institution computer networks and to address the economic challenges emerging in this domain. These were the PublicNet Supreme Council and the Public-Net Technical Council, both affiliated with the Prime Minister's Office. These councils first organized the "Public Computer Networks Conference" in 1998, where an action plan proposal related to cybersecurity was made. These councils continued their work on e-Turkiye until 2002 (Çetinkaya, 2017). The establishment of the Kamu-Net Supreme Council and the Kamu-Net Technical Council should be considered an important step. This regulation paved the way for subsequent work in the field of cybersecurity.

As part of efforts in the field of cybersecurity, the "Turkiye National Information Infrastructure Master Plan" was established in 1999. Supported by the Ministry of Transportation of the Republic of Turkiye, work on this plan was initiated by TÜBİTAK-BİLTEN in 1998 and continued until the project was updated in 2000. In particular, efforts were made to establish infrastructure related to Public Information Technologies and to take the necessary measures in this regard. Later, within the scope of the project called TUENA (Turkiye National Information Infrastructure Master Plan), a national assessment study was conducted on topics related to cybersecurity, and a "master plan" was created that outlined what Turkiye needed to do regarding its "National Information Infrastructure" until 2010 (Ünsal, 2002, 48).

At the very beginning of the 2000s, the Ministry of National Defense carried out a legal study titled "Law on the National Information Security Organization and Its Duties." This legal study planned to establish a supreme council under the Prime Ministry and a public legal entity called the "Presidency

of the National Information Security Agency" to ensure complete security in the field of information technology. Work was also carried out on the necessary infrastructure for this purpose (Karasoy & Babaoğlu, 2021). However, despite the serious efforts that went into preparing this law, it did not come into force.

Between 1999 and 2000, an important law was drafted in Turkiye in the field of cybersecurity. This law is of vital importance in terms of cybersecurity. As is well known, with the increase in cyber threats and dangers, states have had to focus on cyber intelligence activities and allocate significant budgets to this area. This is because cyberattacks cause damage to countries' e-government infrastructure and internet systems, posing serious threats to the existence of states. Turkiye is one of the countries affected by this situation. For this reason, serious plans and efforts are being made in Turkiye regarding cybersecurity, and necessary measures are being taken against attacks. The first effort in this regard was the enactment of the "National Information Security Organization and Its Duties Bill," which was established in 1971 and developed in 2000 (Kutlu et al., 2018). This law provides detailed regulations to ensure that e-government services across the country can be carried out securely. This law is extremely important as it established the first regulations regarding e-government services in Turkiye and prepared the first strategy document and action plan in this regard.

According to Kurnaz and Karatepe, the Information Systems Security Unit was established within TÜBİTAK in 2012. This unit is extremely important in terms of cybersecurity. This is because, in addition to the speed and convenience they provide, information technologies also have numerous drawbacks in terms of cybersecurity. This situation demonstrates how important information systems are. Today, Turkiye is a country that relies on automation systems much more than in the past. Therefore, Turkiye must keep many systems under control, especially national security. Information systems, one of these systems, are particularly vulnerable to cyberattacks. Therefore, it is extremely important to take measures against cyber threats and dangers throughout the country and to carry out related work (Kurnaz & Karatepe, 2019, 2). The Information Systems Security Unit plays a crucial role in this process and in taking precautions against malicious processes.

The Eighth Five-Year Development Plan (2001–2005) adopted in 2001 is significant in terms of national scientific security and cybersecurity. The following objectives were set within the framework of this plan: "a) Access to information will be facilitated by developing the national information infrastructure. b) Internet access capacity will be upgraded to the level required by international developments, and legal and institutional regulations will be implemented within the framework of international rules and standards to develop e-commerce and ensure information security. c) The telecommunications service capacity will be developed at a global level" (Eighth Five-Year Development Plan, 2001: 227). As can be seen, the aforementioned development plan contains significant developments likely to occur in terms of cybersecurity. This plan paved the way for positive steps to be taken regarding Turkiye's security in the coming years.

Security is one of the most important issues in Turkiye's Eighth Five-Year Development Plan. The subheadings of the concept of security are listed as Cyber Security, Transportation and Transport Security, Occupational Health and Safety, General Security, and Disaster Security; however, upon examination of the text, it is noteworthy that the most emphasis is placed on Cyber Security (Biçkin, 2024, 34). This situation is significant as it is the greatest indicator of the degree to which the Republic of Turkiye is sensitive to cybersecurity, even in its development plans.

In terms of cybersecurity, the e-Turkiye Initiative Action Plan was prepared in 2002. In this context, the Prime Ministry Circular dated June 19, 2002, entitled e-Turkiye, states: "In order to achieve one of our country's most important national goals, namely reaching the level of modern civilization, it is necessary to have a competitive, dynamic, and knowledge-based economy and to ensure the transformation into an information society. The implementation of e-Turkiye, with the aim of determining the necessary strategies and establishing and implementing a national information policy, is among the important priorities of our government" (Naralan, 2010). This circular shows the extent to

which strong plans were made to ensure national security with Turkiye's transition to the e-Turkiye system.

According to Aydın, two studies conducted in the 2001–2002 period under the leadership of the State Planning Organization in collaboration with TÜBİTAK to comply with e-Europe+ criteria marked a turning point in terms of cybersecurity. These are two different projects called e-Turkiye and e-Transformation Turkiye, respectively. The two projects mentioned above are important in that they were the first to establish a clear strategy and set concrete goals regarding information technologies in the public sector in Turkiye, thereby ensuring coordination among state institutions (Aydın, 2005). The work of the e-Transformation Turkiye Project has been carried out by the Information Collection Department of the State Planning Organization since 2003. It must be acknowledged that these are very important steps in ensuring cybersecurity in Turkiye.

Since 2003, the increasing use of the internet throughout Turkiye has necessitated certain measures. One of these is the "2003–2004 Short-Term Action Plan (KDEP)." This action plan set out a number of objectives that differed from previous regulations on cybersecurity. One of these objectives, "Technical Infrastructure and Information Security," involves the "TÜBİTAK National Institute of Electronics and Cryptology Research (UEAKE)," which aims to ensure security (Karasoy & Babaoğlu, 2021). Reviews conducted after the announcement of this plan indicate that progress has been made in this area, yielding positive results in terms of internet security.

In the context of cybersecurity efforts in Turkiye in 2005, the "TÜBİTAK BİLGEM Network Security" structure was established to ensure the security of information systems in public institutions. TÜBİTAK BİLGEM Network Security provided training to individuals working in critical state units and those working in the information processing departments of universities. Similarly, the "Cyber Security Institute," established under the aforementioned structure, conducted a number of security tests to protect the infrastructure of critical state institutions and organizations, particularly water, communications, and energy facilities, which are vulnerable to "smart systems" (Çakır & Taşer, 2023). In this way, the work in the field of cybersecurity that began in the early 2000s has continued uninterrupted.

The Law No. 5651 on the Regulation of Publications Made on the Internet and the Fight Against Crimes Committed Through These Publications, enacted in 2007, is an important step taken in the field of ensuring cybersecurity. According to Kılınç, the main purpose of this law is to provide the means and access to connect to the internet, to determine the responsibilities of users as a whole, and to determine the means and methods of intervention in crimes committed via the internet in coordination with service provider companies. With the enactment of this law, Turkiye's "internet content policy" has been consolidated under a single legal text, and the protection of families and children has also been ensured (Kılınç, 2016). In other words, this law protects citizens, children, and young people from harmful content and programs on the internet.

By 2008, the "Electronic Communications Law" was enacted, marking another step toward establishing cybersecurity. Although this law is not entirely new in terms of the planned system for examining the administrative procedures related to the appointment of certain individuals for work to be carried out in the areas specified under the name of communication services and the manner in which public sector services are performed, it is nevertheless extremely important in that it pioneers the re-examination of certain concepts related to established administrative law. In this context, if certain technical aspects known in terms of administrative procedures are not taken into account among the types of authorization regulated by Law No. 5809, such as "notification" and "granting of usage rights," there is no doubt that the authorization process can be carried out through certain procedures that can be described as unilateral by the administration. In light of the problem of determining the place of authorizations within the methods of having services in the public sector performed by individuals in the private sector, it has become necessary to review the state–public service relationship (Öztürk, 2009).

As part of cybersecurity efforts, three cybersecurity exercises were conducted in Turkiye in 2008, 2011, and 2013, with the goal of reaching a total of three exercises by 2020. In 2020, a large-scale

cybersecurity exercise was carried out, bringing the total number of exercises to four. Led by TÜBİTAK and BTK, the 2011 national exercise involved 200 participants with the support of 41 public and private institutions. Among the 200 participants were experts in education, health, finance, defense, and law, in addition to information technology specialists. The 2013 exercise was more comprehensive, with a total of 61 public and private institutions participating as stakeholders, including 20 institutions as observers (Bıçakçı et al., 2015: 35). These exercises in the field of cybersecurity are important in that they demonstrate Turkiye's preparedness against cyberattacks. This is because these exercises involved planning what could be done in the face of threats to national security in the cyber environment.

In 2009, the National Security Policy Document placed particular emphasis on cybersecurity. The National Security Policy Document underscored the importance of cybersecurity for national security and the need to increase efforts in this area. According to Yıldırım, documents prepared in Turkiye at certain times in the context of national cybersecurity strategies establish new plans and set goals to keep pace with rapidly developing technology. For this reason, budget planning and investments are made for cybersecurity. In this context, Turkiye is a country that works with other institutions and organizations from a multidisciplinary perspective and strives for development to ensure cybersecurity (Yıldırım, 2024). The preparation of the 2009 National Security Policy Document also points to this.

Significant institutional and strategic developments in the field of cybersecurity were observed in Turkiye during the 2010–2012 period. In this context, cyber threats were assessed at the National Security Council meeting held on October 27, 2010, and it was decided that this area would be included in the National Security Policy Document. Subsequently, the 1st National Cybersecurity Exercise was held on January 25–28, 2011, in collaboration with TÜBİTAK and the Information and Communication Technologies Authority. The report published after the exercise found that Turkiye was significantly vulnerable to cyberattacks and that public institutions and organizations were not sufficiently implementing the necessary protective and preventive measures.

While this issue was being handled with such sensitivity, a hacker group called Redhack launched cyberattacks on many government agencies providing services through e-government, seriously compromising the security of Turkiye's e-government system. In 2015, an attack on a bank resulted in the theft of millions of people's card details, causing widespread public concern. Similarly, in 2016, the simultaneous DDoS attacks that disabled the websites of many public institutions heightened concerns about the security of Turkiye's critical infrastructure (Yıldırım, 2024). In order to take precautions against similar threats, the "Regulation on the Implementation, Management, and Coordination of National Cyber Security Activities" came into force as a result of a decision taken by the Council of Ministers on October 20, 2012. Within this framework, the aforementioned Council of Ministers Decision and the "Electronic Communications Law" authorized the Ministry of Transport, Maritime Affairs, and Communications to prepare strategy documents and action plans related to cybersecurity (Kutlu et al., 2018).

As of 2013, the other institution authorized to prepare national strategy documents in the cyber domain in Turkiye, apart from the Ministry of Transport, Maritime Affairs, and Communications, is the "National Cyber Incident Response Center." Within the scope of the "2013–2014 National Cyber Security Strategy and Action Plan," approved by the Council of Ministers Decision No. 2013/4890, was adopted. Within the scope of this strategy, the "National Cyber Incident Response Center (USOM, TR-CERT)" was established within TÜBİTAK to conduct studies on what measures could be taken against situations posing a threat to cybersecurity throughout the country and what regulations could be made in this regard, and to share these studies with relevant institutions and organizations (Gündoğdu, 2023). These developments clearly demonstrate the rapid pace of progress in the field of cybersecurity in Turkiye since 2010 and the swift enactment of relevant laws, which have directly contributed to the strengthening of national cybersecurity strategies and paved the way for enhancing USOM's operational capacity.

According to Darıcılı, in addition to the establishment of USOM in 2013, the Turkish Armed Forces also took several steps in the field of cybersecurity. In this context, the establishment of the Cyber Defense Command was announced in 2013 with a brigade-level structure. The duties of this unit are defined as ensuring the cyber defense of all systems in the cyber environment used by the Turkish Armed Forces, responding to cyber incidents on a 24/7 basis, participating in national and NATO-related international exercises, conducting awareness and training activities throughout the army, and regularly conducting cybersecurity audits and tests on networks used by the armed forces (Darıcılı, 2019).

Significant steps have been taken in the field of cybersecurity within the Turkish Armed Forces as well as within the General Directorate of Security. Again, in 2013, the Department of Combating Cybercrime was established within the General Directorate of Security. When this process is examined, it is seen that the security organization has a traditional, top-down hierarchical, authoritarian, and centralizing organizational culture; and that the system of relationships is largely shaped by written rules. However, it is accepted that the organization has made changes to its institutional structure in order to adapt to new needs arising from social and societal transformations and thus has the capacity to create new units to perform different functions (Taşçı & Can, 2015: 238). This reveals that, like the armed forces, the security organization also follows technological developments in the fight against crime and criminals and takes steps in this direction.

As with the General Directorate of Security, a Cybercrime Combat Department has been established within the General Command of Gendarmerie in the field of cybersecurity. Today, both law enforcement agencies are accelerating the recruitment of personnel needed to develop their cyber investigation capabilities and are making plans to combat cybercrime more effectively. In this context, the establishment of R&D laboratories within the General Command of Gendarmerie and the development of project incentive mechanisms aim to eliminate institutional shortcomings that prevent the participation of IT experts working in the public sector, private sector, and universities in these processes (Çakır & Taşer, 2023).

The institutional framework for critical infrastructure security in Turkiye was shaped by the Roadmap for the Protection of Critical Infrastructure published by AFAD in 2014. This document defined AFAD's cybersecurity objectives for the 2014–2023 period, established the theoretical basis for the concept, and classified critical infrastructures by sector. Prior to this document, critical infrastructure was mostly evaluated in terms of cybersecurity. However, critical infrastructure refers to all fundamental physical and non-physical elements of the country that could lead to loss of life, property, and reputation if damaged. In this context, critical infrastructure in Turkiye has been defined in ten main sectors: energy, transportation, health, communications, agriculture and food, water management and dams, culture and tourism, banking and finance, critical public services, and critical production/commercial facilities. The studies also identified sub-sectors in the fields of energy (natural gas, electricity, solid fuels) and transportation (sea, land, rail, and air) (Tanrıverdi et al., 2023). From the perspective of national security, great importance is attached to both cybersecurity policies and the protection of the aforementioned locations.

Within the scope of cybersecurity, Law No. 6698 on the Protection of Personal Data came into force in 2016. In an era where cybersecurity is so important, the enactment of this law became a necessity. According to Bilir, while the right to protection of personal data has been institutionalized within the normative framework developed by the European Union, it has also become the focus of legal debates in Turkiye due to the acceleration of technological transformation. This right was initially defined as a fundamental guarantee in the Constitution and was later systematically regulated in its normative and institutional dimensions through a special law. The aforementioned law also provided for the establishment of the Personal Data Protection Authority as an independent administrative authority to oversee the implementation of the personal data protection regime, enforce sanctions, and perform regulatory and supervisory functions (Bilir, 2023). As stated, everyone's personal information and data must be protected, and this law guarantees this.

The Turkiye Cybersecurity Cluster project, which emerged in 2017 with the participation of relevant public institutions, the private sector, and academics, and is supported by the Presidency of Defense Industries, is currently underway. This project aims to create a collaborative and coordinated working environment for companies that develop domestic and national cybersecurity products and services. In addition, the International Cybersecurity Federation, established to raise cybersecurity awareness in the public sector and create a system based on advanced technology, is also active in the field of cybersecurity.

In the context of cybersecurity, the Digital Transformation Office was established in Turkiye in 2018 following the transition to the Presidential System. Among the departments under the Presidency of the Digital Transformation Coordination Directorate are the Directorate of Digital Technologies, Procurement and Resource Management Directorate, Digital Expertise, Monitoring and Evaluation Directorate, Cybersecurity Directorate, Big Data and Artificial Intelligence Applications Directorate, International Relations Directorate, Information Technologies Directorate, Management Services Directorate, and Legal Advisory Services. Established in 2018, this office is planned to lead the development of digital public administration (Boy Çaykara, 2024: 105). The office and its components are engaged in serious work.

According to Ağdeniz, the Information and Communication Security Measures Circular published in 2019 in the field of cybersecurity is an important regulation aimed at strengthening national information security standards. The main purpose of the circular is to reduce or eliminate information security risks and to determine the minimum security measures for protecting critical information and data that could threaten national security or cause disruptions to public order if their confidentiality, integrity, or availability is compromised. In this context, the circular also defines the framework for activities related to the implementation of these measures at the institutional level (Ağdeniz, 2021). Given that protecting and storing information is extremely difficult today due to cyberattacks, this law can be considered helpful in solving this problem.

As outlined above in a specific chronological order, significant steps are being taken in the field of cybersecurity in Turkiye. One of these is the opening of the first Cybersecurity High School in Istanbul in 2020. In this context, the Istanbul Provincial Directorate of National Education has established a curriculum based on cybersecurity with the aim of training young people who are sensitive to cybersecurity issues. Shortly thereafter, the Teknopark Istanbul Vocational and Technical Anatolian High School was established to focus on cybersecurity (Uluç & Eyüpoğlu, 2024).

Discussions

The present study seeks to confirm a topic that has been frequently discussed in the literature regarding the provision of international security. Specifically, it aims to demonstrate that cybersecurity is not only a technical issue, but also a policy product that is of such significance that it cannot be disregarded in the establishment of national security.

Indeed, consistent with global trends, awareness in Turkiye has increased since the early 1990s. This growth has been driven by the expansion of the legal framework and the restructuring of institutional structures to align with technological advancements. This situation illustrates the evolution of cybersecurity at both the national and global levels, driven by analogous motivations, in tandem with advancements in technological history.

When evaluated in conjunction with the theoretical framework of the study, these findings reveal that Turkiye's cybersecurity policies are particularly consistent with the Realist and Securitization approaches. In contrast, the “individual and society-centered cybersecurity culture” emphasized by the Critical Security approach is still in its developmental stage at the institutional level in Turkiye.

The developments covered chronologically in this study emphasize that cybersecurity is critical not only for ensuring the security of nations, but also for protecting the privacy of citizens and ensuring the secure continuity of economic life. As highlighted in the literature, cyberattacks targeting the finance and especially banking sectors, particularly since the year 2000, known as the millennium, have made it imperative for nations and private companies to develop active policies.

Taking Turkiye as an example, it is observed that cybersecurity is central to the security elements of short-, medium-, and long-term development plans and national strategy documents. However, some studies emphasize that regulations regarding cybersecurity in Turkiye are generally reactive policies, implemented to resolve incidents or threats in the cyber domain after they have occurred. This situation highlights the importance of implementing long-term strategies and proactive approaches to ensure effective cybersecurity.

Another point open to debate is the training dimension of personnel tasked with ensuring cybersecurity. Findings highlight the importance of cybersecurity high schools, established in 2020 as a commendable initiative, in raising awareness among young people and preparing them for the age of cyberspace. However, the literature suggests that the education process should be introduced at an even younger age. This indicates that situational awareness regarding cybersecurity must be widespread not only at the institutional level but also among citizens and disseminated as widely as possible.

In conclusion, when international developments and the literature are compared with the findings obtained in Turkiye, it is observed that developed countries around the world and Turkiye have developed similar strategies, but there are some differences in terms of technological infrastructure development and resource utilization. In particular, the strategic importance of the goals of developing local and national technological products and integrating them into the field of cybersecurity is increasing day by day. Therefore, it is essential for Turkiye to strengthen and increase its domestic and national technological capacity while joining the global cybersecurity ecosystem. In this context, units established within TÜBİTAK, institutions and organizations such as USOM and TR-CERT have played an extremely important role in the development and expansion of the national cybersecurity network. The inclusion of cybersecurity in the National Security Policy Document and the implementation of cybersecurity exercises, sometimes involving deliberate violations, demonstrate the level of determination with which the issue is being addressed at a strategic level. Turkiye's sharing of information in the field of cybersecurity with international organizations such as NATO and the EU provides significant advantages. Turkiye's initiatives in this regard demonstrate its reflex in ensuring cybersecurity and stand out as a superior aspect in this field.

In summary, when examining Turkiye's efforts to protect its cybersecurity, it is observed that it has established and continues to implement the necessary legal regulations, handles the issue of education with sensitivity, and demonstrates a strong profile in terms of its cooperation with international organizations. However, certain weaknesses are apparent in the areas of localizing technological devices and software, developing new strategies with proactive approaches, and spreading and popularizing education. All these issues indicate that Turkiye needs comprehensive, proactive, long-term strategies based on policies that fully embrace cybersecurity, including software and technological devices, in order to become an effective player in the global cybersecurity ecosystem.

Conclusion

In the contemporary era, marked by significant scientific and technological progress, there have been profound developments in human life. However, concomitant with these advancements are multifaceted consequences, both beneficial and detrimental, on the global environment. Notably, the substantial advancement of technology underscores the imperative to safeguard and preserve information, particularly that pertaining to security, which is increasingly being transferred to digital environments. The failure to protect this information jeopardises security both regionally and globally. Consequently, specific measures have been implemented to protect this information. The concept of

cybersecurity is at the forefront of these measures. Thanks to cybersecurity, it is possible to prevent regional or global cyberattacks, thereby ensuring global security to a certain extent.

As is well known, today all information can be easily accessed in a digital environment. This makes it difficult to protect certain information and documents that are very important and sensitive in nature, which form the basis of state security. Indeed, thanks to advances in information and technology, ill-intentioned individuals can obtain information through various means, primarily spyware, posing serious threats to the security of institutions, organizations, regions, countries, etc. This necessitates a comprehensive, not just individual, response to such cyberattacks.

In the context of the information provided above, measures are being taken and new methods developed against attacks to ensure digital security in developed and developing countries, primarily in European countries and the United States, after World War II. In this context, the historical development of cybersecurity began to increase after World War II and showed significant growth in the 1970s. Subsequently, developments continued from the 1980s to the early 2000s and are still continuing unabated today. In essence, this historical development of cybersecurity stems partly from necessity. It is clear that if the necessary cybersecurity measures are not taken against cyberattacks, the world will be defenseless against serious threats.

Throughout the history of cybersecurity, the widespread use of computers and the internet has brought with it many problems. Significant developments in these two areas have led to the creation of new types of malicious software. These include viruses, worms, spyware, adware, Trojan horses, botnets, rootkits, ransomware, and backdoors. Each of these poses a threat to the security of digital data. Therefore, since the early 1980s, measures have been taken against these threats in terms of cybersecurity, and different methods have been researched to eliminate them. Consequently, this process constitutes an important part of the history of cybersecurity.

In today's world, where cyberattacks have increased significantly, Turkiye, like other countries, is severely affected by this situation. As a country in a sensitive location with a strong military, Turkiye must protect its land, sea, and airspace against cyberattacks. For this reason, measures have been taken to ensure cybersecurity in Turkiye since 1970, laws have been enacted, investments have been made in science and technology, and measures taken around the world against cyberattacks have been closely monitored. However, historically, work in the field of cybersecurity in Turkiye essentially began in the early 1990s, and significant developments have been recorded since the mid-2000s. In other words, the historical development of work related to cybersecurity in Turkiye parallels that of work carried out worldwide.

Work in the field of cybersecurity in Turkiye is generally carried out within TÜBİTAK. In addition to official institutions and organizations that play an effective role in Turkiye's defense systems, many ministries and legal units also provide support to TÜBİTAK. Since the early 1990s, numerous laws and regulations have been enacted in Turkiye, primarily legal regulations in the Turkish Penal Code. Furthermore, since the early 2000s, Turkiye has been conducting a number of exercises against cyberattacks, with support from many official and private institutions. In the context of historical developments, Turkiye has recorded such progress and advances in cybersecurity, and this situation continues unabated today.

In general, Turkiye's cybersecurity policies have shown a clear parallelism with global trends, particularly since 2010. However, as the theoretical literature also points out, proactive strategies, international cooperation, domestic technology investments, and social awareness must be addressed in an integrated manner to achieve an effective cybersecurity ecosystem.

Recommendations

In the contemporary global context, the rate of technological advancement has attained an unprecedented apex. Presently, a vast array of personal, informational, and corporate data is predominantly stored in cyberspace, accessible via computer systems. In light of this prevailing reality, ensuring the security of data and information assumes a paramount significance.

In the present study, a chronological examination of the development process of cybersecurity is undertaken, with the development of information systems having given rise to increased interest in the field. It is essential that both government and private business and transactions are carried out in a healthy manner, and to this end, importance must be given to cybersecurity, necessary measures must be taken, and awareness must be raised among all individuals, with education at the primary school level being the most logical place to begin if necessary. The cultivation of cybersecurity experts is of comparable significance to that of white hat hackers. The term "white hat hacker," a prevalent one in the extant literature, denotes experts who operate within an ethical framework to detect malicious attacks and remediate security vulnerabilities. Rather than causing unauthorized damage to systems, white hat hackers seek to enhance defense capabilities by disclosing security vulnerabilities in an authorized manner. In this capacity, they have become a critical component of cyber defense in both government institutions and the private sector (Cole, 2018, 92). As information systems are developed with the intention of streamlining processes, it is imperative that white hat hackers working to identify system vulnerabilities contribute to the development process and conduct continuous monitoring. Indeed, it is vital that they intentionally breach systems in order to ensure that they become more secure.

Declarations and Statements

1. Declaration of Researchers' Contribution: As the study was prepared by a single author, all stages were carried out by the author personally.

2. Conflict of Interest: There is no conflict of interest.

3. Ethics Report: No analysis was performed on the data in the study, and therefore no ethics committee report is required.

4. Research Model: A qualitative research model was employed in the study, and a compilation was meticulously crafted using the document analysis method, drawing upon both primary and secondary sources.

TÜRKÇE SÜRÜM

Giriş

Globalleşen dünya son derece hızlı bir şekilde değişmekte olup; bu değişim sürecinin en önemli sebebi olarak da siber uzayda yaşanan gelişmeler karşımıza çıkmaktadır. Gerek devletler gerekse devlet dışı aktörlerin kendilerine çıkar sağlama ve birbirlerine üstünlük kurma yarışına girdiği günümüz dünyasında siber saldırılar Devletlerarası asimetrik tehditlerin başında gelmektedir. Siber güvenliğin sağlanması devletlerin ve devlet dışı aktörlerin dikkatini çekerek başta ulusal güvenlik politikaları olmak üzere uluslararası alanda önemli bir gündem maddesi haline gelmiştir. Devletlerarası ilişkilerde ciddi bir etki olarak ortaya çıkan siber güvenlik, bugün birçok alanda etkin bir biçimde varlığını sürdürmektedir (Güntay, 2018). Bu sebeplerden mütevellit siber güvenlik, dünya genelinde bilim insanları tarafından araştırılan çok ciddi bir bilimsel konu halini almıştır.

Siber dünyanın güvenlik açısından en önemli yapılarından birisi haline gelmiş olan siber güvenlik, modern hayatın dijital olarak güvenliğini sağlayan bir olgudur. Bu nedenle bilim dünyasında siber güvenliğin ne olduğu hususunda çok sayıda tanım yapılmıştır. Ancak halen siber güvenliğin ana hatlarıyla kesin bir tanımı yapılmış değildir. Teknoloji dünyasının yaşayan bir organizma gibi gün be gün gelişim göstermesi bu alanda bir tanımlama yapılmasını çok da mümkün kılmamaktadır. Zira siber güvenliğin sınırları tam olarak çizilemediğinde; tanımı da hakiki bir biçimde yapılamamaktadır. Buna rağmen siber güvenlik, bugün insanlığın bilgi ve teknoloji alanında güvenliğinin sağlanmasında önemli bir güç haline gelmiştir (Tunca, 2019). Bu nedenle bugün olduğu gibi gelecekte de insanların en fazla üzerinde duracağı ve konuşacağı hususların başsında siber güvenlik gelecektir.

Karasoy'a göre İnsanların hayatına 1990'lı yılların başında çok hızlı bir biçimde giren siber güvenlik, uluslararası alanda başta ekonomi ve güvenlik olmak üzere insanları birbirine bağlamaktadır. Günümüzde güvenlik kuvvetleri, adli birimler, nüfus müdürlükleri, sağlık kuruluşları, bankacılık işlemleri, eğitim faaliyetleri, devletlerin alt ve üst yapı çalışmaları, istihbari bilgiler vs. gibi dijital veri yoğunluklu çalışan kurum ve kuruluşlarda bilginin muhafazası ve saklanması için siber güvenlik, çok büyük bir rol oynamaktadır. Zira bahsi geçen işlerin hepsi devletlerin güvenliği ve vatandaşların huzuru için gerekli olup; korunmaları ciddi önem arz etmektedir. Siber güvenlik, burada devreye girmekte ve bu bilgilerin korunması için gerekli dijital önlemleri almada etkin konumda bulunmaktadır. Bahsi geçen bilgilerin korunması dışında, bu bilgilerin depolanıp kullanıma açılması da önemlidir (Karasoy & Gezici, 2023). Dolayısıyla dijital ortamda bu bilgilerin güvenli bir biçimde paylaşıma sunulması için siber güvenliğin etkin bir biçimde devrede olması elzemdir.

Bilgiye ulaşmanın çok kolay hale geldiği günümüzde devletlerin güvenliğini teşkil eden hassas bilgilerin korunması gittikçe zorlaşmaktadır. Zira siber saldırılarla dijital verilere kolayca girebilen hackerlar, casus yazılımlar vb. illegal yollarla saklı kalması gereken bilgileri ortaya çıkararak dışarıya sızdırmaktadır. Bu durum, devletlerin güvenliği için tehdit ve tehlike oluşturmaktadır. Bunlara karşı kesin olarak önlemlerin alınması gerekir, bunun için de mutlaka siber güvenliğin daha da geliştirilerek aktif bir biçimde devrede olması sağlanmalıdır.

Yukarıda ifade edildiği üzere günümüz dünyasında siber güvenlik, dünya genelinde güvenliğin gerçek anlamda sağlanabilmesi için çok önemlidir. Zira teknolojinin çok geliştiği 21. Yüzyılda hem dünyanın hem de çalışma konumuz olan Türkiye'nin güvenliği tehdit altındadır. Bu nedenle 1990'lı yıllardan beri bütün dünya ülkelerinde ve Türkiye'de dijital güvenliği tehdit eden her tehlikeye karşı siber güvenlik unsurları devreye girmektedir.

1990'lı yılların başından beri dünya genelinde siber güvenlik alanında çok hızlı gelişmeler göze çarpmaktadır. Ciddi bir kaynak taraması yapılarak hazırlanan bu çalışma, iki bölüme ayrılmıştır. Birinci bölümde siber güvenliğin dünyadaki gelişiminin tarihsel süreci irdelenirken; ikinci bölümde de

Türkiye'de 1990'lı yılların başından günümüze kadar siber güvenlik alanında ne gibi gelişmelerin olduğu hususu ayrıntılı bir biçimde izah edilmeye çalışılmıştır. Konuyla ilgili bilimsel çalışmalardan istifade edilerek hazırlanan bu makalede doküman analiz tekniği ile karşılaştırmalı analiz yöntemi kullanılmıştır. Birçok eserden istifade edilerek oluşturulan bu makaleyle siber güvenlik alanında çalışan kişilere faydalanabilecekleri ciddi bir kaynak ortaya çıkarılmaya çalışılmıştır. Bu çalışma genel itibariyle "Siber güvenlik kavramı, uluslararası güvenlik çalışmalarının teorik çerçevesinde tarihsel bağlamda ne şekilde gelişim göstermiş ve bu gelişim Türkiye'de hangi dinamikler ışığında şekil almıştır?" sorusuna cevap aramaktadır. Araştırmaya bu soru açısından bakmak, hem kronolojik olarak tarihsel değişimi anlamayı hem de uluslararası güvenlik perspektifini beraberce ele almayı mümkün kılmaktadır.

Amaç

"Uluslararası Güvenlik Çalışmaları Bağlamında Siber Güvenliğin Tarihsel Gelişimi Üzerine Bir İnceleme: Türkiye Örneği" adlı çalışmanın hazırlanmasındaki amaç 1990'lı yıllardan beri insanların hayatında ciddi bir biçimde yer tutan siber güvenliğin nasıl bir gelişme göstermiş olduğunu ortaya çıkarmaktır. Bu amaç doğrultusunda siber güvenliğin hem dünya genelinde hem de Türkiye'de hangi aşamalardan geçerek bugüne geldiğinin ortaya çıkarılması hedeflenmektedir. Bu çalışmanın hipotezi: "Siber güvenliğin gelişimi, dijital altyapılar devlet güvenliğinin temel öznesi olarak güvenlik politikalarının merkezine alındığı vakit hız kazanmakta ve küresel eğilimlerle birlikte ele alındığında Türkiye'deki gelişimi de bu minvalde paralellik arz etmektedir" görüşü üzerine kurulmuştur. Çalışmanın hipotezi doğrultusunda Türkiye'de siber güvenlik alanındaki gelişmeler tarihsel perspektiften ele alınarak alana katkı sağlamak amaçlanmıştır.

Yöntem

Literatür taraması yapılarak çok sayıda bilimsel eserden istifade edilerek hazırlanan bu makalede doküman analiz tekniği, doküman analizi içerik tekniği ile karşılaştırmalı analiz yöntemi kullanılmıştır.

Doküman analizi kapsamında incelenen kaynaklar; ulusal strateji belgeleri, TÜBİTAK raporları, kalkınma planları, akademik makaleler ve resmi mevzuat metinlerinden oluşmaktadır. Bu kaynaklar, yayın yılı, kurumsal güvenilirlik ve siber güvenlik bağlamına uygunluk kriterlerine göre seçilmiştir.

Karşılaştırmalı analiz tekniği ise siber güvenlik politikalarının küresel gelişimi ile Türkiye'deki uygulamaların zaman içindeki görünümü karşılaştırılarak uygulanmıştır. Bu süreçte özellikle 1990 sonrası gelişmeler analitik olarak sınıflandırılmıştır (Bowen, 2009).

Bulgular

Konuya ilişkin olarak ciddi bir biçimde literatür taraması yapılmış ve konu ayrıntılı bir biçimde ele alınmaya çalışılmıştır. İki başlık halinde ele alınan konular, hakkında değerlendirmeler de yapılmıştır.

Elde edilen bulgular, literatürde belirlenen kuramsal yaklaşımlarla birlikte ele alındığında şu sonuçlara ulaşılmıştır:

• Siber güvenliğin 1990 sonrasında yaşadığı küresel gelişim, Realist yaklaşımın savlarında yer verdiği şekilde devletlerarası güç mücadelesi ekseninde hız kazanmıştır (Baylis & Smith, 2017, 301).

• Türkiye'de yaşanan tarihsel gelişim, 2010 sonrası dönemde hız kazanmış ve özellikle Kopenhag Okulu'nun öngördüğü güvenlikleştirme modeli çerçevesinde ilerleme kaydetmiştir.

• Lakin, Türkiye'de siber güvenlik farkındalığını toplumsal tabana yayma çabaları eleştirel güvenlik perspektifi bağlamında ele alındığında, henüz sınırlı düzeydedir.

Kuramsal Çerçeve: Uluslararası Güvenlik Yaklaşımları ve Siber Güvenlik

Siber güvenliğin uluslararası güvenlik çalışmalarındaki yerinin anlaşılabilmesi için öncelikle temel kuramsal yaklaşımların değerlendirilmesi gerekmektedir. Siber uzayı devletlerin güç mücadelesinde yeni nesil bir boyut olarak ele alan realist yaklaşım, siber saldırıları ulusal güvenliğe kasten yapılmış tehdit olarak yorumlar (Walt, 1991). Kopenhag Okulu ise, siber güvenliği 'sektörel güvenlik' bağlamında ele alarak, dijital altyapının güvenlikleştirilmesi sürecinin hayati önemine dikkat çekmektedir (Buzan, Wæver & de Wilde, 1998, 27). Öte yandan Eleştirel Güvenlik Çalışmaları da siber güvenliğin sadece devlet merkezli değil, teknolojik, toplumsal ve bireysel etkileşimi kapsayan çok kriterli bir süreç olduğunu savunur (Booth, 2007, 145). Yukarıda ele alınan ve kısaca açıklanmaya çalışılan kuramsal yaklaşımlar, çalışmanın genel gidişatında yapılacak analizler için açıklayıcı bir çerçeve sunmaktadır.

Uluslararası Alanda Siber Güvenliğin Gelişim Süreci

1990'lı yılların başından itibaren insanların hayatına giren ve savunma için ne kadar önemli olduğu anlaşılan siber güvenliğin daha iyi bir biçimde anlaşılabilmesi için bu kavram hakkında dünya genelinde ciddi araştırmalar yapılmaktadır ve yapılması da gerekir. Siber güvenliğin dünyadaki tarihsel gelişimine bakıldığında 1990'dan günümüze kadar farklı birçok kavramın ortaya çıktığı anlaşılmaktadır. Bu kavramlar arasında "siber savaş", "siber varlık", "siber olay", "siber zorbalık", "siber casusluk", "siber silah", "siber polis", "siber suç", "siber suçlarla mücadele", "siber terörizm", "siber terörist", "siber saldırı", "siber tehdit", "siber savunma", "siber psikoloji", "siber sağlık" vb. yer almaktadır. (Sağıroğlu, 2018, 21). Görüldüğü üzere günlük hayatta kullanılan pek çok terimin başına siber kelimesi eklenmiş ve bu yeni kelime grupları günümüzde sıkça kullanılmaktadır.

Uluslararası arenada ABD ve AB ülkeleri başta olmak kaydıyla çok sayıda ülke, uluslararası örgüt, kurum ve kuruluş siber güvenliğin tesisi için bilgi paylaşımı yapmakta önemli bilgilerin güvenli paylaşımı konusunda iş birliğine gitmektedir. Siber güvenliğin uluslararası alanda sağlıklı tesisine plan ve programlar yapılarak geleceğe dönük ciddi adımlar atılmaktadır (Ünver vd., 2011, 1). Bu durum uluslararası güvenlik çalışmalarında siber güvenlik olgusunun son derece önemli olduğunu ortaya koymaktadır.

Peki, böylesine önemli olduğu değerlendirilen siber güvenliğin ortaya çıkışı ve uluslararası alanda etkin bir duruma gelişi nasıl olmuştur? Esasında siber güvenlik tek başına çok da bir şey ifade etmemektedir. Siber güvenlik başta bilgi işlem ve dijital sistemler başta olmak üzere birbirine internet ağlarıyla bağlı olan elektronik cihazlar ve bunları korumaya yönelik olan güvenlik önlemlerinin tamamıdır. Bundan dolayı hızla gelişen dijital dünyada siber güvenliğin bir bütün halinde ele alınması gerekir (Solmaz, 2011). Zira günümüzde dünya genelinde çok ciddi siber saldırılar gerçekleşmekte ve bunlara karşı devletlerin önlemler alması gerekmektedir. Bu sürecin tarihsel gelişimi, hızlı bir biçimde olmakta ve buna yönelik önlemler de 1990'lardan beri giderek artmaktadır. Aynı durum, Türkiye için de geçerlidir.

Siber güvenliğin tarihsel gelişimi açısından ilk bilgisayarların icat edilmesi ve kullanılması, birinci süreci oluşturmaktadır. İkinci Dünya Savaşı sırasında ve sonrasında meydana gelen gelişmeler ulusal güvenliğin sağlanmasından sınır güvenliğinin sağlanmasına kadar güvenlik ile ilgili alanlarda sadece insan ve silaha dayalı askeri yöntemlerin yetersiz kaldığının anlaşılmasını sağlamış ve güvenlik alanına teknolojinin adapte edilmesini zorunlu kılmıştır. İcat edilen ilk bilgisayar da öncelikle askeri alanda kullanılmıştır.

Bu bağlamda Alan Turing isimli bilim adamı İkinci Dünya Savaşı devam "algoritma" ve "hesaplamalar yapabilen" basit bir hesaplama makinesi olan "*Turing Makinesi*" ni icat etmiştir. Bu sırada ABD, olumsuz hava koşullarına bağlı olarak hedeflerine gidemeyen uçak vb. savaş araçlarının

hedeflerini kolayca belirleyebileceği bir teknolojik sistem kurmaya çalışmıştır. Bunun için yapılan bilimsel çalışmalar neticesinde 1943'te "*John Mauchly*" ve "*Presper Eckert*" ilk dijital anlamdaki bilgisayar olarak kabul edilen "Elektronik Sayısal Bütünleştirici ve Bilgisayar (ENIAC)" adlı bilgisayarı 1946'da icat etmişlerdir (Gündoğdu, 2023). Esasında 1940-1950 yıllarında dünyada sadece birkaç bilgisayar üretilmiş ve birçok insan bilgisayarın varlığından haberdar olmamıştır. Siber güvenlik açısından 1950'lerden itibaren teknolojik gelişmeler ciddi ilerlemeler kat etmiştir.

1950'lerde güvenliği tehdit etmeye başlayan siber suçlar ortaya çıkmaya başlamıştır. Bu çerçevede 1950'lerde ABD'de gelişmeye başlayan "*Hippi Hareketi*" olarak adlandırılan açık kaynaklı olan programlar içerisinde çok ciddi bir bağlantı bulunmaktadır. Bıçakçı'ya göre; "*Hippilerin kabul edilmiş kurallara karşı asi duruşu bilgisayar temelli teknolojik gelişmelerin ana felsefesini bina etmiştir. Massachusetts Institute of Technology laboratuvarlarında taban bulan bu felsefede programcılar ya da Steven Levy'in anlatımıyla hacker programlar yazılıp bunların kodlarını arkadaşlarının kullanımına sunarlardı. Diğer yazılımcılar da ihtiyaçları ölçüsünde, yazılan bu kodları geliştirip kendi emellerine göre düzenlemiştir. Burada tamamen kişisel tercihlerle ve özgürce paylaşımlar yapılırdı. Burada paylaşımın arkasındaki açık kaynak felsefesi öne çıkmaktaydı. Hippilerin de benzer felsefeye sahip olmaları bu hareketin hackerlar tarafından desteklenmesini sağlamıştır*". (Bıçakçı, 2014). Bu şekilde ABD'de hackerların ortaya çıkmasıyla birlikte dünyada başta askeri olmak üzere birçok alanda güvenliği tehdit etmeye başlayan siber suçların da temeli atılmış olmaktaydı.

Siber güvenlik açısından 1960'larda bilgisayarların önemli ölçüde gelişme göstermesiyle birlikte etkisini büyütmeye çalışan siber suçlar da dünya için tehlike oluşturmaya başlamıştır. Bu çerçevede iletişim teknolojilerindeki gelişmelerle birlikte dünya bir neosfer, farklı anlatımlarda kullanıldığı haliyle yerkürenin bir yandan bir yanına uzanan bir "zihin âlemi", bir "düşünen döngü", "harikulade bir düşünme makinesi", fiber ve ağlarla dolu bir "düşünen kılıf" ve gezegen çapında bir "bilinç" doğurmuştur. Özdemirci'ye göre dünya genelinde görülen her bir olayın ve gelişmenin özünde bilginin ortaya çıkmaya başladığı dünyada canlıların varlıklarını sürdürdükleri yerde, yani "Biyosfer" olarak adlandırılan katmanda canlıların varlıklarını sürdürebilmesi için bir şart daha bulunmaktadır. Bu da bilginin ve zekanın gelişmesi sonucu, ortaya çıkan yeni hayat koşullarıdır. (Özdemirci & Torunlar, 2018). Bu yeni hayat koşulları da doğal olarak siber güvenliğin ne kadar önemli bir duruma gelmeye başladığını ortaya çıkarmaktadır.

Siber güvenlik açısından 1969 yılı son derece önemlidir. Zira bu yıl, *ARPANET60* adındaki ilk bilgisayar ağı Stanford Araştırma Enstitüsü, Santa Barbara Üniversitesi, Los Angeles'taki California Üniversitesi ve Utah Üniversitesi'nde kurularak devreye alınmıştır. Önceleri sadece ABD'nin Savunma Bakanlığı ile birlikte çalışan kurum ve kuruluşlara açık olan sistem, zaman içerisinde bilim adamları tarafından bilimsel amaçlı iletişim kurmak için de kullanılmaya başlanmıştır. Esasında daha çok askeri alanlarda araştırma ve inceleme yapmak amacıyla geliştirilen söz konusu iletişim ağının bilim insanlarınca yoğun bir biçimde kişisel sohbetler için de kullanılmaya başlanmasından sonra; bahsi geçen bu iletişim ağı bütün bilim insanları tarafından kullanılmaya başlanmıştır (Sancakdar, 2021, 16). 1969'dan itibaren bilgisayarların askeri amaçlı kullanılmaya başlanması, doğal olarak başta ABD olmak üzere birçok gelişmiş ülkede siber güvenliği öncelikli bir duruma getirmiştir.

Ünver'e göre siber güvenlik bağlamında "*İleri Araştırma Projeleri Ajansı*" (ARPA) için bu, ABD'de ülke çapında başta Pentagon olmak üzere farklı kurumlardaki kişilerin, bilgisayarların kullanım dışı olduğu olduğu zamanları verimli hale getirmenin ve farklı çalışmalar yapan insanların yararlanmasını mümkün kılmanın yollarını bulmak anlamına gelmiştir. Çalışmalar özellikle üniversiteler arası veri aktarımına çaba sarf etmiş, 1971 yılında ilk "elektronik posta" gönderilmiş ve 1969'da Florida Üniversitesi'nden Stanford'a yapılan ilk ağ bağlantısı, 1972'de kırk düğüm mantığını benimseyerek daha fazla alanı birbirine bağlayacak şekilde büyümüştür. Kısa müddet sonra dünyanın bir çok çok daha fazla araştırma merkezi ve üniversite bu ilk ağa katılmış veya alternatif olarak kendi ağlarını oluşturmuştur (Ünver, 2023, 45). Bu durum, 1969'dan itibaren bilgisayarlardaki gelişimin ne ölçüde hızlı bir biçimde olduğunu göstermesi açısından son derece önemlidir.

Uluslararası alanda siber güvenlik denilince akla ilk gelen kavram olan internetin temeli yani interneti oluşturmuş olan "ARPA" adlı projede yer alan ağa zaman içerisindeki gelişmelere bağlı olarak yeni bilgisayarların dahil edilmesiyle birlikte ağ üzerinden yapılan iletişim ciddi oranda artış göstermiştir. Buna bağlı olarak birçok kullanıcı tarafından kullanılan ve yarar ağladığı düşünülen başta elektronik mesajlar ve dosya transferleri olmak üzere birçok yeni sistemler icat edilmiş ve kullanıcıların hizmetlerine sunulmuştur. Bunlardan sonra 1973'te farklı niteliklere sahip ağların kendi aralarında bilgi paylaşımını sağlayabilmeleri için ortak bir dil oluşturulmaya ve mevcut ağların birleştirilmesine çalışılmıştır. Bu amaç doğrultusunda geliştirilmiş olan "TCP/IP (Transmission Control Protocol/Internet Protocol)" üzerinde kayıtlı değişik özellikteki ağ protokollerinin ve bilgisayarların kendi aralarında verimli bir biçimde iletişim kurabilmelerine olanak sağlayan ortak bir yazılım dili olarak meydana getirilmiş ve kullanılmaya başlanmıştır (Altınbaşak & Karaca, 2009).

Siber güvenlik kavramı açısından 1983 yılı çok önemlidir. Zira 1983 yılında, ticari alanda internet üzerinden ilk e-posta servisi olan MCI postayı başlatma çabalarına öncülük etmiştir. Siber kelimesi il kez bu gelişmeler yaşanırken ortaya atılmıştır. Kelimeyi ilk kez William Gibson 1982'deki çalışmasında "sibernetik" ve "alan" ın bir karışımı olarak kullanmıştır. İki yıl sonra alanın devrim yaratan romanı Neuromancer'de bunu "Her ulusta milyarlarca meşru operatörün her gün tecrübe ettiği bir rızaya dayalı halüsinasyon... Düşünülemez karmaşıklık, Işık çizgileri, zihnin boşluğunda, veri kümelerinde ve takımyıldızlarında yer alan bir metafor" olarak bahsetmiştir (Ünver, 2023, 46). Böylece bu tarihten itibaren dünyada siber güvenlik kavramı bilinmeye ve ciddi anlamda kullanılmaya başlanmıştır.

Siber güvenliğin tarihsel gelişimi bağlamında 1980'lerin sonlarında, interneti yönetmenin araştırma topluluğunun işi olmadığı tespit edilmiştir. Ticari aktörler, interneti geliştirerek büyütmek için gerek duyulan ağ hizmetlerini sağlayabilmekte ve bu gelişimle eş anlı bir biçimde hevesli tüketiciler halini alabilmektedirler. Bu nedenle ABD Beyaz Saray Bilim ve Teknoloji Ofisi, çalışmalarını genişletmek ve ticarileştirmek için bir plan geliştirmiştir. Planlamacılar, 1990'ların sonlarına kadar ticari devir tesliminin son aşamalarının tamamlanmadığı on yıllık bir süreç öngörmüşlerdir.

Yukarıda yapılan açıklamalar bağlamında ABD Kongre Üyesi Gore, yüksek hızlı telekomünikasyonun hem ekonomik büyümenin hem de eğitim sistemimizin iyileştirilmesinin itici gücü olduğu fikrini savunuyordu. Bilim ve akademi alanındaki gelişmeleri iyileştirmenin ötesinde, bilgisayar iletişimlerinin daha geniş bir etkiye sahip olabileceğini kavrayan ilk seçilmiş yetkili oydu. Dünyada internet ile ilgili çalışmalar1973 yılında başlamış ve 1983'te en iyi seviyeye gelmiştir. Ancak bugünkü şekliyle internet, 1983 yılına kadar kullanıma sunulmadı. İnternet henüz kullanımının ilk aşamalarında iken, ABD Kongre Üyesi Al Gore, yüksek hızlı bilgi işlem ve iletişimin potansiyel faydalarının vizyonunu oluşturmaya yardımcı olarak entelektüel liderlik yapmıştır (Wiggins, 2010). Örneğin, doğal afetler ve diğer krizlere karşı devlet kurumlarının koordineli müdahalesi gibi alanlarda ileri teknolojilerin nasıl kullanılabileceğine dair oturumlar düzenlenmiştir. İnternet sistemlerindeki bu gelişme ve ilerlemeler bizi aşama aşama siber güvenlik konusuna doğru götürmektedir.

Önal'a göre DNS olarak adlandırılan sistemler, numaraların yerine akılda daha kolay kalıcı olabilen yapılar üzerinden oluşturulmaya başlanmıştır. 1980'lerin sonunda ise artık internet sisteminin ticari hedefler doğrultusunda kullanılması sürecine geçilmiş ve internet ticaret alanında çok yoğun bir biçimde kullanılmıştır. İnternetin ticaret dahil birçok alanda aktif bir biçimde kullanılmasının bir sonucu olarak dünyadaki ilk arama motoru olan Archie adı verilen sistem ortaya çıkmıştır. Önal'a göre bahsi geçen arama motorunun geliştirilmesi ve internette her alanda kullanılmaya başlanması, siber güvenlik alanında büyük problemlerin ortaya çıkmasına ve ilerleyen dönemlerde de önünün alınamaz bir duruma gelmesine sebep olmuştur. Zira internet kullanımının bu kadar geliştiği bir ortamda 1982 yılında ilk virüsler ortaya çıkmış ve 1988 yılında icat edilmiş olan *MORRİS* adındaki virüs, internet ağına bağlı cihazların çok büyük bir bölümüne zarar vermiştir. (Önal, 2021). Bunun üzerine günümüzde küresel güvenlik kavramının çok önemli bir kolu olan siber güvenlik kavramı meydana çıkmış bulunmaktadır.

Çeliktaş'a göre 1990'dan itibaren Bilgisayarlar ve internetteki gelişmelerin ciddi bir boyuta ulaşması ve dünya genelinde ciddi oranda gelişme göstermesinin bir sonucu olarak başta güvenlik

bilgileri olmak üzere çok sayıda veri siber uzaya aktarılmıştır. Bu da insanoğlunu bilgi ve teknolojiye bağımlı bir duruma getirmiştir. Önceleri büyük fayda sağlayacağı ve insan hayatını ciddi anlamda rahatlatabileceği düşünülen bu durum, zamanla kötü bir hal almıştır. Zira bilgisayara aktarılan bilgiler, kötü niyetli kişi ya da kişilerin ellerine geçmiş ve bu durum insanların ve devletlerin güvenliğini tehlikeye atmıştır (Çeliktaş, 2016, 5). Siber güvenlik, böylesine bir ortamda siber saldırılara ve güvenliği tehlikeye düşüren tehditlere açık hale gelmiş ve bu da geleneksel güvenlik sağlama anlayışından uzaklaşarak yeni sistemlerin bulunmasını zorunlu hale getirmiştir.

Siber güvenliğin gelişiminin bir diğer aşaması da 1991 yılıdır. 1991'i ön çıkaran ise dünyada önemli bir gelişme olan Körfez Krizi'nin yaşandığı bir yıl olmasıdır. Bu süreçte Körfez Savaşı'ndaki hava taarruz harekatının mimarı olarak görülen Amerikalı John A. Warden, bütün devletlerin ve stratejik yapıya sahip unsurların sistem yaklaşımıyla birlikte analiz edilmesi gerektiğini öne sürmüştür. Warden, bu ifadeden hareketle iç içe geçmiş olan toplamda beş adet halkanın varlığından söz etmiştir. Bu halkalar sırasıyla şunlardan oluşmaktadır: a) liderlik, b) önemli yapılar, c) alt yapı, d) nüfus, e) askeri kuvvetler. 1991'den itibaren bunlara ilave olarak internet ağı da son derece önemli bir duruma gelmeye başlamıştır. Zira siber ağ saldırılarının başlaması ve artması üzerine ülkelerin saldırı güçlerinin ve bahsi geçen beş halkanın yetersiz kalmasından dolayı teknolojik üstünlüğe dayalı savunma sistemleri elzem bir hal almıştır (Güneş, 2019). Bu da teknolojik üstünlüğü temel alan siber güvenlik sistemlerinin önemini bir kez daha ortaya çıkarmıştır.

1990 yılında, İsviçre'de bulunan "*Nükleer Araştırma Merkezi'nde* (CERN)" bir araştırmacı bilgileri, bir çok harfin belirsiz bir şekilde ilişkili olduğu bilgisayardaki belge ve dökümanlarla yeni bir ağ ara yüzü kurmuştur. Bu Hiper Metin Aktarım Protokolü (HTTP)'dür. *Tim Berners-Lee,* bilgisayara ilintili belgeleri (URL) oluşturmak için eşlik eden bir sistemle *World Wide Web'i* (www) icat etmiştir. Singer ve Friedman'ın ifadesine göre, Berners-Lee bunu akademik bir sempozyumda sunmaya çalıştığında, buluşu yeterince kıymetli görülmemiştir (Ünver, 2023, 52). Bunun yerine, bir koridorda üzerinde bir posteri tutmaya mahkûm edilmiştir.

Siber güvenlik bağlamında ilk web sitesi 1991'de yapılmıştır. Yılmaz'a göre bu tarihten itibaren "*World Wide Web*" olarak adlandırılan sistem, bilgi ve belgeler ile bilgisayar ağlarının "*hiper metinler*" ve dijital teknoloji yoluyla birbirilerine bağlanması şeklinde ifade edilmektedir. Ancak şunu unutmamak gerekir: Web ile internet birbirinin eş anlamlısı olarak kullanılamaz. Zira internet, bütün bilgilerin ve bilhassa da resmi kurum ve kuruluşlara ait bilgilerin açık erişime sunulduğu ağların birleşimi anlamına gelmektedir. Web ise ağ üzerinden bir tarayıcı vasıtasıyla bilgi akışını sağlayan internetin bir alt bileşenidir. Bu bağlamda elektronik postalar, sosyal medya platformları olan facebook, instagram vs. ile bloglar ve arama motorları internetin bir parçasıdır. Yani bunlar birer web değildir (Yılmaz, 2021). Web sayfalarının kullanımı arttıkça internete dayalı siber güvenlik açısından çok ciddi sorunlar oluşmuştur. Yani internetin kullanımı arttıkça ve web sayfaların sayısı arttıkça sanal anlamda ciddi bir güvenlik sorunu ortaya çıkmıştır. Bu da siber güvenliğin önemini arttırmıştır.

Siber güvenliğin tarihinde internetin ve web sistemlerin gelişimi kadar zararlı yazılımlar olan virüslerin ortaya çıkışı da son derece önemlidir. Dünyada bilinen ilk virüs Robert Tappan Morris tarafından eğlence amacıyla yazılmış olan "*MORRİS VİRÜSÜ*" dür. Türkçede "*MORİS SOLUCANI*" şeklinde tanımlanan ve adı geçen kişi tarafından bir hata neticesi ortaya çıkarılan bu zararlı yazılım programı, ortaya çıktığı ilk günden itibaren dünya genelinde internet ağına bağlı olan bilgisayarların yaklaşık olarak %10'una zarar vermiştir. Akabinde de 1996'da makro virüsler ortaya çıkmıştır (Acarer, 2020). Bu virüslerden hemen sonra sanal dünya üzerinden siber saldırılar gerçekleştirilmeye başlanmış ve bu da ciddi tehlikeler oluşturmuştur. Bu da siber güvenliği bir kez daha önemli bir konuma getirmiştir. Zira virüsler, bilgisayarlar ve bilgi ağları açısından ciddi bir tehlike ve tehdit oluşturmuştur.

2000'li yılların başında dünyada kredi kartı dolandırıcılığı ortaya çıkmış ve bu da ciddi güvenlik sorunu oluşturmuştur. Siber güvenlik, birçok alanda etkili olduğu gibi ekonomi sistemlerini de etkilemektedir. Siber güvenliğe ekonomi alanındaki sistemler açısından bakıldığında; bankacılık işlemleri, kredi kartları, yatırım fonları vb. çok sayıda işlemler internet üzerinden bankalar, kredi kartı hizmet sağlayıcıları ve fon yönetim şirketleri gibi finansal kuruluşları, kişilere ait başta kimlik bilgileri

ve ev adresleri olmak üzere çok sayıda bilgiyi bünyesinde barındırmaktadır. Bu durum da siber suçluların ilgisini ciddi oranda çekmektedir (Akçakanat vd., 2021). Bu nedenle 2000'li yıllardan bugüne kadar kredi kartı ve diğer alanlardaki sanal dolandırıcılıklar arttığı için bu da siber güvenlik alanında ciddi önlemlerin alınmasını zorunlu kılmıştır.

2000 yılında ortaya çıkan 'I LOVE YOU' virüsü ise küresel ölçekte iki gün gibi kısa bir süre içerisinde yaklaşık 50 milyon bilgisayara bulaşarak tarihin en hızlı yayılan zararlı yazılımlarından biri olmuştur. E-posta üzerinden çoğalan bu virüs, özellikle kamu kurumları ve büyük şirketlerde ciddi veri kayıplarına yol açmış; sosyal mühendisliğin siber saldırılardaki etkinliğini göstermesi bakımından literatürde önemli bir örnek haline gelmiştir (Reagan, 2001).

2007 yılında Estonya'ya karşı gerçekleştirilen geniş ölçekli DDoS saldırıları, modern anlamda devlet hedefli ilk büyük siber operasyonlardan biri olarak kabul edilmektedir. Bu saldırılar; bankacılık, devlet portalları, medya kuruluşları ve parlamentonun resmi sitelerini devre dışı bırakarak ülke yönetimini doğrudan etkileyen sonuçlar doğurmuştur. Estonya örneği, siber saldırıların ulusal egemenlik ve kritik altyapı açısından ne denli yıkıcı olabileceğini dünya gündemine taşımıştır (Ottis, 2008, 24).

Benzer şekilde 2008'de Gürcistan, Rusya ile yaşanan askeri gerilim sırasında eş zamanlı siber saldırılara maruz kalmıştır. Bu saldırılar fiziki çatışmayla eşgüdümlü yürütülmüş ve 'hibrit savaş' kavramının siber güvenlik literatüründe yer edinmesine sebebiyet vermiştir (Shakarian, 2011). Bu iki olay, devletlerin siber savunma stratejilerini yeniden şekillendirmelerine neden olmuş ve uluslararası güvenlik çalışmalarında siber alanın askeri boyutla bağlantısı açık biçimde ortaya çıkmıştır.

Siber savaş kavramını temelden değiştiren bir diğer önemli gelişme ise 2010 yılında keşfedilen Stuxnet saldırısıdır. ABD–İsrail ortak operasyonu olduğu değerlendirilen Stuxnet, İran'ın Natanz nükleer tesisindeki santrifüjleri hedef almış ve fiziksel tahribat yaratmıştır. Bu saldırı, tarihte ilk kez bir zararlı yazılımın fiziksel altyapıyı doğrudan sabote etmek için kullanılması nedeniyle literatürde 'dijital silahların miladı' olarak kabul edilmektedir (Zetter, 2014, 58). Stuxnet, devletlerin siber operasyon kapasitesine ilişkin stratejik düşünceyi kökten değiştirmiştir.

2000'li yıllarla birlikte sağlık, e-ticaret ve bankacılık sektörleri küresel çapta en sık hedef alınan alanlar haline gelmiştir. Örneğin 2015'te ABD'de Anthem sağlık şirketinin sistemlerine düzenlenen saldırı sonucunda yaklaşık 80 milyon vatandaşın kişisel verileri ele geçirilmiştir. Benzer şekilde 2014'te JPMorgan Chase saldırısı, finans sektörünün karşı karşıya olduğu riskleri küresel çapta görünür kılmıştır (Kshetri, 2016, 78). Bu olaylar, dijitalleşen sektörlerin devlet politikaları kadar özel sektör için de kritik güvenlik boyutları oluşturduğunu göstermiştir.

2000'li yılların ortalarından itibaren siber teknolojilerde gözlenen ivmeli ilerleme, özellikle bulut bilişim temelli uygulamaların kurumsal ve bireysel düzeyde yaygınlaşmasını sağlamıştır. Bu gelişme, veri ve bilgi bütünlüğünün korunmasına yönelik güvenlik protokollerinin güçlendirilmesini zorunlu kılmış; aynı zamanda artan tehdit vektörleri ve saldırı yüzeyleri karşısında bilişim sistemlerinin direnç kapasitesinin yükseltilmesine ilişkin kapsamlı iyileştirme süreçlerini tetiklemiştir. Veri güvenliğinden sistem sürekliliğinin sağlanmasına kadar geniş bir yelpazeyi kapsayan siber güvenlik, günümüzde hem kamu politikalarının hem de günlük yaşam pratiklerinin merkezinde konumlanan stratejik bir alan hâline gelmiştir. İnsan yaşamının dinamik ve sürekli değişen doğası ise risklerin minimize edilmesini sağlayacak etkin siber güvenlik mimarilerinin ve bilgi sistemlerinin tesis edilmesini zorunlu bir gereklilik olarak ortaya çıkarmaktadır (Kestane & Kurt, 2024). Bilhassa ağ, bulut ve siber güvenliğin çözümleri olarak bilinen Cisco, 2013 yılı başında 8,7 milyar cihazın internete bağlandığını belirtmiş ve bu sayının 2020'li yılların başında kırk milyara ulaştığı vurgulamıştır.

Kestane'ye göre son olarak günümüzde teknolojinin gelişmesi ile her geçen gün yeni tür zararlı yazılımlar ile karşılaşmak mümkün olmaktadır. Günümüzde sıklıkla karşımıza çıkabilecek zararlı yazılım türlerinin başlıcaları ise virüsler, solucanlar (worms), casus yazılımlar (spyware), reklam yazılımları (adware), Truva atları (Trojen horses), botnetler, korsan amaçlı kullanılan yazılımlar (rootkits), fidye yazılımları (ransomware) ve arka kapılardır. Bunlar beraberinde siber saldırıları etkin

duruma getirmektedir (Kestane, 2025). Bu saldırılara karşı günümüzde dünya genelinde ciddi bir mücadele verilmektedir. Zira siber saldırılara karşı ciddi bir biçimde siber güvenlik politikaları takip edilmezse bu durum dünyanın varlığı ve güvenliği açısından çok büyük bir tehlike oluşturacağı değerlendirilmektedir.

Türkiye'de Siber Güvenliğin Gelişim Süreci

Bıçakçı'ya göre Dünya genelinde olduğu gibi Türkiye'de güvenlik açısından ciddi bir sorun haline gelmeden önce, siber saldırılar daha çok hukuk alanında öne çıkan meseleler olarak bilinirdi. Ancak zamanla devletlerin silahlı kuvvetleri tarafından siber saldırıların hava, deniz ve kara kuvvetleri açısından ne gibi tehlikeler doğurmaya başladığının görülmesi üzerine bu konuya büyük bir önem verilmeye başlanmıştır. Zira artık geleneksel savaş anlayışından siber saldırı temelli savaşlara geçilmiştir. Bu saldırılar, dış alanda olduğu gibi iç alanda da olmaktaydı. Bu nedenle siber saldırılara karşı önlem alınması gerekmekteydi. Bu bağlamda Türkiye'de siber suçlar ilk olarak 16 Haziran 1991'da 3756 Sayılı Türk Ceza Kanunu'nda yapılan değişiklik sonucu yer almıştır. Burada dijital suçların neler olduğu sayılmış ve buna karşı cezai işlemlerin nelerden ibaret olduğu belirtilmiştir. (Bıçakçı vd., 2015, 4). Bu tarihten beri de Türkiye'de siber tehlikelere karşı hem iç hukuk sisteminde ciddi önlemler alınmaya başlanmış hem de uluslararası sözleşmeler yapılarak ciddi önlemler alınması yoluna gidilmiştir.

Yukarıda izah edilen durum 1997'de TÜBİTAK bünyesinde bazı çalışmaların yapılmasıyla olumlu yönde değişmeye başlamıştır. Bu bağlamda 1997'de "Bilişim Sistemleri Güvenliği Birimi" adı altında "TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE)" kurularak çalışmalarına başlamıştır. Daha sonra ise UEKAE, Bilişim Sistemleri Güvenliği Biriminden ayrılarak TÜBİTAK BİLGEM bünyesinde ayrı bir enstitü olarak çalışmalarını sürdürmüştür. Siber Güvenlik Enstitüsü adını alan bu yapı, Türkiye'de bilgi teknolojileri güvenliği ve siber güvenlik başta olmak üzere bu alanlara ilişkin birçok bilgi, belge, mevzuat ve doküman hazırlamıştır. Yani bu alanda ciddi çalışmalar yapmıştır (Fidancıoğlu, 2023: 5). Bu da bilhassa Türkiye'de siber tehditlere karşı siber güvenlik çalışmalarının ve politikalarının olumlu yönde gelişme gösterdiğini ortaya koyması bakımından önemlidir.

Türkiye'de 1997'den itibaren TÜBİTAK bünyesinde başlatılan ve 2000'li yıllarda arttırılan siber güvenlik politikaları, ülkenin güvenliği açısından son derece önemlidir. Zira Siber güvenlik, Türkiye'nin içinde bulunduğu durum açısından ulusal güvenliğin sağlanabilmesi için üzerinde durulması elzem olan hususlardan birisidir. Bilhassa 1990'lı yılların sonlarından itibaren Türkiye'ye ait şirketlerin ve bazı devlet kurumlarının siber casuslar tarafından tehdit edilmeleri, siber güvenlik alanında yatırım ve çalışmalar yapılmasını zorunlu kılmıştır (Yıldırım, 2024). Bu nedenle 2000'li yılların başından beri TÜBİTAK'ın öncülüğünde hem Emniyet Genel Müdürlüğü hem de Jandarma Genel Komutanlığı bünyesinde ciddi çalışmalar yapılmaktadır.

Siber güvenlik alanında 1998'de Türkiye'de son derece önemli bir adım atılmıştır. Bu yıl içerisinde kamu kuruluşlarındaki bilgisayar ağlarında ortaya çıkan sorunların çözülmesi, değerlendirilerek analiz edilmesi ve bu alanda ortaya çıkan ekonomik sorunların çözülmesi amacıyla iki adet kurul tesis edilmiştir. Bunlar: Başbakanlık Müsteşarlığına bağlı olan KamuNet Üst Kurulu ile Kamu-Net Teknik Kuruludur. Bu kurullar, ilk olarak 1998'de "Kamu Bilgisayar Ağları Konferansı" düzenlemiş ve burada siber güvenliğe ilişkin bir eylem planı önerisi yapılmıştır. Bu kurullar 2002 yılına kadar e- Türkiye konusunda çalışmalarını sürdürmüştür. (Çetinkaya, 2017). Kamu-Net Üst Kurulu ve Kamu-Net Teknik Kurulu'nun kuruluşunu önemli bir adım olarak değerlendirmek gerekir. Zira bu düzenleme daha sonraları siber güvenlik alanında yapılan çalışmalara öncü olmuştur.

Siber güvenlik alanında yapılan çalışmalar kapsamında 1999'da "Türkiye Ulusal Enformasyon Altyapısı Ana Planı" oluşturulmuştur. Türkiye Cumhuriyeti Ulaştırma Bakanlığının desteğiyle TÜBİTAK-BİLTEN tarafından gerçekleştirilen söz konusu planla ilgili çalışmalara 1998'de başlanmış ve 2000'de projenin yeniden güncellenmesine kadar devam edilmiştir. Burada bilhassa Kamu Bilişim Teknolojilerine ilişkin olarak altyapı oluşturulmaya çalışılarak bu hususta gerekli olan önlemler alınmaya çalışılmıştır. Daha sonraları ise TUENA (Türkiye Ulusal Enformasyon Altyapı Master Planı)

adlı proje kapsamında siber güvenliğe dair hususlarda belirlenen konu başlıklarında ulusal bir durum tespit çalışması yapılmış ve Türkiye'nin 2010 yılına kadar "*Ulusal Enformasyon Altyapısı*" konusunda yapması gerekenleri ortaya koyan bir "ana plan" oluşturulmuştur (Ünsal, 2002, 48).

2000'li yılların hemen başında Milli Savunma Bakanlığı tarafından "*Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun*" adlı bir yasal çalışma gerçekleştirilmiştir. Bu yasal çalışmayla bilgi teknolojileri alanında güvenliğin tam olarak sağlanabilmesi için Başbakanlığa bağlı olarak bir üst kurul ve kamu tüzel kişiliğine sahip "*Ulusal Bilgi Güvenliği Kurumu Başkanlığı*" tesis edilmesi planlanmıştır. Bunun için de gerekli olan alt yapıya ilişkin çalışmalar yapılmıştır. (Karasoy & Babaoğlu, 2021). Ancak ciddi çalışmalar yapılarak hazırlanan bu kanun yürürlüğe girememiştir.

Türkiye'de 1999-2000 yılları arasında siber güvenlik alanında önemli bir kanun hazırlanmıştır. Bu kanun, siber güvenlik açısından hayati önem taşımaktadır. Bilindiği üzere siber tehdit ve tehlikelerin artması üzerine devletler, siber istihbarat çalışmalarına ağırlık vermiş ve bu alana ciddi bütçeler ayırmak zorunda kalmıştır. Zira siber saldırılar sonucu ülkelerin e-devlet alt yapılarına ve internet sistemlerine zarar verilerek devletlerin varlığı açısından ciddi tehlikeler oluşturulmaktadır. Türkiye'de bu durumdan etkilenen ülkelerden birisidir. Bu nedenle Türkiye'de siber güvenliğe ilişkin ciddi plan ve çalışmalar yapılmakta ve saldırılara karşı gerekli önlemler alınmaya çalışılmaktadır. Bu anlamda yapılan ilk çalışma, 1971'de kurulan 2000'de geliştirilmiş olan "*Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun Tasarısı*"nın yürürlüğe konulmasıdır. (Kutlu vd., 2018). Adı geçen kanun, ülke genelinde e-devlet adı altında yapılan hizmetlerin güvenli bir biçimde yürütülebilmesi için ayrıntılı bir biçimde düzenlemeler öngörmüştür. Bu kanun, Türkiye'de e-devlet hizmetlerine ilişkin olarak ilk düzenlemeleri yapması ve buna ilişkin ilk strateji belgesi ve eylem planı hazırlamış olması bakımından son derece önemlidir.

Kurnaz ve Karatepe'ye göre 2012'de TÜBİTAK bünyesinde Bilişim Sistemleri Güvenliği Birimi kurulmuştur. Bu birim, siber güvenlik açısından son derece önemlidir. Çünkü bilgi teknolojilerinin, sağlamış olduğu hız ve kolaylığın dışında siber güvenlik açısından çok sayıda sakıncaları da bulunmaktadır. Bu durum, bilişim sistemlerinin ne kadar önemli olduğunu göstermektedir. Bugün Türkiye, geçmişe oranla çok daha fazla bir biçimde otomasyon sistemlerine bağlı bir ülke konumundadır. Bu nedenle de Türkiye'nin başta ulusal güvenlik olmak üzere birçok sistemi denetim altında tutması gerekir. Bilhassa bu sistemlerden birisi olan bilişim sistemleri, siber saldırılar açısından son derece hassas bir durumdadır. Bu nedenle siber tehdit ve tehlikelere karşı ülke genelinde önlemlerin alınması ve buna ilişkin çalışmaların yapılması son derece önemlidir (Kurnaz & Karatepe, 2019, 2). Bunun yapılmasında ve kötü süreçlere karşı önlem alınmasında Bilişim Sistemleri Güvenliği Birimi son derece önemli bir görev üstlenmektedir.

Ulusal bilimsel güvenlik ve siber güvenlik açısından 2001'de yapılan Sekizinci Beş Yıllık Kalkınma Planı (2001-2005) önemlidir. Bu plan çerçevesinde şunlar hedeflenmiştir: "a) Ulusal bilgi altyapısı geliştirilerek bilgiye erişim kolaylaştırılacaktır. b) İnternete erişim kapasitesi uluslararası gelişmelerin gerektirdiği düzeye yükseltilecek, elektronik ticareti geliştirmek ve bilgi güvenliğini sağlamak için uluslararası kural ve standartlar çerçevesinde hukuki ve kurumsal düzenlemeler yapılacaktır. c) Telekomünikasyon hizmet yeteneğinin küresel düzeyde geliştirilmesi amaçlanacaktır" (Sekizinci Beş Yıllık Kalkınma Planı (2001-2005), 2001:227). Görüldüğü üzere siber güvenlik açısından bahsi geçen kalkınma planında ciddi anlamda yapılması muhtemel gelişmeler bulunmaktadır. Bu plan, sonraki yıllarda Türkiye'nin güvenliği açısından olumlu adımların atılmasına ortam hazırlamıştır.

Türkiye'nin Sekizinci Beş Yıllık Kalkınma Planı içerisinde en önemli konuların başında güvenlik olgusunun geldiği görülmektedir. Güvenlik kavramının alt başlıkları ise Siber Güvenlik, Taşıma ve Ulaşım Güvenliği, İş Sağlığı ve Güvenliği, Genel Güvenlik, Afet Güvenliği şeklinde sıralanmakla birlikte metin incelendiğinde en çok vurgu yapılan hususun Siber Güvenlik olduğu dikkati çekmektedir (Biçkin, 2024, 34). Bu durum Türkiye Cumhuriyeti'nin kalkınma planlarında dahi siber güvenliğe ne derecede hassas yaklaştığının en büyük göstergesi olması bakımından önemlidir.

Siber güvenlik açısından 2002'de e-Türkiye Girişimi Eylem Planı: hazırlanmıştır. Bu bağlamda 19 Haziran 2002 tarihli e- Türkiye adını taşıyan Başbakanlık Genelgesinde şu ifade yer almaktadır: "*Ülkemizin en önemli milli hedeflerinden biri olan çağdaş uygarlık düzeyine ulaşmak için; rekabetçi, dinamik ve bilgiye dayalı ekonomiye sahip olunması ve bilgi toplumuna dönüşümün sağlanması gerekmektedir. Gerekli stratejilerin belirlenip, ulusal bilgi politikasının oluşturulması ve uygulanması amacıyla e-Türkiye'nin gerçekleştirilmesi hükümetimizin önemli öncelikleri arasında yer almaktadır*" (Naralan, 2010). Bu genelgeyle Türkiye'nin e-Türkiye sistemine geçişle birlikte ulusal güvenliğin sağlanması için ne derecede güçlü planlar yapıldığını göstermektedir.

Aydın'a göre e-Avrupa+ kriterlerine uyum amacıyla, 2001-2002 döneminde TÜBİTAK ile birlikte Devlet Planlama Teşkilatı'nın öncülüğünde yapılan iki çalışma, siber güvenlik açısından bir dönüm noktası olmuştur. Bunlar sırasıyla e-Türkiye ve e- Dönüşüm Türkiye adlı iki farklı projedir. Bahsi geçen iki proje, Türkiye'de kamu kesiminde bilişim teknolojilerine ilişkin olarak açık bir strateji belirleyerek somut hedefler ortaya koyarak devlet kurumları arasında koordinasyonu sağlamada ilk olmaları açısından önem taşımaktadırlar (Aydın, 2005). e-Dönüşüm Türkiye Projesinin çalışmaları, 2003 yılından itibaren Devlet Planlama Teşkilatı Bilgi Toplama Dairesi tarafından yürütülmektedir. Bunların, Türkiye'de siber güvenliğin temin edilmesi bağlamında çok önemli adımlar olduğunun kabul edilmesi gerekir.

2003'ten itibaren Türkiye'de ülke genelinde internet kullanımın giderek artması, birtakım önlemlerin alınmasını zorunlu kılmıştır. Bunlardan birisi, "*2003-2004 Kısa Dönem Eylem Planı (KDEP)*" dır. Bu eylem planında siber güvenliğe yönelik daha önceleri yapılan düzenlemelerden farklı birtakım hedefler ortaya konulmuştur. Bu hedeflerden birisi olan "*Teknik Altyapı ve Bilgi Güvenliği*" içerisinde yer alan ve güvenliği sağlamayı amaçlayan "*TUBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEAKE)*" görev almaktadır. (Karasoy & Babaoğlu, 2021). Açıklanan bu plandan sonra yapılan incelemelerde bu alanda ilerlemelerin sağlandığı ve bunun da internet güvenliği açısından olumlu neticeler doğurduğu anlaşılmaktadır.

Türkiye'de 2005'te siber güvenlik alanında yapılan çalışmalar bağlamında kamu kuruluşlarında bilgi sistemlerinde güvenliği sağlamak amacıyla "*TÜBİTAK BİLGEM Ağ Güvenliği*" adlı yapı kurulmuştur. TÜBİTAK BİLGEM Ağ Güvenliği, devletin kritik birimlerinde görev yapanlara ve üniversitelerin bilgi işlem daire başkanlıklarında görev alan kişilere birtakım eğitimler verilmiştir. Aynı şekilde bahsi geçen yapının altında kurulan "*Siber Güvenlik Enstitüsü*" de "*akıllı sistemler*" e karşı korumasız hale düşen başta su, haberleşme ve enerji tesisleri olmak üzere devletin kritik kurum ve kuruluşlarının altyapılarının korunması için birtakım güvenlik testleri yapmıştır (Çakır &Taşer, 2023). Bu şekilde 2000'lerin başında başlayan siber güvenlik alanındaki çalışmalar aralıksız olarak devam ettirilmiştir.

2007 yılında çıkarılan 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkındaki Kanun siber güvenliğin sağlanması alanında atılan önemli bir adımdır. Kılınç'a göre bu kanunun temel amacı, internete bağlanma için yer ve erişim imkanı sağlama, kullanıcıların bir bütün olarak sorumluluklarını belirleme ve servis sağlayıcı şirketlerle kurulan koordinasyonla birlikte internet üzerinden işlenen suçlara müdahalenin yolunu ve yöntemini belirlemektir. Bu kanunun yürürlüğe girmesiyle birlikte Türkiye'de "*internet içerik politikası*" tek bir hukuk metni altında toplanmış ve dahi aile ve çocukların da korunması sağlanmıştır (Kılınç, 2016). Bir diğer ifade ile açıklamak gerekirse bu kanunla vatandaşlar, çocuklar ve gençler internetin zararlı içerik ve programlarına karşı güvence altına alınmıştır.

2008 yılına gelindiğinde ise "*Elektronik Haberleşme Kanunu*" çıkarılarak siber güvenliğin tesisi için yeni bir adım daha atılmıştır. Her ne kadar bu kanun, haberleşme hizmetleri ismiyle belirlemiş olduğu alanlarda yapılacak çalışmalar bağlamında bazı kişilerin özel olarak vazifelendirilmesine ilişkin olmak üzere idari işlemlerinin yapılması ve kamu sektöründeki hizmetlerinin yapılma şekilleri açısından incelenmesinde planlanmış olan sistem tamamıyla yeni olmasa da en azından, yerleşmiş olan idare hukukuna ilişkin bazı kavramların yeniden ele alınmasına öncülük etmesi bakımından son derece önemlidir. Bu bağlamda "*5809*" Sayılı Kanun ile düzenlenmiş yetkilendirilme türleri arasında yer alan

"*bildirim*" ve "kullanım hakkı verilmesinin" idari işlemler açısından bilinen bazı teknik boyutları dikkate alınmayacak olunursa idarenin tek yanlı olarak adlandırılabilecek bazı işlemleriyle yapılabileceğinden şüphe olmayan yetkilendirme işleminin, kamu sektöründe yer alan hizmetlerin özel sektördeki kişilere yaptırılması yöntemleri içerisindeki yerinin belirlenmesi sorunu karşısında, devlet - kamu hizmeti ilişkisinin gözden geçirilmesi zorunlu hâle gelmektedir (Öztürk, 2009).

Siber güvenlik çalışmaları kapsamında Türkiye'de 2020 yılına kadar 2008,2011 ve 2013 yıllarında olma üzere üç kez siber güvenlik tatbikatı yapılmıştır. 2020 yılında ise geniş kapsamlı bir siber güvenlik tatbikatı gerçekleştirilerek tatbikat sayısı dörde yükseltirmiştir. TÜBİTAK ve BTK'nın öncülüğünde gerçekleştirilen bu tatbikatlardan 2011'deki ulusal tatbikatta 41 adet kamu ve özel kurumun desteğiyle 200 kişi görev almıştır. Görevlendirilen 200 kişi arasında bilişim teknoloji uzmanları dışında eğitim, sağlık, finans, savunma ve hukuk alanında uzman kişiler de yer almıştır. 2013'teki tatbikat daha kapsamlı olmuş ve burada 20 kurum gözlemci olmak üzere toplamda 61 kamu ve özel kurum paydaş olarak yer almıştır. (Bıçakçı vd., 2015: 35). Siber güvenlik alanında yapılan bu tatbikatlar, Türkiye'nin siber saldırılara karşı hazırlıklı olduğunu göstermesi bakımından önemlidir. Zira bu tatbikatlarda siber ortamda ülke güvenliğine karşı olabilecek tehditler karşısında neler yapılabileceğine dair planlamalar yapılmıştır.

2009'da yapılan çalışmalar kapsamında "*Milli Güvenlik Siyaset Belgesi*" nde siber güvenliğe bilhassa vurgu yapılmıştır. "*Milli Güvenlik Siyaset Belgesi*" nde siber güvenliğin ülkenin güvenliği açısından ne kadar önemli olduğu ve buna yönelik çalışmaların artırılması gerektiği hususunun altı çizilmiştir. Yıldırım'a göre Türkiye'de belirli dönemlerde ulusal siber güvenlik stratejileri bağlamında hazırlanan belgelerde, hızla gelişen teknolojiye uyum sağlamak amacıyla yeni planlar oluşturulmakta ve hedefler belirlenmektedir. Bu nedenle siber savunmaya yönelik bütçe planlaması ve yatırımlar yapılmaktadır. Bu bağlamda Türkiye, siber güvenliği sağlamak için diğer kurum ve kuruluşlar ile multi-disipliner bir bakış açısı ile çalışan ve gelişim gayreti gösteren bir ülke konumundadır (Yıldırım, 2024). Zaten 2009 tarihli Milli Güvenlik Siyaset Belgesi'nin hazırlanması da buna işaret etmektedir.

2010–2012 döneminde Türkiye'de siber güvenlik alanında kayda değer kurumsal ve stratejik gelişmeler yaşandığı görülmektedir. Bu kapsamda, 27 Ekim 2010 tarihli Millî Güvenlik Kurulu toplantısında siber tehditler değerlendirilmiş ve bu alanın Millî Güvenlik Siyaset Belgesi'nde yer alması kararlaştırılmıştır. Ardından, TÜBİTAK ile Bilgi Teknolojileri ve İletişim Kurumu'nun iş birliğiyle 25–28 Ocak 2011 tarihlerinde I. Ulusal Siber Güvenlik Tatbikatı gerçekleştirilmiştir. Tatbikat sonrasında yayımlanan raporda, Türkiye'nin siber saldırılara karşı önemli ölçüde kırılgan olduğu; kamu kurum ve kuruluşlarının ise gerekli koruyucu ve önleyici tedbirleri yeterince uygulamadığı tespit edilmiştir.

Konu bu şekilde hassasiyetle ele alınırken Redhack isimli bir hacker grubu e-devlet üzerinden hizmet sağlayan pek çok devlet kurumuna siber saldırı düzenlemiş ve Türkiye'nin e-devlet sistem güvenliğini ciddi anlamda tehlikeye düşürmüştür. 2015 yılında bir bankaya yönelik gerçekleştirilen saldırıda milyonlarca kişinin kart verilerinin çalınması kamuoyunda geniş yankı uyandırmıştır. Benzer şekilde 2016'da birçok kamu kurumunun web sitesinin eş zamanlı DDoS saldırılarıyla devre dışı bırakılması, Türkiye'nin kritik altyapı güvenliğine ilişkin hassasiyetleri artırmıştır (Yıldırım, 2024). Benzer tehlikelere karşı önlem almak amacıyla 20 Ekim 2012 tarihinde Bakanlar Kurulu tarafından alınan karar neticesinde "*Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Yönetmelik*" yürürlüğe girmiştir. Bu çerçevede söz konusu Bakanlar Kurulu Kararı ve "*Elektronik Haberleşme Kanunu*" ile siber güvenliğe ilişkin strateji belgelerinin hazırlanması ve eylem planlarının oluşturulması için Ulaştırma, Denizcilik ve Haberleşme Bakanlığı yetkilendirilmiştir (Kutlu vd., 2018).

2013 yılı itibarıyla Türkiye'de siber alanda ulusal strateji belgelerinin hazırlanmasında Ulaştırma, Denizcilik ve Haberleşme Bakanlığı dışında yetkili olan bir diğer kurumda "*Ulusal Siber Olaylara Müdahale Merkezi*" dir. 2013/4890 sayılı Bakanlar Kurulu Kararı ile "*2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı*" kapsamında, ülke genelinde siber güvenlik açısından tehlike oluşturan durumlara karşı ne gibi önlemler alınabileceği ve buna ilişkin ne gibi düzenlemelerin yapılabileceğine

dair çalışmaların yapılması ve ilgili kurum ve kuruluşlarla paylaşılmasını sağlamak amacıyla TÜBİTAK bünyesinde teşkil edilen "*Ulusal Siber Olaylara Müdahale Merkezi (USOM, TR-CERT)*" siber güvenliği tehlikeye düşürebilecek tehditlere karşı önlemler almak için çalışmalar yapmaktadır. (Gündoğdu, 2023). Bu gelişmeler, 2010'dan itibaren Türkiye'de siber güvenlik alanında ne derece hızlı adımların atıldığı ve buna ilişkin kanunların nasıl hızlı çıkarıldığını açıkça ortaya koymuş, ulusal siber güvenlik stratejilerinin güçlendirilmesine doğrudan etki etmiş ve USOM'un operasyonel kapasitesinin artırılmasına zemin hazırlamıştır.

Darıcılı'ya göre 2013'te USOM'un kuruluşuna ek olarak Türk Silahlı Kuvvetleri 'de siber güvenlik alanında birtakım adımlar atmıştır. Bu bağlamda 2013 yılında alay seviyesinde bir yapılanma ile Siber Savunma Komutanlığı'nın kuruluşu ilan edilmiştir. Bu birimin görevleri, Türk Silahlı Kuvvetleri'nin kullandığı siber ortamda bulunan tüm sistemlerin siber savunmasını sağlamak, siber olaylara 7/24 esasına göre müdahale etmek, ulusal ve NATO bağlantılı uluslararası tatbikatlara iştirak etmek, ordu çapında bilinçlendirme ve eğitim faaliyetleri yürütmek, silahlı kuvvetler tarafından kullanılan ağlarda düzenli olarak siber güvenlik denetlemeleri ve testleri yapmak şeklinde belirlenmiştir (Darıcılı, 2019).

Siber güvenlik alanında Türk Silah Kuvvetlerinde olduğu gibi Emniyet Genel Müdürlüğü bünyesinde de ciddi adımlar atılmıştır. Yine 2013 yılında Emniyet Genel Müdürlüğü bünyesinde Siber Suçlarla Mücadele Daire Başkanlığı kurulmuştur. Bu süreç incelendiğinde, emniyet teşkilatının yapılanmasının geleneksel, yukarıdan aşağıya işleyen hiyerarşik, otoriter ve merkeziyetçi bir örgüt kültürüne sahip olduğu; ilişkiler sisteminin ise büyük ölçüde yazılı kurallara dayalı biçimde şekillendiği görülmektedir. Bununla birlikte teşkilatın, toplumsal ve sosyal dönüşümler sonucu ortaya çıkan yeni ihtiyaçlara uyum sağlamak amacıyla kurumsal yapısında değişikliklere gittiği ve böylelikle farklı işlevleri yerine getirmek üzere yeni birimler oluşturma kapasitesine sahip olduğu kabul edilmektedir (Taşçı & Can, 2015: 238). Bu da silahlı kuvvetlerde olduğu gibi emniyet teşkilatının da suç ve suçlularla mücadelede teknolojik gelişmeleri takip ettiğini ve bu yönde adımlar attığını ortaya çıkarmaktadır.

Siber güvenlik alanında Emniyet Genel Müdürlüğü'nde olduğu gibi Jandarma Genel Komutanlığında da Siber Suçlarla Mücadele Daire Başkanlığı kurulmuştur. Günümüzde her iki kolluk biriminde de siber soruşturma kapasitesinin geliştirilmesi amacıyla ihtiyaç duyulan personel alımları hızlandırılmış ve siber suçlarla daha etkin mücadeleye yönelik planlamalar yapılmaktadır. Bu bağlamda, Jandarma Genel Komutanlığı bünyesinde Ar-Ge laboratuvarlarının kurulması ve proje teşvik mekanizmalarının geliştirilmesiyle; kamu, özel sektör ve üniversitelerde görev yapan bilişim uzmanlarının süreçlere katılımını engelleyen kurumsal yetersizliklerin giderilmesi hedeflenmektedir (Çakır &Taşer, 2023).

Türkiye'de kritik altyapı güvenliğine yönelik kurumsal çerçeve, 2014 yılında AFAD tarafından yayımlanan Kritik Altyapıların Korunması Yol Haritası Belgesi ile şekillendirilmiştir. Bu belgede, 2014–2023 dönemi için AFAD'ın siber güvenlik alanındaki hedefleri tanımlanmış; kavramın kuramsal temeli oluşturulmuş ve kritik altyapılar sektörel olarak sınıflandırılmıştır. Belge öncesinde kritik altyapılar çoğunlukla siber güvenlik ekseninde değerlendirilmektedir. Oysa kritik altyapılar, zarar görmeleri hâlinde can, mal ve itibar kaybına yol açabilen, ülkenin fiziki ve fiziki olmayan tüm temel unsurlarını ifade etmektedir. Bu kapsamda Türkiye'de kritik altyapılar enerji, ulaştırma, sağlık, iletişim, tarım ve gıda, su yönetimi ve barajlar, kültür ve turizm, bankacılık ve finans, kritik kamu hizmetleri ile kritik üretim/ticari tesisler olmak üzere on ana sektörde tanımlanmış; çalışmalar sonucunda enerji (doğalgaz, elektrik, katı yakıtlar) ve ulaştırma (deniz, kara, demir ve hava yolu) alanlarında alt kırılımlar da belirlenmiştir (Tanrıverdi vd., 2023). Ülke güvenliği açısından hem siber güvenlik politikalarına hem de bahsi geçen yerlerin korunmasına son derece önem verilmektedir.

Siber güvenlik kapsamında 2016'da 6698 Sayılı Kişisel Verilerin Korunması Kanunu yürürlüğe girmiştir. Siber güvenliğin bu kadar önemli olduğu dönemde söz konusu kanunun çıkarılması bir zorunluluk halini almıştır. Bilir'e göre kişisel verilerin korunması hakkı, Avrupa Birliği'nde geliştirilen normatif çerçeve içinde kurumsallaşmış olmakla birlikte, teknolojik dönüşümün hızlanmasıyla Türkiye'de de hukuki tartışmaların odağına yerleşmiştir. Bu hak, ilk aşamada Anayasa'da temel bir güvence olarak

tanımlanmış, daha sonra ise özel bir Kanun aracılığıyla normatif ve kurumsal boyutlarıyla sistematik şekilde düzenlenmiştir. Anılan Kanun, kişisel veri koruma rejiminin uygulanmasını gözetmek, yaptırımları yürütmek ve düzenleyici-denetleyici işlevi yerine getirmek üzere bağımsız bir idari otorite olarak Kişisel Verileri Koruma Kurumu'nun ihdas edilmesini de sağlamıştır (Bilir, 2023). İfade edildiği üzere herkesin kişisel bilgilerinin ve verilerinin korunması gerekmektedir ve bu kanun da bunu güvence altına almaktadır.

2017 yılında ilgili kamu kurumları, özel sektör ve akademisyenlerin katılımlarıyla ortaya çıkan ve Savunma Sanayii Başkanlığı tarafından desteklenen bir proje olan Türkiye Siber Güvenlik Kümelenmesi projesi bulunmaktadır. Bu projeyle yerli ve milli siber güvenlik ürün ve hizmetleri geliştiren firmaların üye olduğu iş birliği ve eşgüdümlü çalışma ortamı yaratılması amaçlanmaktadır. Bunun yanı sıra, kamuda siber güvenlik farkındalığını artırmak, ileri teknolojiye dayalı bir sistem yaratmak amacıyla kurulmuş olan Uluslararası Siber Güvenlik Federasyonu da siber güvenlik alanında faaliyet göstermektedir.

Siber güvenlik bağlamında Türkiye'de Cumhurbaşkanlığı Sistemine geçilmesiyle birlikte 2018'de Dijital Dönüşüm Ofisi kurulmuştur. Dijital Dönüşüm Koordinasyon Dairesi Başkanlığının bağlıları arasında Dijital Teknolojiler, Tedarik ve Kaynak Yönetimi Dairesi Başkanlığı, Dijital Uzmanlık, İzleme ve Değerlendirme Dairesi Başkanlığı, Siber Güvenlik Dairesi Başkanlığı, Büyük Veri ve Yapay Zekâ Uygulamaları Dairesi Başkanlığı, Uluslararası İlişkiler Dairesi Başkanlığı, Bilgi Teknolojileri Dairesi Başkanlığı, Yönetim Hizmetleri Dairesi Başkanlığı, Hukuk Müşavirliği" şeklinde hizmet birimleri bulunmaktadır. 2018'de kurulan bu ofisin, dijital kamu yönetiminin geliştirilmesine öncülük etmesi planlanmıştır (Boy Çaykara, 2024: 105). Söz konusu ofisin bileşenleriyle birlikte ciddi çalışmaları bulunmaktadır.

Ağdeniz'e göre siber güvenlik alanında 2019 yılında yayımlanan Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi, ulusal düzeyde bilgi güvenliği standartlarının güçlendirilmesine yönelik önemli bir düzenlemedir. Genelgenin temel amacı; bilgi güvenliği risklerinin azaltılması veya ortadan kaldırılması, ayrıca gizliliği, bütünlüğü ya da erişilebilirliği ihlal edildiğinde millî güvenliği tehdit edebilecek ya da kamu düzeninde aksamalara yol açabilecek kritik bilgi ve verilerin korunmasına yönelik asgari güvenlik tedbirlerinin belirlenmesidir. Bu kapsamda genelge, söz konusu tedbirlerin uygulanmasına ilişkin faaliyetlerin çerçevesini de kurumsal düzeyde tanımlamaktadır (Ağdeniz, 2021). Günümüzde siber saldırılardan dolayı bilgileri korumak ve saklamak son derece zor olduğundan bu kanunun söz konusu sorunu çözmede yardımcı olduğu düşünülebilir.

Yukarıda belirli bir kronolojiye bağlı kalınarak sıralandığı üzere Türkiye'de siber güvenlik alanında önemli adımlar atılmaktadır. Bunlardan birisi de 2020'de İstanbul'da ilk Siber Güvenlik Lisesinin açılmasıdır. Bu bağlamda İstanbul Milli Eğitim Müdürlüğü tarafından siber güvenliği temel alarak müfredatı oluşturulan liseden siber güvenlik alanında duyarlı gençlerin yetiştirilmesi amaçlanmıştır. Hemen akabinde ise siber güvenlik üzerine faaliyet göstermesi amacıyla Teknopark İstanbul Mesleki ve Teknik Anadolu Lisesi kurulmuştur (Uluç & Eyüpoğlu, 2024).

Tartışma

Bu çalışma, alan yazında uluslararası güvenliğin sağlanması hususunda sık sık dile getirilen bir konuyu tasdik etmek amacını gütmektedir: siber güvenlik, sadece teknik bir konu değil, aynı zamanda ulusal güvenliğin tesisinde göz ardı edilemeyecek derecede önemli bir politika ürünüdür. Nitekim global dünya ölçeğinde yaşanan gelişmelerle eş güdümlü şekilde Türkiye'de de 90'lı yılların başından itibaren yükselişe geçen farkındalık, kanuni çerçevenin genişletilmesi ve kurumsal yapının teknolojik gelişmelere bağlı olarak yapılandırılması ile beslenmiştir. Bu durum, siber güvenliğin teknoloji tarihinde meydana gelen gelişmelerle birlikte hem ulusal hem de küresel seviyede benzer saiklerle şekil aldığını göstermektedir.

Bu bulgular, çalışmanın kuramsal çerçevesiyle birlikte değerlendirildiğinde Türkiye'nin siber güvenlik politikalarının özellikle Realist ve Güvenlikleştirme yaklaşımlarıyla uyumlu olduğu görülmektedir. Buna karşın Eleştirel Güvenlik yaklaşımının vurguladığı 'birey ve toplum merkezli siber güvenlik kültürü', Türkiye'de henüz kurumsal düzeyde gelişim aşamasındadır.

Çalışma içeriğinde kronolojik bir biçimde işlenen gelişmeler, siber güvenliğin sadece ulusların güvenliğini sağlamak için değil, aynı zamanda vatandaşların mahrem hayatının koruma altına alınması ve ekonomik hayatın güvenli şekilde devamlılığının sağlanması bakımından da kritik önemi haiz olduğunu vurgulamaktadır. Alan yazında da altı çizildiği üzere, özellikle milenyum olarak adlandırılan 2000 yılı ve sonrasında finans ve bilhassa bankacılık sektörüne kast eden siber saldırılar, ulusların beraberinde özel şirketlerinde aktif politikalar üretmesini elzem hale getirmiştir.

Bir örnek olarak Türkiye ele alındığında, kısa-orta-uzun vadeli kalkınma planları ve ulusal strateji belgelerinin güvenlik unsurları içerisinde siber güvenliği merkeze aldığı gözlemlenmektedir. Lakin birtakım araştırmalar, Türkiye'de siber güvenliğe dair düzenlemelerin genellikle reaktif politikalar olduğunu, siber alanda belirli vukuatlar ya da tehditlerden sonra olayı çözmek için devreye alındığının altını çizmektedir. Bu durum, siber güvenliğin etkili bir şekilde sağlanabilmesi için uzun vadeli stratejilerin ve proaktif yaklaşımların hayata geçirilmesinin önemini ortaya koymaktadır.

Tartışmaya açık bir diğer nokta ise siber güvenliği sağlamakla görevlendirilecek elemanların eğitim boyutudur. Bulgular, 2020'de takdir edilecek bir girişimle kurulan siber güvenlik liselerinin gençlerin bilinçlendirilmesi ve siber uzay çağına yetiştirilmesi açısından önemli olduğunu göz önüne çıkarmaktadır. Ancak alan yazında, eğitim sürecinin daha da genç yaşlardan itibaren devreye alınması gerektiği şeklinde görüşler yer almaktadır. Bu da siber güvenliğe dair durumsal farkındalığın kurumsal seviyede olduğu kadar vatandaş nezdinde de yaygınlaşması ve olabildiğince tabana yayılması gerektiğine işaret etmektedir.

Netice olarak, uluslararası gelişmeler ve alan yazın ile Türkiye nezdinde elde edilen bulgular karşılaştırıldığında, dünyanın gelişmiş ülkeleri ile Türkiye'nin benzer nitelikte stratejiler oluşturduğu, lakin teknolojik altyapı geliştirme ve kaynak kullanımı bakımından bazı farklılıkların bulunduğu gözlemlenmektedir. Özellikle yerli ve milli teknolojik ürünlerin geliştirilerek siber güvenlik alanına entegre edilmesine yönelik gayelerin stratejik önemi her geçen gün artmaktadır. Dolayısıyla Türkiye'nin, global dünyada siber güvenlik ekosistemine dahil olurken yerli ve milli teknolojik kapasitesini güçlendirerek artırması gerektiği hususu elzem bir konudur. Hal böyleyken TÜBİTAK bünyesinde kurulan birimler, USOM ve TR-CERT gibi kurum ve kuruluşlar ulusal siber güvenlik ağının geliştirilmesi ve genişletilmesi hususunda son derece önemli rol üstlenmişlerdir. Siber Güvenlik konusunun Milli Güvenlik Siyaset Belgesi'ne eklenmesi, zaman zaman kasti ihlaller yapılarak siber güvenlik tatbikatları icra edilmesi konunun stratejik düzeyde ne denli kararlılıkla ele alındığının göstergesidir. Türkiye'nin siber güvenlik alanında gerek NATO gerekse AB gibi uluslararası oluşumlarla paylaşımda bulunması ciddi avantajlar sağlamaktadır. Türkiye'nin bu girişimleri, siber güvenliği sağlama konusunda gösterdiği refleksin göstergesi ve bu alanda üstün görülen bir husus olarak karşımıza çıkmaktadır.

Ezcümle, Türkiye'nin siber güvenliğini koruma altına alması yönündeki çabalarına bakıldığında; gerekli hukuki düzenlemelerin yapıldığı ve yapılmaya devam ettiği, eğitim konusunu hassasiyetle ele aldığı ve uluslararası örgütlerle iş birliği içerisinde olması açısından güçlü bir profil sergilediği müşahede edilmektedir. Teknolojik cihaz ve yazılımları yerlileştirme, proaktif yaklaşımlarla yeni stratejiler geliştirme, eğitimi tabana yayma ve yaygınlaştırma konularında ise birtakım zayıflıklar barındırdığı görülmektedir. İrdelenen tüm bu hususlar Türkiye'nin global dünya siber güvenlik ekosisteminde etkili bir oyuncu olabilmesi için; yazılım ve teknolojik cihazlar dahil olmak üzere bütüncül, proaktif stratejilere dayalı uzun vadeli ve siber güvenlik alanını tümüyle benimseyen politikalara ihtiyaç duyduğunu göstermektedir.

Sonuç

Bilimsel teknolojinin büyük bir gelişme gösterdiği çağımızda insanoğlunun hayatında çok büyük gelişmeler olmaktadır. Ancak bu gelişmelerin birçok olumlu yönleri olduğu gibi dünyayı olumsuz etkileyen tarafları da bulunmaktadır. Bilhassa teknolojinin çok büyük gelişme kaydetmesi, başta her türlü verilerin bilgisayar ortamına aktarıldığı güvenliğe ilişkin bilgiler olmak üzere birçok alandaki bilgilerin korunması ve muhafaza edilmesi, son derece büyük önem arz etmektedir. Zira bunların korunmaması, sadece bölgeleri değil; aynı zamanda dünyanın güvenliğini tehlikeye düşürmektedir. Bu nedenle bunların korunması için bazı önlemler alınmıştır. Bu önlemlerin başında ise siber güvenlik kavramı gelmektedir. Zira Siber güvenlik sayesinde bölgesel veya küresel çaplı siber saldırılar önlenebilmekte ve kısmen de olsa dünyanın güvenliği sağlanabilmektedir.

Bilindiği üzere günümüzde her bilgiye kolay bir biçimde dijital ortamda ulaşılabilmektedir. Bu da devletlerin güvenliğini oluşturan çok önemli olan ve hassas nitelik taşıyan bazı bilgi ve belgelerin korunmasını zorlaştırmaktadır. Zira bilgi ve teknolojik gelişmeler sayesinde iyi niyetli olmayan kişi ve kişilerce başta casus yazılımlar olmak üzere birçok yoldan bilgiler ele geçirilmekte ve bu da kurumların, kuruluşların, bölgelerin, ülkelerin vs. güvenlikleri için ciddi büyük tehlikeler oluşturmaktadır. Bu da söz konusu siber saldırılara karşı sadece bireysel değil topyekûn mücadeleyi zorunlu kılmaktadır.

Yukarıda verilen bilgiler bağlamında 2. Dünya Savaşı'ndan sonra başta Avrupa ülkeleri ve ABD olmak üzere gelişmiş ve gelişmekte olan ülkelerde dijital güvenliği sağlamak amacıyla önlemler alınmakta ve saldırılara karşı yeni yöntemler geliştirilmektedir. Bu bağlamda siber güvenliğin tarihsel gelişimi 2. Dünya Savaşı sonrasında artış göstermeye başlamış ve 1970'li yıllarda büyük bir gelişme göstermiştir. Sonrasında 1980'li yıllardan 2000'li yılların başına kadar devam eden gelişmeler, bugün de hız kesmeden devam etmektedir. Esasında siber güvenliğin bu denli tarihsel gelişimi, biraz da zorunluluktan kaynaklanmaktadır. Siber saldırılara kaşı gerekli siber güvenlik anlamında önlemler alınmazsa dünyanın ciddi tehlikelere karşı savunmasız kalacağı aşikârdır.

Siber güvenliğin tarihsel sürecinde bilgisayarların ve internetin yaygınlaşması, beraberinde birçok sorunu doğurmuştur. Zira söz konusu iki alanda büyük gelişmelerin olması sonucu yeni tür zararlı yazılımlar geliştirilmiştir. Bunlar arasında virüsler, solucanlar (worms), casus yazılımlar (spyware), reklam yazılımları (adware), Truva atları (Trojen horses), botnetler, korsan amaçlı kullanılan yazılımlar (rootkits), fidye yazılımları (ransomware) ve arka kapılar yer almaktadır. Bunların her biri, dijital verilerin güvenliğini tehlikeye atmaktadır. Bu nedenle 1980'li yıların başından beri siber güvenlik açısından bunlara karşı önlemler alınmakta ve bunları yok etmek için farklı metotlar araştırılmaktadır. Dolaysıyla da bu süreç, siber güvenlik tarihinin önemli bir bölümünü oluşturmaktadır.

Siber saldırıların büyük oranda arttığı günümüzde diğer devletler gibi Türkiye de bu durumdan son derece olumsuz yönde etkilenmektedir. Zira bulunduğu alanda hassas bir konumda olan ve güçlü bir orduya sahip olan Türkiye'nin kara, deniz ve hava sahasını siber saldırılara karşı koruması gerekmektedir. Bu nedenle Türkiye'de 1970'ten itibaren siber güvenliği sağlamak amacıyla önlemler alınmakta, kanun maddeleri çıkarılmakta, bilim ve teknoloji alanında yatırımlar yapılmakta ve dünyada siber saldırılara karşı alınan önlemler yakından takip edilmektedir. Ancak tarihsel açıdan Türkiye'de siber güvenlik alanında çalışmalar, esas olarak 1990'lı yılların başında başlamış ve 2000'li yılların ortasından itibaren de büyük gelişmeler kaydedilmiştir. Yani Türkiye'de siber güvenliğe ilişkin yapılan çalışmaların tarihsel gelişimi, dünya genelinde yapılan çalışmalarla paralellik göstermektedir.

Türkiye'de siber güvenlik alanında yapılan çalışmalar genel olarak TÜBİTAK bünyesinde gerçekleştirilmektedir. TÜBİTAK'a Türkiye'nin savunma sistemlerinde etkili olan resmi kurum ve kuruluşlar dışında birçok bakanlık ve hukuk birimleri de destek vermektedir. 1990'lı yıların başından itibaren Türkiye'de başta Türk Ceza Kanunu'nda hukuki düzenlemeler olmak üzere çok sayıda kanun ve yönetmelik çıkarılmıştır. Ayrıca Türkiye'de 2000'li yılların başından beri siber saldırılara karşı birtakım tatbikatlar yapılmakta ve bunlara çok sayıda resmi ve özel kurunlar destek vermektedir. Tarihsel süreç bağlamında siber güvenliğe ilişkin bu denli gelişmelerin ve ilerlemelerin kaydedildiği Türkiye'de aynı durum, günümüzde de ara verilmeksizin devam etmektedir.

Genel bir değerlendirme yapılacak olursa, Türkiye'nin siber güvenlik politikaları özellikle 2010 sonrasında küresel eğilimlerle belirgin bir paralellik göstermektedir. Ancak kuramsal literatürün de işaret ettiği üzere, etkili bir siber güvenlik ekosistemi için proaktif stratejiler, uluslararası iş birliği, yerli teknoloji yatırımları ve toplumsal farkındalık bütünleşik bir şekilde ele alınmalıdır.

Öneriler

Globalleşen Dünyada teknolojinin gelişim hızı tüm zamanların en yüksek seviyesine çıkmıştır. Kişisel, bilgi ve kurumsal verilerin nerdeyse tamamı artık siber uzayda depolanmakta ve bu bilgilerin kullanımı bilgisayar sistemleri üzerinden gerçekleşmektedir. Hal böyle olunca verilerin ve bilgilerin güvende tutulması hayli önem arz etmektedir. Çalışmada kronolojik olarak ele aldığımız siber güvenliğin gelişim sürecinde olduğu gibi bilgi sistemlerinde yaşanan gelişim alana olan ilgiyi artırmıştır. Gerek devlet gerekse özel iş ve işlemlerin sağlıklı şekilde yürütülebilmesi için siber güvenliğe önem verilmeli, gerekli tedbirler alınarak bu alandaki eğitimler gerekirse ilkokul seviyesinden başlatılarak tüm bireylerin farkındalığı artırılmalıdır. Siber güvenlik uzmanları yetiştirilmesi ne kadar önemli ise beyaz şapkalı hackerlarında yetiştirilmesi de son derece önemlidir. Literatürde sıkça kullanılan 'beyaz şapkalı hacker' kavramı, kötü niyetli saldırıların tespit edilmesi ve güvenlik açıklarının kapatılması amacıyla etik çerçevede çalışan uzmanları ifade etmektedir. Beyaz şapkalı hackerlar, sistemlere izinsiz zarar vermek yerine, yetkilendirilmiş bir biçimde güvenlik açıklarını ortaya çıkararak savunma kapasitesini artırmayı hedeflerler. Bu yönleriyle hem devlet kurumlarında hem de özel sektörde siber savunmanın kritik bir bileşeni haline gelmişlerdir (Cole, 2018, 92). Hayatı kolay kılmaya yönelik bilgi sistemleri geliştirildikçe sistemin açığını yakalamaya yönelik çalışan beyaz şapkalı hackerlar gelişime katkı sağlamalı ve devamlı denetlemeler yapmalı hatta kasti ihlaller yaparak kurulan sistemlerin daha da güvenli olmasını sağlamalıdırlar.

Beyan ve Açıklamalar

1. Araştırmacıların katkı oranı beyanı: Çalışma tek yazarlı olarak hazırlandığından tüm safhalar bizzat yazar tarafından yürütülmüştür.

2. Çıkar çatışması: Herhangi bir çıkar çatışması bulunmamaktadır.

3. Etik Raporu: Çalışmada veriler üzerinden analiz yapılmamış olup etik kurul raporu gerektirmemektedir.

4. Araştırmanın Modeli: Çalışmada nitel araştırma modeli kullanılmış olup doküman analizi yöntemiyle birincil ve ikincil kaynaklardan faydalanılarak bir derleme yapılmıştır.

References

Acarer, T. (2020). Macro cybersecurity measures that can be taken for our national security. *UBGMD, 6(2)*, 61–71. https://doi.org/10.18640/ubgmd.796168

Ağdeniz, Ş. (2021). A study on the role and competencies of public internal auditors in information and communication security auditing. *Alanya Academik Review, 5(2)*, 525-545. https://doi.org/10.29023/alanyaakademik.869215

Akçakanat, Ö., Özdemir, O., & Mazak, M. (2021). Cybersecurity risks and information technology auditing in businesses: an examination of banks' cybersecurity practices. *Mehmet Akif Ersoy University Journal of Applied Sciences, 5(2)*, 246-270. https://doi.org/10.31200/makuubd.978263

Altınbaşak, İ., & Karaca, E. S. (2009). İnternet advertising and an application on the assessment of internet advertising. *Ege Academic Review, 9(2)*, 463-487.

Aydın, M. D. (2005). eEurope+ and Turkey: compliance with European Union criteria in the field of information technology. *Hacettepe University Journal of Economics and Administrative Sciences, 23(1)*, 287-311.

Baylis, J., & Smith, S. (2017). *The globalization of world politics: An introduction to international relations (7th ed.)*. Oxford University Press.

Bıçakçı, S. (2014). NATO's emerging threat perception: cyber security in the 21st century. *International Relations, 10(40)*, 100-130.

Bıçakçı, S., Ergun, F. D. & Çelikpala, M. (2015). The cyber security scene in Turkey. The Centre for Economics and Foreign Policy Studies. https://edam.org.tr/wp-content/uploads/2016/03/edam_cyber_security_report.pdf

Biçkin, R. (2024). An examination of the concept of security in Turkey's five-year development plans [Master's thesis, Topkapı University Graduate School of Education].

Bilir, F. (2023). The emergence of applications and legal regulations for the protection of personal data. *Justice Journal (71)*, 631-651. https://doi.org/10.57083/adaletdergisi.1391733

Booth, K. (2007). *Theory of world security*. Cambridge University Press.

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal, 9(2)*, 27–40. https://doi.org/10.3316/QRJ0902027

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.

Cole, E. (2018). *Cybersecurity for beginners: Ethical hacking and defense strategies*. CyberTech Press.

Çakır, H., & Taşer, M. (2023). Evaluation of cybersecurity activities and training programs in Turkey. *Gazi University Journal of Science Part C: Design and Technology, 11(2)*, 347-366. https://doi.org/10.29109/gujsc.1165131

Çeliktaş, B. (2016). The development of the concept of cybersecurity and an assessment specific to Turkey [Master's thesis, Karadeniz Technical University].

Çetinkaya, N. (2017). The effects of e-government services on education and social life in Turkey. *International Journal of Social Sciences Academic Research, 1(1)*, 12-21.

Darıcılı, A. B. (2019). Analysis of Turkey's cybersecurity policies; recommendations for Turkey's cybersecurity model. *TESAM Academy Journal, 6(2)*, 11-33. https://doi.org/10.30626/tesamakademi.613517

Gündoğdu, S. (2023). Cyber security as an influence tool in international politics and the implementation of Turkey's cyber security policy: National Cyber İncident Response Center (USOM). *Firat University Journal of Social Sciences, 33(3)*, 1325-1337. https://doi.org/10.18069/firatsbed.1261707

Güneş, A. (2019). Global powers' national cybersecurity strategies: The case of the United States. *Cyberpolitik Journal, 4(8)*, 242–258.

Güntay, V. (2018). The transformation of cybersecurity into an instrument of influence in international politics and international actors. *Journal of Security Strategies, 14(27)*, 79-111. https://doi.org/10.17752/guvenlikstrtj.432151.

Karasoy, H. A., & Babaoğlu, P. (2021). Cyber security in Turkey: legal and institutional infrastructure. *Legislative Journal (44)*, 123-155.

Karasoy, H., & Gezici, H. S. (2023). From bombs to bytes: the role of cybersecurity in national security and the importance of artificial intelligence in cybersecurity. *International Journal of Management Academy, 6(1)*, 173-188. https://doi.org/10.33712/mana.1254015

Kestane, A., & Kurt, G. (2024). Cloud security audit: Internal audit in cloud cybersecurity applications. *Journal of the Faculty of Economics and Administrative Sciences, Ömer Halisdemir University, 17(3)*, 667-690. https://doi.org/10.25287/ohuiibf.1482734

Kestane, Ö. (2025). Cyber attacks and the need for cybersecurity audits. *İzmir SMMM Solidarity Journal, 8(1)*, 41–49.

Kılınç, D. (2016). Protection of privacy under article 9/a of law no. 5651 on the regulation of publications made on the internet and the fight against crimes committed through these publications. *Ankara Hacı Bayram Veli University Law Faculty Journal, 20(2)*, 577-624.

Kshetri, N. (2016). *Cybersecurity and cybercrime in the global context*. Routledge.

Kurnaz, S., & Karatepe, S. (2019). Cyber security of airports in Turkey within the scope of critical infrastructure security. ASAM International Public Administration Symposium Proceedings, 1–12.

Kutlu, Ö., Sevinç, Y., & Kahraman, S. (2018). Analysis of security risks in e-government applications in Turkey. *Turkish Studies, 13(21)*, 129–156.

Naralan, A. (2010). e-preparation and e-government in Turkey. *Atatürk University Journal of Economics and Administrative Sciences, 23(1)*, 1-17.

Ottis, R. (2008). Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective. Cooperative Cyber Defence Centre of Excellence Report, 1–30. https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

Önal, M. A. (2021). Dimensions of cybersecurity in the context of cyberspace and security relations. *Hitit Journal of Economics and Politics, 1(2)*, 114–123.

Özdemirci, F., & Torunlar, M. (2018). Information-Exchange-Cybersecurity-Independence. *Information Management, 1(1)*, 78-83.

Öztürk, K. B. (2009). The legal nature of authorization in electronic communications services. *Ankara Bar Association Journal (1)*, 26-42.

Reagan, J. (2001). The Love Bug virus and global email vulnerabilities. *Cybersecurity Review, 4(1)*, 38–45.

Sağıroğlu, Ş., & Alkan, M. (2018). *Cybersecurity and defense: awareness and deterrence*. Grafiker Publishing.

Sancakdar, A. (2021). Floridi's philosophy of information and big data [Master's thesis, Istanbul University].

Shakarian, P. (2011). Georgia's cyber security vulnerabilities. *Military Cyber Affairs, 2(1)*, 1–15.

Solmaz, S. B. (2011). Milestones in cybersecurity history: The evolution of threats and defense strategies. *Middle East and Asia-Caucasus Research Journal, 3(1)*, 1–9.

Tanrıverdi, E., Kurada, B., Şen, M. F., Demirkol Kılıç, E. (2023). The concept of critical ınfrastructure in the context of disaster management in Turkey. *Ankara University Journal of Environmental Sciences, 10(1)*, 1-8.

Tunca, S. (2019). The concept of cyber security in the modern age. *Dumlupınar University Journal of Economics and Administrative Sciences (3-4)*, 1-7.

Uluç, C., & Eyüpoğlu, C. (2024). The capture the flag competition approach for training qualified workforce in the field of cyber security. *Istanbul Commerce University Journal of Science, 23(46)*, 292-318. https://doi.org/10.55071/ticaretfbd.1529412

Ünsal, H. (Ed.). (2002). Turkey Information Technology Council e-government working group. Turkey Information Technology Council. https://eski.tbd.org.tr/usr_img/cd/kamubib12/diger/digercalismalar.htm

Ünver, M., Canbay, C., & Mirzaoğlu, A. G. (2011). Cybersecurity activities of international organizations. Information Technologies and Communications Authority Publishing. https://bgys.iku.edu.tr/sites/bgys/files/inline-files/Uluslararası%20Kuruluşların%20Siber%20Güvenlik%20Faaliyetleri.pdf

Ünver, N. G. (2023). *A comparative analysis of cybersecurity policies: the case of Turkey and the United Kingdom*. Livre De Lyon Publications.

Walt, S. M. (1991). The renaissance of security studies. *International Studies Quarterly, 35(2)*, 211–239.

Wiggins, R. (2010). Al Gore and the creation of the internet. *Journal of Peer Reviewed Journal on the Internet, 1(1)*, 1–17.

Yıldırım, A. (2024). Analysis of Turkey's cybersecurity policy through its action plans. *Journal of Organization and Management Sciences, 16(1)*, 23–47.

Yıldırım, E. (2024). Cyber security strategies and critical infrastructures in Turkey. *Journal of Security and Strategy, 9(1)*, 25–42.

Yılmaz, Ö. (2021). The history of Web 1.0, 2.0, 3.0, and 4.0. *Maltepe University Faculty of Communication Journal, 8(2),* 344–350.

Zetter, K. (2014). *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon*. Crown Publishing.