Terörizm ve Radikalleşme Araştırmaları Dergisi
Journal of Terrorism and Radicalization Studies

Haziran 2025, Cilt: 4, Sayı: 2, ss. 223-265

June 2025, Volume: 4, Issue: 2, pp. 223-265

ISSN 2792-0518 (Basılı/Print) **ISSN 2822-2334 (Çevrimiçi/Online)**

Makaleye ait Bilgiler / Article Information

Araştırma Makalesi / Research Article

Makale Başvuru Tarihi / Application Date : 13 Ocak 2025 / 13 January 2025

Makale Kabul Tarihi / Acceptance Date : 21 Nisan 2025 / 21 April 2025

Makalenin Başlığı / Article Title

Cybersecurity in Critical Infrastructures and Cyber Terrorism: A Strategic Analysis on Türkiye

Kritik Altyapılarda Siber Güvenlik ve Siber Terörizm: Türkiye Üzerine Stratejik Bir İnceleme

Yazar(lar) / Writer(s)

Seçkin AKÖZ & Hatice SÜRURİ

Atıf Bilgisi / Citation:

Aköz, S. and Süruri, H. (2025). Cybersecurity in Critical Infrastructures and Cyber Terrorism: A Strategic Analysis on Türkiye. *Journal of Terrorism and Radicalization Studies,* 4(2), pp. 223-265. DOI: 10.61314/traddergi.1618580

Aköz, S. ve Süruri, H. (2025). Kritik Altyapılarda Siber Güvenlik ve Siber Terörizm: Türkiye Üzerine Stratejik Bir İnceleme. *Terörizm ve Radikalleşme Araştırmaları Dergisi,* 4(2), ss. 223-265. DOI: 10.61314/traddergi.1618580

Terörizm ve Radikalleşme ile Mücadele Araştırma Merkezi Derneği

Research Center for Defense Against Terrorism and Radicalization Association

Adres/Address: Beytepe Mah. Kanuni Sultan Süleyman Bulvarı

5387. Cadde No:15A D:58

06800 Çankaya/Ankara

www.tradergisi.com

e-posta/e-mail: editortrad@teram.org

Terörizm ve Radikalleşme Araştırmaları Dergisi-TRAD, 2025, 4(2) : 223-265 Araştırma Makalesi
Journal of Terrorism and Radicalization Studies-TRAD, 2025, 4(2): 223-265 Research Article
DOI: 10.61314/traddergi.1618580

CYBERSECURITY IN CRITICAL INFRASTRUCTURES AND CYBER TERRORISM: A STRATEGIC ANALYSIS ON TÜRKİYE

Seçkin AKÖZ[*], Hatice SÜRURİ[**]

ABSTRACT

Cyber-attacks that may pose a threat to critical infrastructures (CI) have the potential to cause wide-ranging negative effects ranging from economic losses to service interruptions and social chaos. Türkiye is in a high-risk group against cyber-attacks due to its strategic geographical location and rapidly digitalizing infrastructures. Denial of service attacks on energy grids, ransomware threats in health infrastructures and data breaches on banking systems are concrete examples of the cyber security vulnerabilities that Türkiye faces. The study addresses the global dimension of cyber threats by taking into account large-scale cyber-attacks experienced internationally and examines the local effects of these threats with examples specific to Türkiye. The study evaluates Türkiye's current policies, legal regulations and defense strategies against threats. In the fight against cyber threats, the development of domestic and national technologies, strengthening cooperation at global, regional, national, international and institutional levels, international information sharing and the establishment of proactive response mechanisms against cyber threats are among the prominent strategic measures. In this context, cyber security is not only a technical issue; it is a necessity in terms of national security, economic sustainability and social stability.

Keywords: *Critical Infrastructures, Cybersecurity, Cyberterrorism, Türkiye, National Strategy, National Security*

KRİTİK ALTYAPILARDA SİBER GÜVENLİK VE SİBER TERÖRİZM: TÜRKİYE ÜZERİNE STRATEJİK BİR İNCELEME

ÖZET

Kritik altyapılara yönelik tehdit unsuru oluşturabilecek siber saldırılar, ekonomik kayıplardan, hizmet kesintilerine ve toplumsal kaosa kadar geniş kapsamlı olumsuz etkilere yol açabilecek potansiyeli barındırmaktadır. Türkiye, stratejik coğrafi konumu ve hızla dijitalleşen altyapıları nedeniyle siber saldırılara karşı yüksek risk grubunda yer almaktadır. Enerji şebekelerine yönelik hizmet reddi saldırıları, sağlık altyapılarındaki fidye yazılım tehditleri ve bankacılık sistemlerine yönelik veri ihlalleri, Türkiye'nin karşı karşıya olduğu siber güvenlik zafiyetlerinin somut örnekleridir. Çalışma, uluslararası düzeyde yaşanan büyük çaplı siber saldırılardan yola çıkarak, siber tehditlerin küresel boyutunu ele almakta ve Türkiye özelindeki örneklerle bu tehditlerin yerel etkilerini incelemektedir. Çalışmada tehditlere karşı Türkiye'nin mevcut politikaları, yasal düzenlemeleri ve savunma stratejileri değerlendirilmektedir. Siber tehditlerle mücadelede, yerli ve milli teknolojilerin geliştirilmesi, küresel, bölgesel, ulusal, uluslararası ve kurumsal düzeyde işbirliklerinin güçlendirilmesi, uluslararası bilgi paylaşımı ve siber tehditlere yönelik proaktif müdahale mekanizmalarının oluşturulması öne çıkan stratejik önlemler arasında yer almaktadır. Bu kapsamda, siber güvenlik, yalnızca teknik bir mesele değil; ulusal güvenlik, ekonomik sürdürülebilirlik ve toplumsal istikrar açısından bir zorunluluktur.

Anahtar Kelimeler: *Kritik Altyapılar, Siber Güvenlik, Siber Terörizm, Türkiye, Ulusal Strateji, Ulusal Güvenlik*

[*] Bağımsız Araştırmacı, Güvenlik Bilimleri Uzmanı, akzseckin@gmail.com. ORCID: 0000-0003-3233-1552.

[**] Dr. Gebze Teknik Üniversitesi Teknopark, haticesururi@gmail.com, ORCID: 0000-0003-0717-3230.

INTRODUCTION

As digitalization accelerates, critical infrastructures (CI) have become the building blocks of national security and social order. While the digitalization of vital systems such as energy, health, finance and transportation has increased the efficiency and accessibility of these infrastructures, it has also brought new security risks. This study aims to evaluate the cyber threats inherent in digitalized infrastructures and to reveal strategic approaches that can be developed against these threats, especially in Türkiye. As an inevitable consequence of digitalization, cybersecurity has become not only a technological issue but also a threat to the political and economic stability and national security of countries. Digital attacks on critical infrastructures can lead to a wide range of negative effects, from service interruptions to data theft, from economic losses to social chaos (Lewis, 2019, p.21). In this context, it is inevitable that cybersecurity will become a priority issue in digitalizing infrastructures. Any disruption to the functioning of critical infrastructures affects not only the individuals using these systems, but also other sectors due to interdependence between systems. Therefore, it is imperative for states to implement holistic cybersecurity policies in order to maintain national security and political stability.

Cyber terrorism threatens the security of individuals, societies and states through the malicious use of information technologies, targets critical infrastructures and aims to create fear and panic in society. Within the scope of this study, the multi-layered risks posed by cyber terrorism, both physically and digitally, are analyzed and the destructive effects of these risks on critical infrastructures are evaluated. In the information ecosystem where the physical world and the virtual world intersect, the primary targets of cyber terrorism include vital areas such as energy grids, health systems, air traffic control systems, telecommunications and financial infrastructures (Collin, 1997, p.15). The scale of these threats is not only limited to damaging individual infrastructures, but also has the potential to create instability by changing interstate dynamics in international relations and undermining global peace (Dubyna et al. 2024, p. 6952). In this framework, cyber threats are complex, destructive and challenging for states. To combat malicious cyber threats, international organizations such as the European Union (EU), the Organization for Security and Cooperation in Europe (OSCE), the United Nations (UN) and NATO (North Atlantic Treaty

Organization) focus on strategies to detect, prevent and respond to cyber-attacks (NATO, 2024). In this context, in 2016, NATO declared cyberspace as an area of operation against possible ultimate threats and developed cyber defense policies based on deterrence, defense, crisis prevention, management and cooperation to combat cyber threats (NATO, 2024).

It is observed that the effects of cyber terrorism and attacks are not only limited to short-term disruptions, but also damage public confidence and the sustainability of strategic sectors. Türkiye's focus on technological innovations, legal regulations and international cooperation in combating these threats is of vital importance for the management of these risks. Türkiye is in position more vulnerable to these threats due to its strategic location and rapidly developing digital infrastructures. As an important energy transit point on both national and regional scales, Türkiye is becoming one of the primary targets of cyber terrorism due to its geopolitical importance. This situation necessitates Türkiye to adopt a more comprehensive and holistic approach in its cyber security strategies. This article discusses the vulnerability of critical infrastructures in the face of digital threats, strategically analyzes Türkiye's current situation, and proposes concrete solutions to improve cybersecurity.

1. THE IMPORTANCE OF CRITICAL INFRASTRUCTURES IN INTERNATIONAL SECURITY IN A DIGITALIZING WORLD

The digital transformation of the 21st century has radically changed not only technology but also the understanding of international security. Access to information has become significantly easier, and the boundlessness of communication has reached alarming proportions. This situation has reshaped the security priorities of states. Wars are no longer confined to the battlefield; they now occur in energy lines, data centers, satellites, and even hospital systems. As a result, protecting critical infrastructure has ceased to be merely a technical task and has become a political, economic, and strategic necessity.

Globalization and the developments that accompany it demonstrate that today, a country's security is measured not only by its military power but also by the robustness of its water resources, energy systems, and financial infrastructure. In today's global security structure, states must be prepared not only for traditional threats but also for new risks brought about by the digital age. Threats such as cyberattacks, infrastructure sabotage, and AI-driven information manipulation have reached a borderless, complex, and often unpredictable dimension. Therefore, the protection of critical infrastructure lies at the heart of not only national security policies but also international cooperation and strategic partnerships. While digitalization has made security more complex, it has also exposed vulnerabilities more quickly. For this reason, developing a layered, comprehensive, and proactive security approach for infrastructure now forms the foundation of modern security understanding.

1.1. International Security and Critical Infrastructures in the Digitalizing World

Critical infrastructures are the physical and virtual systems necessary to ensure the continuity of the basic functions of societies and have a central role in the functioning of societies. Any failure or attack on critical infrastructure systems has the potential to directly threaten national security Critical infrastructures consist of "systems, assets and networks, whether physical or virtual" (NATO, 2021). These systems, which provide essential services such as energy, transportation, health and finance, have become smarter, more connected and more efficient as digitalization has accelerated.

However, this transformation has increased the vulnerability of critical infrastructures to cyber threats by expanding the attack surface. In this context, especially energy grids and telecommunication infrastructures are becoming targets due to the widespread use of digital control systems (Ercan, 2015, p. 4). Since critical infrastructures generate and store data on a large scale, the security of this data creates domino effects that can affect not only the organizations that provide services, but also society as a whole. Therefore, it is inevitable that the digitalization process should be addressed together with security.

The protection of critical infrastructures is not only a technical problem, but also a strategic priority in terms of national security and social order. In the process shaped by the digital transformation of society, the dependence on digital infrastructure is increasing exponentially, and the proliferation of information and communication technologies in critical infrastructures makes these systems more complex and dynamic (KAS & EDAM, 2022, p. 10). In this context, the development of national and international cybersecurity strategies, technology-oriented solutions and the integrated operation of legal regulations play a critical role in protecting critical infrastructures against cyber threats.

New security paradigms are needed to manage these threats brought about by digitalization and to increase the resilience and durability of infrastructure systems. As cyber threats are expected to become more complex in the future, strengthening these infrastructures within the framework of cyber security has become a common responsibility at both national and international levels. With the change in the dynamics of security understanding in the global framework and digitalization, a large number of threats have dominated the international arena. With the existence of new threats, non-traditional asymmetric threats have framed national and international competition and opened a space where the resilience of states and political powers is tested. These asymmetric threats are considered to be the products of the new world order in the field of defense. With modernity, the concept of total war has brought the speed of instant communication to the forefront with the changes in information and machine technologies.

In this new field of competition, cyber threats to critical infrastructures have been explicitly recognized as a significant threat element in NATO’s 2022 Strategic Concept (NATO, 2024). This explicit recognition is particularly important for the academic and strategic literature, as NATO's strategic doctrines serve as normative frameworks that influence the cybersecurity and defense postures of member states (NATO, 2024).

NATO’s framing of cyber threats as collective security issues provides not only a policy direction but also a theoretical foundation for understanding cyber conflict in international relations. NATO emphasizes operational strategies for defense, resilience, and the stability of the alliance by developing systems integrated with artificial intelligence strategies against external interventions targeting the protection of critical infrastructures. This integration of emerging technologies into strategic defense frameworks marks a paradigm shift in cybersecurity governance and has been highlighted in literature as a move toward anticipatory security models (Bellanova et al., 2022, p. 337). In this framework, international organizations such as NATO (North Atlantic Treaty Organization), OSCE, UN, and EU (European Union) are developing measures to increase resilience by improving national defense capacities, ensuring secure access to critical infrastructures, and providing alternative defense perspectives in times of crisis (NATO, 2024). Such coordinated institutional efforts reflect what Deibert (2019) terms the "securitization of cyberspace," where cyber resilience becomes a shared transnational responsibility rather than a solely national concern. In this context, the concept of cyber resilience comes to the forefront as a critical solution within cyber security strategies due to the increasing complexity and frequency of cyber threats. As Carrapico and Barrinha (2018) emphasize, the inclusion of cyber resilience in NATO doctrine signals a growing recognition of the need for adaptive, multi-layered defense structures in the face of persistent and asymmetric threats. Therefore, NATO's approach not only informs operational practices but also contributes Therefore, NATO's approach not only informs operational practices but also makes a significant contribution to the academic literature on collective" defense, digital sovereignty and strategic adaptation in the era of hybrid warfare.

1.2. Converging Threats in International Security

In the digital age, the line between cybercrime and cyber terrorism has increasingly blurred, giving rise to converging threats that pose significant risks to national and international security. As Lewis (2019) argues, cyber capabilities now allow both state and non-state actors to target critical infrastructures with disruptive, and at times, destructive intent. Particularly in geopolitically exposed countries like Türkiye, the convergence of cyberattacks with broader terror strategies has made cyberterrorism a tool not just for disruption, but for political signaling and psychological impact.

The growing sophistication of attacks on energy grids, financial networks, and public institutions demonstrates that these threats are no longer hypothetical but operational realities (Radziwill, 2018). The 2023 and 2024 ransomware attacks on Turkish public institutions and the 2020 assault on gas distribution networks are stark examples of how intertwined cyber and physical security domains have become (Kriter Dergi, 2023; Kandır, 2025). As threats evolve in complexity and attribution becomes increasingly difficult, national cyber defense strategies must adapt by integrating intelligence, infrastructure resilience, and international cooperation mechanisms (Rid & Buchanan, 2015). Thus, cyber security and cyber terrorism should no longer be treated as separate policy domains, but rather as intersecting dimensions of a comprehensive national security paradigm.

1.2.1. Cyber Security and Cyber Terrorism

Cyber security and cyber-attacks in cyberspace have become one of the most important security issues and threats of the digital age. Cyberspace, as a strategic area beyond mere technological infrastructures, represents a multi-dimensional battlefield where security, sovereignty and power dynamics come together (Kello, 2013).The concept of cyberspace encompasses not only Internet-based systems but also unmanned aerial vehicles, airplanes, radio systems and all information systems (Libicki, 2009, p.12). Unlike traditional security paradigms where physical barriers define territorial control, cyberspace blurs these boundaries, creating an asymmetric and decentralized threat environment (Rid, 2011). In cyberspace, which is defined as an "interdependent network", attackers resort to DDoS (Distributed Denial of Service) attacks to damage the availability of internet systems, and more recently to the more effective and alarming ransomware. In this context, cyber threats are deliberate attacks aimed at disrupting, disrupting or completely destroying the computer systems and critical infrastructures of the target audience (Lin, 2010, p.63). In cyberspace, where information becomes a target for attacks, all strategies designed within the framework of establishing information security have built the concept of cyber security.

Cyber terrorism is characterized by terrorist groups' efforts to damage critical infrastructures, create social fear and achieve political goals by using digital tools. DDoS attacks are among the methods frequently used by sub-state terrorist groups. DDoS attacks overload target systems with excessive data, disabling their functions and disrupting infrastructure services (Bayrakçı & Koçman, 2023, p. 188). DDoS attacks are usually carried out by networks called botnets, which consist of a group of computers hijacked with malicious software. These attacks can cause serious operational damage to states by making the targeted systems vulnerable and they are also highly attractive due to the attackers' ability to conceal their identities. Such tactics highlight how cyberspace provides an opportunity for asymmetric warfare, in which non-state actors can challenge state authority without engaging in conventional military conflicts (Arquilla & Ronfeldt, 1996; p.4).

Cyber terrorism has the potential to cause large-scale economic and social damage at both individual and institutional levels. For example, an attack on energy grids can not only affect the national economy, but also other infrastructures such as health systems (Yılmaz & Sağıroğlu, 2013). The vulnerability of critical infrastructures to such attacks makes it imperative for countries to give greater priority to cyber security policies in their national security strategies. In this context, the securitization of cyberspace has led to a paradigm shift, where digital assets are now treated as critical components of national security and necessitating coordinated international responses (Dunn Cavelty, 2008). In the future, cyber-attacks supported by the Internet of Things and artificial intelligence are expected to increase. In this context, adopting an approach supported not only by technological solutions but also by legal regulations and international cooperation will be inevitable in the fight against cyber terrorism. Moreover, cooperation with international organizations (NATO, UN and EU, etc.) are among the factors that can play a key role in managing these threats. For example, NATO has accepted cyberspace as an operational domain by integrating cyber resilience into its collective defense strategy (NATO, 2021). In countries like Türkiye that are rapidly developing their digital infrastructures, it is critical to include individuals in the digital security chain through education and awareness activities.

In cyber security, it is inevitable to develop resilient defense mechanisms against cyber threats. Early warning systems and threat analysis tools that will create resilience against cyber threats ensure that attacks are detected early and damages are minimized (Şeker, 2020, p.114). In addition, information sharing and coordination among international organizations can also form an effective defense mechanism against cyber threats (NATO, 2021, p.12). National policies to mitigate the effects of cyber threats need to cover not only technical but also economic and social dimensions. In order to fully address the geopolitical impacts of cyber threats, state actors need to go beyond traditional deterrence models and adopt multidimensional security strategies that include cyber intelligence, digital diplomacy and cross-Dectoral cooperation (Tikk & Kerttunen, 2020). In particular, to prevent economic losses, the resilience and resilience of critical infrastructures should be increased and regular stress tests should be implemented. Consequently, governance of cyberspace requires a hybrid approach that combines technological resilience, legal frameworks, and strategic alliances to counter the evolving nature of cyber threats.

1.2.1.1. Cyber Risks and Threats Affecting Critical Infrastructure

With the acceleration of digitalization, critical infrastructures have increasingly become targets of cyber threats. Vital sectors such as energy, water, transportation, and finance are subjected to attacks carried out by state-sponsored groups and organized crime syndicates. For example, in 2023, Chinese hacker groups infiltrated ports, energy grids, and telecommunications networks in the United States, demonstrating their capability to disable these infrastructures at will (The Wall Street Journal, 2025, p. 1). Similarly, in 2023, the Russia-linked group APT28 exploited a vulnerability in Microsoft Outlook to target the defense and technology sectors in Germany (The Guardian, 2024, p. 2).

The impact of cyberattacks is not limited to state-sponsored actors; financially motivated groups also target critical infrastructures. In 2023, a vulnerability in the MOVEit file transfer software was exploited by the ransomware group Cl0p, compromising the data of over 2,700 organizations worldwide (Robinson, 2025). This attack caused serious disruptions in sectors such as healthcare, finance, and public services.

Türkiye has also faced similar threats. In 2023, it ranked among the countries most affected by cyberattacks on a global scale. Iran-backed MuddyWater and Russia-linked groups targeted Türkiye’s energy and telecommunications infrastructures (Kriter Dergi, 2023, p. 4). These attacks have once again underscored the importance of enhancing the country’s cybersecurity capacity and protecting its critical infrastructures.

2. CYBER SECURITY AND CRITICAL INFRASTRUCTURES

In terms of cybersecurity, critical infrastructures has two dimensions: defense and offense. The rapid development in network technologies has led to decisions to manage critical infrastructure, which is vital for a state’s national security and public functioning, through operating systems that rely heavily on internet technologies. Therefore, states engaged in power struggles within the international system can damage each other’s critical infrastructure sectors and consider them as military targets. In this context, it is imperative for states to protect their critical infrastructure against cyber-attacks by investing in the defense capacity of these systems and trying to provide security for them. The other dimension is cyber-attack capacity. A state may seek to fully or partially damage an adversary state’s critical infrastructure by seeking opportunities, developing capabilities in this capacity, and conducting covert operations. These infrastructures not only cause economic losses if their functionality is disrupted, but also pose serious threats to national security and social order (Afyonluoğlu, 2020, p. 11). As part of a complex, interconnected ecosystem, their failure and destruction, whether physical or virtual, has the potential to weaken states in terms of national security, national public health and economic security (NIST, 2016).

Digitalization poses significant risk areas for states due to the potential for increased exposure to cyber-attacks and cybersecurity incidents, jeopardizing energy supply security, supply chains, public safety and the confidentiality of critical data for states. With the increase in cyber threats, the protection of these infrastructures has become a fundamental element of national security policies. Today, digitalization necessitates the implementation of not only physical security measures but also cyber security strategies in the defense of critical infrastructures. International organizations such as the EU and NATO create roadmaps and strategies at the level of awareness and preparedness to protect critical infrastructures within the scope of cyber security policies (EU, 2024). In this framework, the EU published the EU Security Union Strategy in 2020, aiming to ensure European security in both physical and digital areas covering the whole society at national level. While the focus of the strategy concept is on the energy sector, the strategy defined operational solution phases that can make critical infrastructures resilient against physical, cyber and hybrid threats. In strategically important countries such as Türkiye, the strategy focuses on international cooperation and local technology production for the protection of critical infrastructures, and establishes action and response plans with effective planning, monitoring and crisis management, prioritizing common minimum requirements.

2.1. Definition and Scope of Critical Infrastructure

Critical infrastructures are systems that are vital for a country's economic, social and national security. While sectors such as energy, health, transportation, communication and finance stand out in the definitions made by the European Union, new security risks arise with the integration of these systems (Karabacak, 2011, p. 2). The US Department of Homeland Security considers water supply, financial systems and communication infrastructures as critical infrastructures (Lee & Conway, 2022, p. 5). Critical infrastructures are essential services that support society and serve as the backbone for its security (NIST, 2016). According to the US National Council for the Improvement of Public Service (1990), "critical infrastructure" is defined as facilities with long economic life, economic development, high fixed costs, and a tradition of public sector involvement (CRS, 2004, p.6). In this context, critical infrastructures are the structures that build the foundations of a strong economy and national security, including airports, water and energy resources.

The concept of critical infrastructure, which has been prominent in the EU and its member states since the early 2000s (Pursuianen, 2009, p.721), has also been discussed in a multidisciplinary manner in the literature. Russia has defined its critical infrastructure strategy within the framework of national security. In this context, in its approach focused on civil defense, emergencies and national security, critical infrastructures are based on human security within the framework of a comprehensive security approach. From a state-centered national security perspective, critical infrastructures are seen as a necessity to protect society and the state from internal and external threats, to protect systems that will guarantee the implementation of constitutional rights and freedoms, independence and sustainable economic development (Pursuianen, 2021, p.22)

AFAD's (Disaster and Emergency Management Presidency) definition of critical infrastructure is; "It is the whole of networks, assets, systems and temples that may pose serious threats to citizens, health, security and economy as a result of the negative impact on the environment, social order and public services when they do not fulfill their function partially or completely" (AFAD, 2014). In Türkiye, critical infrastructures include the energy, transportation, health and finance sectors, but communication infrastructures and digital systems are also becoming increasingly important (Demirci, 2021, p.54). However, a comprehensive national strategy and standards need to be developed for these infrastructures. In particular, energy infrastructures are one of the sectors that need to be protected as a priority due to Türkiye's geopolitical position. The scope of critical infrastructures is expanding with advancing technology and digitalization. In this context, Türkiye needs to make regulations in line with international standards and focus on local solutions to ensure the security of its infrastructures. In this context, in the event of cyber-attacks on critical infrastructures, states should shape their cyber security strategies based on military, economic, civilian, social and psychological defense, as well as implement a resilience-based crisis management cycle. Resilience is the ability of a system to withstand and resist stress (Pursuianen, 2021, p.26). When faced with processes where service interruptions become difficult to prevent, it is inevitable to develop strategies that build redundancy and adaptive capabilities.

2.2. Importance of Cyber Security for Critical Infrastructures

Cyber security plays a key role in protecting critical infrastructures. Cyber security covers all activities carried out to ensure security in cyberspace. In this context, it is the existence of systems that can ensure confidentiality, integrity and accessibility criteria for cyber security (Ardielli & Ardielli, 2017, p.43). Violation of these three criteria in cyberspace means that there may be an existing threat. Especially when sectors such as energy, transportation and health systems are exposed to cyber-attacks and terrorist attacks, large-scale service interruptions and economic losses can occur. For example, the Black Energy (BE) cyber-attack on the Ukrainian energy infrastructure on December 23, 2015, has caused hundreds of thousands of people to experience unplanned power outages and demonstrated the vulnerability of critical infrastructures to cyber threats (Lee, Assante, & Conway, 2014, p.6). This attack demonstrated that remote access to energy grids can be used to take control of systems and cause large-scale damage and disruption. States’ energy infrastructures are highly interdependent through transit gas pipelines or electricity transmission networks. In this context, the protection and resilience of the relevant infrastructure element will prevent system disruption (Zoli et al., 2018, p.4). Terrorist organizations and non-state actors also target critical infrastructures, especially where interdependence exists, to expand the sphere of influence of their mass actions. The academic draft approach to understanding the interdependencies of countries came to the forefront in the 2001s. The interconnected nature of critical infrastructures makes it important to identify the problems that may arise in each infrastructure in order to manage the related interdependencies. The problem is that when critical systems are considered holistically, the failure or damage that may occur in a single element of the system may be reflected in the whole system due to interdependencies. Therefore, an attack on systemically critical infrastructures may pose a risky threat that could disrupt the entire operation.

In Türkiye, when we evaluate critical infrastructures holistically, energy grids and healthcare systems are among the most vulnerable areas. Health infrastructures are particularly exposed to attacks such as ransomware. By encrypting patient data, attackers disrupt healthcare services and put patient safety at risk (Lewis, 2006, p.1). For example, the ransomware attacks against many hospitals in Europe and Türkiye in 2020 have once again highlighted the inadequacies in protecting these infrastructures.

Cyber security strategies should not be limited to technological solutions. Early warning systems and artificial intelligence-supported threat detection systems are at a level that will allow such such attacks to be detected in advance. In addition, the resilience of infrastructures should be increased by strengthening corporate collaborations. Türkiye’s development of local software solutions in this area will reduce foreign dependency and increase its cyber defense capacity.

3. CYBER TERRORISM AND CRITICAL INFRASTRUCTURES

Cyber terrorism is a form of terrorism that targets society through attacks in the digital environment, usually aimed at creating fear and panic through cyber-attacks on states or critical infrastructures. This type of terrorism is considered a digital extension of traditional terrorism and is an expanding global threat in which individuals, institutions and states can be targeted. Considering cyber terrorism as an integral element of the digital domain, national security and intelligence-based digital surveillance has become an essential element of surveillance for states in the fight against cyber terrorism. In addition to the measures taken at the national level, the expansion of defensive practices by states against threats that may come with virtual surveillance has led to a decrease in risks in the context of national and international security.

The main purpose of cyber terrorism is to throw societies into economic and social chaos and to strain the capacity of states in crisis management (Singer & Friedman, 2014, p. 29). Such attacks are usually carried out by cyber criminals, hacker groups or terrorist organizations. Since cyber terrorism can be effectively carried out in the digital environment, its targets often cover a wider area compared to traditional terrorism. Especially the digital infrastructures of developed countries offer great opportunities for attackers. This situation shows that not only economic but also social and psychological effects can be created cyber attacks. Critical infrastructures can be targeted by cyber terrorists and cause widespread effects that can stop the functioning of states or societies (Sağıroğlu & Alkan, 2018, p. 9). For example; In the Russia-Ukraine war, cyber attacks targeting Ukraine's critical infrastructures has been a cyber terror act linked to hacktivist groups designed by Russia.

According to intelligence sources, threats to critical infrastructures are increasingly being carried out by cybercriminal organizations and states carrying out "covert" actions. Cyber terrorism can directly affect societies through attacks on these critical infrastructures. The magnitude of the impact area of the related attacks is of a nature that can have long-term consequences not only economically but also socially and psychologically (Kurum, Bilgiç, & Çardak, 2022, p. 443). In this context, cyber security measures and strategies require not only technical solutions but also global coordination and more effective information sharing. Increasing inter-country solidarity will enable for a stronger fight against cyber threats.

From a policy perspective, states are planning cyber terrorism and terrorism as a growing threat in cyberspace and developing national security policy mechanisms using an "all-hazards awareness and preparedness model" based on risk and resilience, where multiple risk factors are addressed simultaneously. Terrorist organizations and sub-state groups also build critical infrastructures or aim to seize critical infrastructures in order to target critical points and carry out their actions (Asal et al., 2015, p.5). These emerging terrorist groups are pushing the boundaries and possibilities of critical infrastructures to serve the mass purposes of the organizations all for the sole purpose of action and expanding and their area and, to get one man closer to their course.

Cyber terrorism and the protection of critical infrastructures are of increasing importance for states. In this context, resistance against cyber threats should be increased by developing national security strategies, cyber security measures, international cooperation and cyber defense policies (Atasever, Özçelik & Sağıroğlu, 2019, p.239). Protecting critical infrastructures against cyber-attacks is a policy necessity for states due to the destructive effects of digital technologies. In this context, cyber terrorism is a public responsibility for states to combat and prevent due to the limitlessness of the area it covers (Weiss & Biermann, 2021, p.1). The rapidly evolving structure of technology requires continuous updating of cyber defense systems. This will enable states to prepared to identify, control and manage cyber-attacks and risks that may arise with a stronger and more flexible infrastructure.

3.1. Definition and Scope of Cyber Terrorism

Information systems and the digital space are considered as a vulnerable area and are placed in the target of terrorists. There for using information systems to determine a target area and plan an attack is one of the important stages of cyber terrorism activity (Jormakka and Mölsa, 2005). Parks and Duggan (2011) defined cyber terrorism as an extension of conventional terrorism and a new approach in which terrorist organizations take action in cyberspace to achieve their goals. Cyber terrorism refers to terrorist activities carried out in the digital environment and generally aims to create fear and panic in society through attacks on critical infrastructures. According to Pollitt, cyber terrorism is defined as “premeditated, ideologically motivated attacks on computer systems, non-combatant targets, computer programs and data by sub-national organizations and covert intelligence agents” (Pollitt, 1998). According to Evan Kohlmann (2008), cyber terrorism is defined as “any act of terrorism that takes place on the Internet”. In this context, cyber terrorism is the use of the tools of the virtual world by terrorist organizations in cyberspace in attacks targeting online computers, networks and the information stored on them for communication, recruitment, coordination, fundraising on behalf of organizations, action planning and intelligence gathering (Kohlmann et al., 2008). Such attacks are carried out by non-state actors or state-sponsored groups and are considered the digital extension of traditional terrorism. The main objectives of cyber terrorism include threatening public security, targeting economic infrastructure and undermining public faith in state security (Singer & Friedman, 2014, p. 29). This reveals the complex nature and wide-ranging effects of cyberterrorism, as cyberattacks have a wider reach, with attacks taking place digitally rather than through physical violence (Sağıroğlu & Alkan, 2018, p. 37). According to Robert S. Mueller, cyber terrorists focus on combining physical attacks with cyber-attacks by recruiting from outside while training their members to carry out their actions in cyberspace (Nakashima, 2010). In this context, the fight against cyber-terrorism will not only be specific to states, but individual, society and state-related methods of struggle will be decisive.

Cyber terrorism also has the potential to surpass traditional terrorism with its social and psychological effects. Such attacks can create iimediate social fear and panic, while in the long run they can undermine confidence in the security and stability of the state (Kurum, Bilgiç, & Çardak, 2022, p. 458). While cyber security is becoming more important with each passing day, the complexity and impact of attacks are also increasing. This is because the global interconnectedness of digital systems allows an attack to spread rapidly over a wide area (Atasever, Özçelik, & Sağıroğlu, 2019, p. 238).

3.2. Differences between Cyber Terrorism and Traditional Terrorism

One of the main differences between cyber terrorism and traditional terrorism is the means used. While traditional terrorism uses physical violence and explosive devices to cause massive damage to targeted locations, cyber terrorism is more often a digital attack. Cyber terrorists often use digital tools such as computer viruses, ransomware and denial of service attacks (DDoS) to bring down the systems of targeted organizations or states (RAND Corporation, 2015, p. 21). In this context, traditional terrorism involves physical violence, geographical limitations, and visibility and high risk factors. Cyber terrorism, on the other hand, is a wide-area terrorism method in which attacks are carried out using digital tools such as computers, networks and software, and systems around the world can be targeted. Cyber terrorism is operationally covert, operationally low-risk and high-cost attacks.

These differences also make the impact of cyber terrorism more widespread because a cyber-attack can spread around the world in a few seconds and cause chaos on a global scale (Kurum, Bilgiç, & Çardak, 2022, p. 460). Attacks carried out in the digital environment leave fewer traces, it becomes much more difficult to track. This increases the impossibilities that attackers have to hide their identities and that states or organizations face when taking security measures (Atasever, Özçelik, & Sağıroğlu, 2019, p. 239).

3.3. Examples of Cyber Terrorism against Critical Infrastructure

3.3.1. International Cases

3.3.1.1. Estonia DDoS (Distributed Denial of Service) 2007 Attacks

The cyber-attacks on Estonia in 2007 are one of the most prominent examples of cyber-terrorism. Estonia was subjected to one of the most coordinated and comprehensive cyber-attacks against a single country to that date. The attacks took the form of Distributed Denial of Service Attacks (DDoS) on the websites of public organizations and the banking system. These attacks posed a serious threat to Estonia’s digital infrastructure and led the country to take comprehensive measures in the field of cyber security (Sağıroğlu & Kanca, 2022, p. 70; Tikk & Kaska, 2010, p. 288). Estonia’s rapid response to these attacks has been an important lesson on how to develop cyber defense strategies worldwide. The Estonian attacks not only affect inter-state relations, but also threaten the security of a nation’s digital infrastructure. These attacks have demonstrated how critical the cyber defense capacities of states are and this highlights the importance of international cooperation in the field of cybersecurity (Singer & Friedman, 2014, p. 72).

3.3.1.2. Natanz Nuclear Facility Attack

The 2010 cyber-attack on Iran’s Natanz Nuclear Facility was an example of cyber warfare as a real national security threat in the international arena. This attack was carried out with the use of a computer worm called Stuxnet and caused serious damage to Iran’s nuclear program. Stuxnet is considered to be the most sophisticated and targeted computer virus (worm) ever discovered. It specifically targets industrial control systems and is designed to sabotage centrifuges used in Iran’s nuclear facilities. After infiltrating the nuclear facility’s networks, the Stuxnet worm manipulated the systems that control the speed of centrifuges (984 centrifuges), causing them to spin at excessive speeds and thus causing damage (Holloway, 2015; Kesler, 2011). The focus of the Stuxnet attack was the ability of the virus to penetrate deeply into targeted systems. The virus used various techniques to bypass the facility’s firewall and remained undetected for a long time. The attack on the Natanz facilities opened a new dimension in international relations. It signaled that cyber threats, in addition to conventional warfare methods, could also affect international relations and even lead to conflicts. The attack increased international tension and antagonism between Iran and the other countries, causing states to take measures to increase their capacities in the cyber domain and invest more in defense systems.

4. CURRENT STATUS OF CRITICAL INFRASTRUCTURES IN TÜRKİYE

In the digital domain, where cyber-attacks have become prominent and are also used by sub-state groups, state-sponsored organizations and terrorist organizations, the protection of critical infrastructures has entered the agenda of national and international security. However, the threat posed by cyber-attacks has paved the way for states to focus on developing collective capabilities and capacities to respond to cyber-attacks, and to implement regulatory legal arrangements and strategic roadmaps between public and private institutions. Although there is disagreement in the literature on which factors should be included in the critical infrastructure classification, communication infrastructures, financial sector, commercial facilities, defense industry, emergency services, energy grids and nuclear facilities, transportation and information technology systems are considered critical infrastructures (Lewis, 2019). However, some of these sectors can be subject to attacks that can pose serious problems independent of cyberspace. The European Union (2022), has defined the sectors where a cyber threat is believed to have potentially catastrophic consequences as high critical infrastructures sectors. Accordingly, high criticality critical infrastructures are defined as transportation, energy, banking and financial infrastructures, health, drinking water, wastewater, digital infrastructures, information and communication technologies, public spaces and space (EU, 2022).

4.1. Energy Infrastructure

Türkiye is strategically located on energy transit routes, making energy infrastructures more critical for national security. Besides having national distribution lines in Türkiye's existing energy infrastructure, there are also international oil and natural gas pipelines (Baku-Tbilisi-Ceyhan Pipeline, TANAP, Turkish Stream Gas Pipeline, Kerkük-Yumurtalık Crude Oil Pipeline, etc.) is also in the transit corridor.

In energy grids and electrical systems in the energy infrastructure include all connections that allow the transmission of electricity from suppliers to consumers. They consist of power plants, storage facilities, transmission lines, distribution lines, transformers and power switches. Attacks on international power lines are focused on managing and protecting critical infrastructures that cannot be guaranteed. In cyberattacks on energy infrastructure, smart grid systems are needed to protect infrastructures (Gündüz & Daş, 2020, p.971). The goals of smart grids are to increase efficiency and reliability by using automatic control and high-power smart converters. DDoS attacks on electricity grids leave the energy sector vulnerable and negatively affect other sectors with knock-on effects (Libicki, 2009, p.66). For example, a cyber-attack on energy infrastructures in Türkiye in 2016 temporarily disabled the functionality of electricity distribution systems, clearly demonstrating the vulnerability of these infrastructures (NTV, 2016). The security of energy infrastructures can be enhanced through regular stress tests and threat detection systems. Furthermore, to build cyber resilience in the energy sector, investments should be made in domestic solutions and international standards should be harmonized. In this context, cooperation with NATO and the European Union can play a critical role in the defense of energy infrastructures.

4.2. Health Systems

The healthcare sector is particularly vulnerable to cyber threats such as ransomware and data breaches. Health infrastructures in Türkiye have faced security vulnerabilities with the digitalization process. There has been a significant increase in ransomware attacks on healthcare systems, especially during the COVID-19 pandemic. These attacks disrupted the operations of healthcare organizations and jeopardized the treatment processes of patients (KAS & EDAM, 2022, p. 12). The use of AI-powered security solutions and encryption technologies is critical to protect healthcare infrastructures. In addition, awareness should be raised by providing regular cyber security trainings for healthcare professionals, and their capacity to respond quickly to attacks should be strengthened (Booker & Musman, 2020, p.1). Measures to be taken within this framework are;

- “Identify and prepare for potential threats and risks that may occur,

- Taking measures to reduce the security vulnerabilities of critical infrastructures, systems and networks identified in connection with internal-external and interdependencies in critical sectors in the health sector,

- Mitigating the potential threatening effects of critical infrastructures during or as a result of emergencies that may occur and ensuring that the relevant failure is eliminated after damage detection,

- Regardless of the causal factors, it will be decisive to establish systems that are resilient to interruptions caused by emergencies and systems that can adapt to changing conditions in order to quickly recover from damages that may occur, as well as preventive response systems that prevent systematic and operational attacks across the sector" (EU, 2024).

4.3. Financial Systems

Banking and financial infrastructures are one of the most frequently targeted sectors by cybercriminals. Ransomware and data theft attacks on banking systems in Türkiye have caused serious disruptions in the financial sector (Yeşilyurt, 2015, p.101). For example, in 2020, an attack on a banking institution in Türkiye resulted in the leakage of customer information and millions of liras in losses. This situation shows the necessity of continuous monitoring and rapid response teams in protecting financial systems. Another cyber-attack that took place in 2015 was a large-scale DDoS attack against *Türk Telekom and the Information and Communication Technologies Authority* (BTK). The attacks caused internet services to be interrupted, and along with the speed disruption, there were disruptions or even complete stoppages in digital and sometimes physical internet-based activities across the country.

Blockchain-based solutions and artificial intelligence-supported software should be used to protect financial infrastructures (Goeva et al., 2024, p.1). In addition, comprehensive training programs should be implemented to raise individuals' financial security awareness and regulatory bodies should strengthen cybersecurity protocols.

5. TÜRKİYE'S GEOSTRATEGIC POSITION AND INCREASING RISKS AND THREATS TO CRITICAL INFRASTRUCTURE

21. century, traditional geopolitical concepts such as land-based borders, maritime control or air superiority are no longer sufficient to explain strategic power. Instead, cyberspace has emerged as a distinct and dynamic space in which national interests are discussed and redefined. Rather than analyzing Türkiye's position through classical geopolitical lenses, its geostrategic importance must now be included in the developing cyberspace logic, which is an area shaped by digital infrastructures, information flows and cyber sovereignty. In this new environment, power is not solely determined by physical control, but also by a state's ability to protect,

disrupt, or govern the virtual architectures that sustain both civilian life and national security (Castells, 2009; Nye, 2010; Rid, 2020). These attacks in cyberspace not only cause infrastructural damage, but also target a state's strategic capacity, international reputation and social integrity.

In this multi-layered threat environment, Türkiye's geostrategic location makes it not only a physical bridge but also a "digital transit corridor". Türkiye is both a target and a transit route for attacks that may occur in cyberspace, as it is the crossroads of digital data flows connecting Europe, Asia and the Middle East. This situation necessitates Türkiye to address its cybersecurity policies not only from a defense perspective but also as a geopolitical priority.

Türkiye stands out as an important actor on both regional and global scales due to its geopolitical position. As an energy transit hub between Europe, Asia and the Middle East, Türkiye plays a strategic role in energy security with projects such as TANAP (Trans Anatolian Natural Gas Pipeline) and Baku-Tbilisi-Ceyhan. However within the context of cyberspace, these infrastructures represent not just physical assets but also critical digital terrains- vulnerable to cyberterrorism and state-sponsored attacks. These infrastructures are increasingly becoming high-value targets for adversial actors employing asymmetric methods such as ransomware, malware, or sabotage. Such attacks not only compromise operational continuity but also trigger cascading disruptions across financial markets, trade routes, and diplomatic engagements.

The strategic logic of cyberspace significantly undermines the basic assumptions of classical deterrence and war theories. The frequent targeting of Türkiye's financial, communication and defense infrastructures concretizes the geopolitical risk this new area poses. Indeed, ransomware attacks targeting the banking sector in recent years have clearly revealed the digital vulnerabilities and structural weaknesses of these infrastructures (Aydın, Barışkan & Çetinkaya, 2021, p. 156). The perpetrators of cyberattacks are often unidentifiable, and unlike classical security threats, the threshold for attack is often unclear; conflicts begin before they are officially declared and progress in a hybrid form (Rid, 2020). For this reason, cyberspace stands out as a strategic area of competition that disrupts traditional military power balances and enables asymmetric actions. As Joseph Nye (2010, p.1) stated, cyberpower is not only technical capacity, but also the ability to manage perception, manipulate information and disrupt the opposing party's decision-making mechanisms.

As Joseph Nye (2010) points out, cyber power is inherently asymmetric; it privileges those who can move flexibly within open, decentralized networks. For Türkiye, this requires a strategic shift: national cyber security cannot be considered solely as a defensive posture, but must also include active deterrence, digital diplomacy, and network resilience. Manuel Castells (2009) emphasizes that power in the information age flows through networks; not only military alliances, but also data infrastructures and software ecosystems. In this sense, Türkiye's integration into transnational cyber defense networks (e.g. NATO's CCDCOE) becomes a way to strengthen not only protection but also digital sovereignty.

Moreover, cyberspace challenges the Westphalian paradigm by shifting the locus of sovereignty from territory to information. In such an environment, strategic depth is measured not in kilometers but in milliseconds of response time, degrees of system redundancy, and real-time threat detection capabilities. Türkiye's increasing participation in NATO's cyber doctrines (especially those emphasizing resilience and multilayered defense) reflects this transition (NATO, 2023). Moreover, cyberterrorism, which blurs the lines between political violence and digital sabotage, highlights the urgency of rethinking national security beyond traditional borders.

The convergence of cybersecurity and cyberterrorism highlights the need to reconceptualize geostrategy through the lens of cyberspace. As the boundaries between state and non-state actors, war and crime, and public and private sectors continue to erode, cyber resilience is becoming not only a technical requirement but also a geopolitical imperative. For a state like Türkiye, at the crossroads of continents, alliances, and conflicts, digital sovereignty and strategic adaptability in cyberspace are now essential components of national power On the other and increasing complexty of cyber threats requies coordination not only national level but also at the regional level. Türkiye should develop its own cyber policy doctrine against freely evolving threats, taking into account all this inclusiveness.

5.1. Threats Specific to Türkiye

Türkiye’s geostrategic position and rapid digitalization have significantly increased its exposure to cyber threats, particularly targeting critical infrastructure sectors such as energy, finance, and public services. Among these, the energy sector has become a primary target due to its strategic importance and technological vulnerability.

These developments reveal that digital and physical security areas can no longer be addressed separately. It is clear that Türkiye needs an integrated security strategy to protect its critical infrastructures. This strategy should encompass not only technological solutions but also institutional coordination, crisis management capacity and public-private sector collaboration.

Cyberattacks targeting Türkiye’s energy infrastructure have escalated both in frequency and complexity. According to Kaspersky's 2022 report, the percentage of industrial control system (ICS) computers in Türkiye’s energy sector that encountered malicious objects reached 43.2% in the second half of the year—an increase of 1.8 percentage points compared to the first half (Kaspersky, 2023). These attacks aimed to infiltrate and disrupt industrial systems that manage energy generation and distribution, highlighting a critical vulnerability in the nation’s cyber defense posture. This upward trend in cyber threats demonstrates the urgent need for Türkiye to reassess its national energy security paradigm—not only in terms of physical resilience but also through comprehensive cyber defense strategies. Given the cross-border and non-attributable nature of cyberattacks, enhanced collaboration with international cybersecurity frameworks, including NATO, is essential to mitigate such evolving threats.

In 2023, several banks in Türkiye were targeted by DDoS attacks on their digital platforms, resulting in significant disruptions to internet banking services. These attacks prevented users from accessing their accounts and caused considerable delays in financial transactions (Kriter Dergi, 2023). In the same year, ransomware attacks were carried out against the digital infrastructures of various public institutions, leading to the temporary suspension of municipal services. As a result, citizens experienced interruptions in accessing essential public services, and the security of public data was severely compromised (Kriter Dergi, 2023). In recent years, Türkiye has increasingly become a target of both cyber and physical security threats. This trend underscores the necessity of a comprehensive and multidimensional security approach, particularly for the protection of critical sectors such as public institutions, the energy sector, and healthcare infrastructure.

In 2015, large-scale DDoS attacks targeted DNS servers with the ".tr" extension; access to thousands of websites was temporarily cut off. These attacks revealed the vulnerabilities in Türkiye's digital infrastructure and the lack of resilience of public information systems (Kandır, 2025). In 2020, a ransomware attack on an energy company that distributes natural gas in major cities halted the company's operations and revealed the infrastructure's vulnerability to cyber threats (Kandır, 2025). In the same year, the websites of various government ministries were subjected to simultaneous cyber attacks; Access to many institutions, including the Presidency's of the Republic of Türkiye Directorate of Communications, has been temporarily cut off (DGRNET, 2024, p. 4).

A cyber attack on the Ministry of Health in 2021 targeted personal health data. This incident has once again shown how sensitive health systems are in terms of cybersecurity, especially during the pandemic (DGRNET, 2024, p. 2). In addition to cyber threats, security risks related to the physical domain and intelligence have also come to the forefront. The terrorist attacks targeting the Ministry of Interior in October 2023 and the TUSAŞ facilities in 2024 have demonstrated that national security concerns are not limited to the digital sphere, but also encompass the physical domain and intelligence dimensions (Ceylan, 2024, p. 6).

These developments show that digital and physical security areas can no longer be considered separately. It is clear that Türkiye needs an integrated security strategy to protect its critical infrastructures. This strategy; in addition to technological solutions, it should also include elements such as institutional coordination, crisis management capacity and public-private sector cooperation

6. CYBER SECURITY AND THE FIGHT AGAINST CYBER TERRORISM IN TÜRKİYE

Türkiye is taking important steps in the field of cyber security against the increasing cyber threats on a global scale and developing various strategies to combat cyber terrorism. Within the framework of national security strategies, cyber security is seen as the guarantee of both the state's understanding of security and economic and social security. In recent years, Türkiye has been trying to overcome its deficiencies in this field with the policies and strategies it has developed in the field of cyber security and has been conducting a more effective fight against cyber terrorism. In this context, cyber resilience, proactive cyber defense and deterrence, people-oriented cyber security approach, safe use of technology, domestic and national technologies in combating cyber threats, as well as the activities carried out by the Digital Transformation Office, ICTA and TÜBİTAK are effective.

6.1. National Cyber Security Policies and Strategies

Türkiye published its first National Cyber Security Strategy in 2013 and updated it in 2019. The National Cyber Security Strategy aims to protect critical infrastructures, detect cyber-attacks and develop effective response methods. While strengthening Türkiye's digital security infrastructure, the strategy also emphasizes the development of domestic cyber security products (Sağıroğlu & Alkan, 2018, p. 51). With its cyber security strategy, Türkiye aims to combat cyber threats not only at the national level but also at the global level.

The success of cyber security strategies depends on the strong cooperation of both the state and the private sector. Türkiye's cybersecurity strategy emphasizes the need to spread cybersecurity awareness in the public and private sectors. In particular, it is stated that institutions should have the capacity to detect threats in advance and take precautions. At this point, including the private sector in these strategies will be an important step in protecting critical infrastructures (Kurum, Bilgiç, & Çardak, 2022, p. 461). In addition, Türkiye's indigenous technologies developed in the field of cyber security have great potential for increasing its cyber defense capacity. Indigenous software and hardware reduce foreign dependency, while at the same time increasing the international competitiveness of domestic producers in this field. However, the rapidly changing nature of cyber threats requires continuous updating of cyber security policies. Within the framework of these policies, the "Cyber Security Presidency" was established with the decree published in the Official Gazette dated January 8, 2025. The Presidency will develop action plans and strategies to develop policies and objectives to ensure cyber security.

6.2. Legal and Regulatory Framework

The legal and regulatory framework in Türkiye plays an important role in combating cybercrime and ensuring cybersecurity. Law No. 5651 provides an important legal basis for combating cybercrime and crimes committed in the digital environment. This law defines offenses such as defamation, slander, and violation of personal data committed over the internet and imposes criminal sanctions (Acay, 2021, p.87). In addition, the Law on the Protection of Personal Data adopted in 2016 introduced important regulations for the protection of personal data in the digital environment. However, only legal regulations are not sufficient for cyber security. The effective implementation of these regulations requires strengthened oversight mechanisms and more training. Furthermore, active support from the private sector should be sought in the fight against cybercrime.

Türkiye's success in combating cybercrime relies on the effectiveness of both legal and administrative structures. From a national security perspective, broader cooperation is needed to combat a threat as complex and transnational as cyber terrorism. In order to combat global threats, Türkiye's cybersecurity laws should be continuously updated in parallel with international developments (Sağıroğlu & Alkan, 2018, p. 36). In this context, the National Cyber Security Law No. 7545, which entered into force in March 2025, has been a transformative step in Türkiye's cyber governance. This comprehensive legislation has brought significant reforms. Some of these reforms include mandatory periodic cyber risk assessment reports for critical infrastructure sectors (such as energy, finance, telecommunications), the establishment of the National Cyber Threat Intelligence Center, and gradual sanction mechanisms for non-compliance. The law also clarified the obligations of public and private sector actors regarding incident reporting processes, expanded the authorities of the National Cyber Incident Response Center (USOM), and institutionalized international cybersecurity cooperation. One of the most striking aspects of Law No. 7545 is that it has brought Türkiye's cyber resilience planning more in line with EU and NATO standards by placing public-private sector cooperation on a legal basis (Resmi Gazete, 2025).

Developing cybersecurity laws within the framework of international cooperation will play a critical role in mitigating the effects of cybercrime and cyberterrorism not only in Türkiye but also worldwide. Therefore, Türkiye’s harmonization with global cybersecurity regulations is important in terms of consolidating international cooperation.

6.3. Current Situation in the Protection of Critical Infrastructures

In Türkiye, critical infrastructures in the energy, healthcare and finance sectors can be vulnerable to cyber threats. Especially in the energy sector, cyber-attacks can cause major damage by targeting critical systems. Therefore, more effective cyber security measures are needed to protect energy infrastructures (Kurum, Bilgiç, & Çardak, 2022, p. 460). Türkiye’s energy sector should be harmonized with cybersecurity standards and the resilience of systems against cyber threats should be increased. However, infrastructures in the healthcare sector are also highly vulnerable to cyber threats. Cyberattacks on the energy and manufacturing sectors in Türkiye are on the rise. According to Kaspersky's 2022 data, 41.9% of Industrial Control System (ICS) computers in Türkiye faced cyber threats. The energy sector is among the most attacked sectors (Kaspersky, 2023).

Critical data such as digital health records, patient information and medication management can be targeted by cyber-attacks, which can not only breach personal data but also harm public health (Singer & Friedman, 2014, p. 75). Protecting digital systems in the healthcare sector is critical to preventing cyberattacks that threaten public health. Healthcare organizations need to invest more in cybersecurity and strengthen their infrastructure. Financial systems are one of Türkiye’s most vulnerable sectors and should have the highest standards of cybersecurity. Türkiye should adopt a more integrated and comprehensive security approach for continuous monitoring and protection of digital infrastructures in the financial sector (Tikk & Kaska, 2010, p. 293). Cyber-attacks targeting financial systems can cause huge economic losses and seriously undermine public confidence. Therefore, closing vulnerabilities in financial systems is an important part of cybersecurity policy.

7. DEFENSE AND PREVENTION STRATEGIES

Cyber security plays a critical role in ensuring national security, economic stability and social trust in today’s digitalized world. In particular, cyber terrorism and cybercrime pose significant threats to states and the private sector. An effective fight against these threats is not only possible through technology-based solutions, but also requires the development of strong defense and prevention strategies. These strategies are necessary not only to defend against cyber-attacks, but also to anticipate the effects of these attacks and minimize risks through early response and rapid recovery mechanisms. In this framework, it will be decisive to take prevention and response steps to detect and prevent cyber-attacks in advance and to create deterrent mechanisms (NATO, 2024).

Defense and prevention strategies are generally shaped around domestic and national technologies, public-private partnerships, international cooperation and proactive response approaches (Aksu Ereker, 2019). These strategies include key elements such as strengthening cyber security infrastructure, early detection of threats and rapid response to attacks. In addition, increasing information sharing among countries and establishing common defense mechanisms are also of great importance in the fight against cyber terrorism. Türkiye's cyber security strategies are shaped in this direction and include many important steps, from the development of indigenous solutions to the strengthening of international cooperation.

7.1. Domestic and National Technological Solutions

Domestic and national technological solutions play a critical role in Türkiye's cyber security strategies. In recent years, the development of indigenous cyber security software and hardware has enabled Türkiye to take important steps towards reducing its dependence on foreign sources. These solutions both reinforce national security and make Türkiye more resilient against cyber threats. Domestic software and hardware increase Türkiye's security power not only in the local scale but also in the international arena (Sağıroğlu & Alkan, 2018, p. 167).

Türkiye's success in this field shows that in addition to domestic production solutions, innovative strategies in cyber security should also be developed. The state's cyber security strategies become more effective through collaborations with the private sector. Public and private sectors acting together not only strengthen the cybersecurity infrastructure, but also increase Türkiye's technology production capacity in this field (Kurum, Bilgiç, & Çardak, 2022, p. 446). Since externally dependent systems may lose their effectiveness, especially in times of crisis, local solutions will also help to respond more quickly and effectively to cyber threats. Developing indigenous solutions is of great importance not only for national security but also for economic development. In this context, the development of indigenous technologies will increase Türkiye's technology exports as well as its goal of becoming an independent country in the field of cyber security. Türkiye's investments in indigenous solutions in cyber security will also provide a significant advantage in its competition with other countries.

7.2. Public-Private Sector Cooperation Models

Public-private partnerships are especially important in combating threats to critical infrastructures. The effectiveness of cybersecurity strategies in Türkiye relies on cooperation between the governments's regulatory and oversight role and the private sector's innovative solutions. This collaboration enables faster and more efficient implementation of cybersecurity strategies. Especially in critical sectors such as financial and energy infrastructures, a stronger cybersecurity infrastructure can be created when the private sector's capacity to produce technology and the public sector's regulatory role are combined (Kurum, Bilgiç & Çardak, 2022, p. 461). However, cooperation between the public and private sectors should not be limited to joint projects. A stronger interaction between these two sectors should also be ensured in information sharing and training processes. This approach is critical not only for cyber security but also for the security of all digital infrastructures (Hekim & Başıbüyük, 2013, p. 137). Cyber security infrastructures developed through public-private partnerships will create a more secure environment in the digital environment and enable faster reactions to cyber threats. Moreover, the development of these collaborations may lead to more research and development (R&D) activities in the field of cyber security. These R&D activities will increase the effectiveness of Türkiye's cybersecurity strategies, not only for the country's internal security, but also on a global level. Strong collaborations between the public and private sectors can make Türkiye a more independent and powerful actor in cybersecurity. Cyber security should not be limited to technical measures; it should also include education, awareness, and international cooperation. For example, institutions such as CISA in the USA cooperate with the private sector in protecting critical infrastructures. In addition, international norms adopted under the leadership of the United Nations require states to act responsibly in the cyberspace and avoid attacks on critical infrastructures (Kesan, Hayes, & Bashar, 2021).

7.3. International Cooperation and NATO Integration

Since cyber security is a threat that transcends national borders, international cooperation against this threat is of great importance. Within the framework of its NATO membership, Türkiye is strengthening international cooperation in cyber security and developing a collective defense mechanism against cyber terrorism. NATO aims to develop a common strategy against cyber security threats among member states and Türkiye plays an important role as a part of these strategies (Singer & Friedman, 2014, p. 78).

By strengthening its cyber defense capacity with NATO, Türkiye is establishing a common line of defense against global cyber threats. This cooperation creates a strong solidarity against cyber threats not only for Türkiye but also for all NATO member states. Sharing cyber security knowledge and experience at the international level will play a key role in eliminating vulnerabilities in this area (Polat, 2020, p. 149). Information sharing with NATO and other international organizations will not only enable early detection of cyber-attacks, but will also help establish an international standard in cyber security. Türkiye’s NATO integration will enable a more effective response to global cyber threats and strengthen international cooperation.

7.4. Proactive and Reactive Response Mechanisms

The effectiveness of cyber security strategies relies on both proactive and reactive response mechanisms. Proactive intervention involves detecting threats in advance and taking necessary measures against them. Such interventions are made possible by early warning systems and continuous monitoring (Tikk & Kaska, 2010, p. 294). Türkiye is working on developing such proactive systems to detect threats to its critical infrastructures in advance.

Reactive response, on the other hand, ensures a fast and effective response when a cyber-attack occurs. These responses help limit the impact of cyber-attacks and allow infrastructures to return to normal quickly. By strengthening these response mechanisms, Türkiye is becoming more resilient against cyber-attacks (Çahmutoğlu, 2020, p. 68). Proactive response means detecting attacks before they occur and being prepared for these threats. Reactive response, on the other hand, requires effective crisis management to minimize the damage caused by attacks. Türkiye’s strategies combining these two approaches play a key role in ensuring strong protection against cyber threats to critical infrastructures.

8. STRATEGIC RECOMMENDATIONS FOR TÜRKİYE

8.1. Roadmap for Countering Cyber Terrorism in Critical Infrastructure

Türkiye is developing strong cyber security strategies against cyber threats to critical infrastructures. The relevant strategies cover both cybersecurity and cyberterrorism dimensions in line with national security policies. Türkiye's National Cybersecurity Strategy, published in 2019, provides a guiding framework on how to approach cyberattacks to critical infrastructures (Tüzün, 2022). This strategy aims to detect cyber threats in advance, respond quickly to potential attacks, and take the necessary precautions. Within this framework, cyberattacks deepening with connectivity are important and the "cyber resilience" strategy is important for continuity in the cyber world (Demhack, 2011, p.76). The 2024-2028 National Cybersecurity Strategy and Action Plan was prepared based on the themes of "Human", "Defense", "Deterrence" and "Cooperation" and focused on the transformation of relevant themes into action within a concrete framework (UAB, 2024).

In the event of attacks on critical infrastructures, states are trying to resolve the issue with a paradigm shift from "protection to resilience". In the 2000s, the European Union launched the European Critical Infrastructure Program (EPCIP) to combat cyber threats. The focus of the EPCIP program is to offer solutions with a conventional approach to protect critical infrastructures. Since the conventional approach carries the risk of not being sufficient to prevent all threats, it will not be possible to protect all critical infrastructures. In this context, strategies such as robustness, stress resistance and resilience of critical infrastructures against possible crises have been focused on (Liu & Song, 2020). The term resilience is derived from the Latin word "*resiliere*", which means "bounce back". In this context, resilience refers to the capacity to adapt to changing conditions, withstand disruptions caused by emergencies and recover quickly. The focus is on resilience "against a variety of expected and unexpected events and risks". These risks are systemic due to their operational dimensions, their ability to be realized through virtual or physical means, and the uncertainty and complexity of the threats.

The first step to prevent cyber threats to critical infrastructures should be to continuously update national security policies. The rapidly changing nature of technology requires cyber security strategies to be in constant evolution. Türkiye should consider not only current threats but also potential future cyberattacks and be prepared for them (Polat, 2020, p. 136). Within the scope of this strategy, developing domestic technologies, reducing foreign dependence and using domestic cyber security products have an important place. In Türkiye's cyber security strategy, a structure supported by innovative solutions from the private sector and academic research should be established. In this way, knowledge accumulation and technology development processes in the field of cyber security will become faster and more effective. Moreover, public-private sector cooperation will ensure more successful implementation of these strategies.

8.2. The Role of Academia and the Private Sector

Collaboration between academia and the private sector is crucial for success in cyber security. Academic research enables a better understanding of cyber threats and the development of new security technologies. Universities and research institutions in Türkiye (e.g. TÜBİTAK BİLGEM, BTK) play an important role in cybersecurity knowledge production (Hekim & Başıbüyük, 2013, p. 155). These institutions work to develop next-generation cyber security solutions and take precautions against potential cyber-attacks.

The private sector is a critical stakeholder in cyber security with its innovative solutions and technology development capacity. In particular, Türkiye's leading technology companies are developing indigenous cyber security solutions and implementing these solutions in cooperation with the government. These collaborations between the public and private sectors will enable Türkiye to fight more effectively against cyber threats (Sağıroğlu & Alkan, 2018, p. 36). A strong collaboration between the academic world and the private sector will ensure that research in the field of cyber security is transformed into viable solutions. These collaborations also allow for a stronger preventive mechanism against future cyber threats. Universities and the private sector in Türkiye can build a more robust digital infrastructure by developing joint projects in cybersecurity.

8.3. Strengthening International Information Sharing and Cooperation

As cyber security has become a global threat, strengthening international cooperation is of utmost importance. In this context, Türkiye needs to increase its cooperation with NATO and other international organizations. NATO's strategies in the field of cyber security enable member states to act in a common language (Polat, 2020, p. 145). By strengthening its integration with NATO, Türkiye can create a more effective defense mechanism against global cyber threats. Such cooperation enables not only information sharing but also the coordinated development of cyber defense strategies.

International cooperation will contribute to enhancing Türkiye's cybersecurity capacity and enable the creation of a broader cybersecurity network. Increasing information sharing between countries on a global scale allows for a faster and more effective response to cyber threats (Çahmutoğlu, 2020, p. 69). Türkiye's strengthening international cooperation in cybersecurity will contribute significantly to both the prevention of cybercrime and the fight against cyberterrorism. International information sharing provides not only defense in cybersecurity but also global solidarity against cyber threats. Türkiye's cooperation with NATO is an example of global information sharing in this area. As cyber-attacks increase on a global scale, Türkiye's strengthening of such cooperation will help ensure not only national security but also worldwide security.

CONCLUSION

This article has aimed to comprehensively examine the cybersecurity risks faced by Türkiye's critical infrastructures and the strategic approaches required to combat cyber terrorism. In today's rapidly digitizing world, critical infrastructures are not only technological systems but also fundamental pillars of national security and social stability. Infrastructures serving sectors such as energy, healthcare, and transportation have become integral components directly affecting the daily functioning of society. However, with increasing digitization, these systems are increasingly exposed to cyber threats, which in turn makes defense requirements more complex. Due to both its strategic location and the rapid development of its digital infrastructure, Türkiye finds itself in a particularly vulnerable position against threats like cyber terrorism.

The study has addressed Türkiye's current cybersecurity policies, their practical implementations, and potential strategic steps to counter emerging threats. Prioritizing domestic and national technologies, strengthening public-private sector cooperation, enhancing international information sharing, and developing proactive intervention systems are of critical importance for increasing Türkiye's resilience against cyber threats. These elements should be considered not only on a technical level but also as part of a holistic approach involving governance and strategic development. Moreover, constructive collaborations with international institutions will not only assist in neutralizing external threats but also bolster Türkiye's competitiveness on the global cybersecurity stage.

Progress in cybersecurity cannot be achieved solely through technical and institutional measures. Raising awareness across all segments of society is essential to ensuring the long-term effectiveness of security policies. Cybersecurity should not be regarded solely as a matter for the state or certain institutions, but as a shared responsibility encompassing a wide range of actors—from individuals and private sector entities to public institutions and academic circles. In this context, educational policies must be restructured around digital literacy and cybersecurity awareness. Encouraging younger generations to engage with this field from an early age is a strategic investment not only to address current threats but also to build the cybersecurity architecture of the future. This approach could contribute to Türkiye becoming a regional hub for cybersecurity in the long run.

Looking ahead, it is of great importance for Türkiye to invest in AI-supported defense systems, increase its pool of qualified human resources, and implement sector-specific risk analyses in order to further strengthen its capacity in this domain. In the coming years, it will be essential not only to build mechanisms that can defend against existing threats, but also to develop an effective deterrence capacity. In this regard, forming more integrated and functional partnerships with international structures such as NATO will play a key role in elevating Türkiye's cybersecurity ecosystem to global standards. In conclusion, the findings of this study demonstrate that while Türkiye has made significant strides in enhancing the security of its critical infrastructure and building resilience against cyber threats, this process can only be rendered sustainable through a continuous, strategic, and multidimensional approach. Combatting cyber terrorism requires a comprehensive will that extends beyond technical solutions and encompasses political, economic, and social dimensions.

REFERENCES

Acay, F. (2021). Sosyal Medya Aracılığıyla Hakaret Suçu ve Suçun Tespitine Ilişkin Uygulamalar. *İstanbul Aydın University Faculty of Law Journal*, *7*(1), 71-140. Accessed: November 12, 2024.

AFAD (2014). AFAD Critical Infrastructure Protection Roadmap Document. Accessed: November 20, 2024. https://www.afad.gov.tr/kurumlar/afad.gov.tr/3906/xfiles/teknolojik-afetler-son.pdf.

Afyonluoğlu, M. (2020). *Siber Güvenlik ve Kamu Politikaları*, Teknoloji ve Kamu Politikaları Kitabı, ss. 379-411, (Editör: Mete Yıldız-Cenay Babaoğlu), Gazi Kitabevi, Ankara, 2020.

Aksu Ereker, F. (2019). “NATO’s Security Understanding and Strategic Concepts”. Security Articles Series, No.23, October 2019. Accessed: December 12, 2024. https://trguvenlikportali.com/wp-content/uploads/2019/11/NATOStratejikKonseptleri_FulyaAksuEreker_v.1.pdf. https://doi.org/ 10.13140/RG.2.2.12855.47527.

Ardielli, E. & Ardielli, J. (2017). Cyber Security In Public Administration of the Czech Republic. *Social & Economic Review, 15*(4). https://fsev.tnuni.sk/revue/papers/147.pdf.

Arquilla, J. & Rondfeldt, D. (1996). *The Advent of Netwar*. Published Rand Corporation, ISBN: 0-8330-2414-0, National Defence Research Institute. Accessed: March 30, 2025. https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR789/RAND_MR789.pdf.

Asal, V. H., Park, H. H., Rethemeyer, R. K., & Ackerman, G. (2015). With Friends Like These Why Terrorist Organizations Ally. *International Public Management Journal*, 19(1), 1–30. https://doi.org/10.1080/10967494.2015.1027431.

Atasever, A., Özçelik, A. & Sağıroğlu, Ş. (2019). *Cyber Terrorism and DDoS*. Süleyman Demirel University Journal of Natural and Applied Sciences Volume 23, Issue 1, 238-244, 2019. DOI: 10.19113/sdufenbed.507948.

Aydın, H., Barışkan, M. A., & Çetinkaya, A. (2021). *Siber Güvenlik Kapsamında Enerji Sistemleri Güvenliğinin Değerlendirilmesi*. *Güvenlik Bilimleri Dergisi, 10*(1), 151-174.

Bayrakçı, E. & Koçman, M. A. (2023). *Bilgi Güvenliği ve Elektronik Harp. Necmettin Erbakan Üniversitesi Siyasal Bilgiler Fakültesi Dergisi, 5(Özel Sayı), 184-206.*

Booker, L. B., & Musman, S. A. (2020). A Model-based, Decision-theoretic Perspective on Automated Cyber Response. *arXiv preprint arXiv:2002.08957*. Accessed: December 12, 2024. https://doi.org/10.48550/arXiv.2002.08957.

Bellanova, R., Carrapico, H., & Duez, D. (2022). Digital/Sovereignty and European Security Integration: an Introduction. *European Security, 31*(3), 337–355. https://doi.org/10.1080/09662839.2022.2101887.

Carrapico, H. & Barrinha, A. (2018). European Union Cyber Security as an Emerging Research and Policy Field. *European Politics and Society, 19*(3), 299–303. https://doi.org/10.1080/23745118.2018.1430712.

Castells, M. (2009). The Rise of the Network Society. Oxford: Blackwell Publishing. ISBN: 978-1-405-19686-4.

Ceylan, F. (2024). "'Kritik Altyapının Korunması ve Dayanıklılık", Çevrimiçi Yayın, 1 Kasım 2024. https://www.uikpanorama.com/blog/2024/11/01/tusas-saldiri-altyapi-fc.

CISA (2009). Critical Infrastructure Security and Resilience. Accessed: December, 10 2024. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience.

Collin, B. (1997). The Future of Cyberterrorism: Where the Physical and Virtual Worlds Converge. *Crime and Justice International*, *13*(2), 15-18. Accessed: 28.12.2024 https://www.ojp.gov/ncjrs/virtual-library/abstracts/future-cyberterrorism-physical-and-virtual-worlds-converge.

CRS (2004). Critical Infrastructure and Key Assets: Definition and Identification. CRS Report for Congress Received through the CRS Web. https://apps.dtic.mil/sti/pdfs/ADA454016.pdf.

Çahmutoğlu, E. (2020). Siber Uzayda Güç ve Siber Silah Teknolojilerinin Küresel Etkisi. Analytical Politics, 1(1), 63-79.

DGRNET (2024). Türkiye'nin Maruz Kaldığı Şimdiye Kadarki En Büyük 5 Siber Saldırı. https://www.dgrnet.com.tr/2024/08/turkiyenin-maruz-kaldigi-simdiye-kadarki-en-buyuk-5-siber-saldiri/.

Deibert, R.J. (2019). The Road to Digital Unfreedom: Three Painful Truths About Social Media. *Journal of Democracy 30*(1), 25-39. https://dx.doi.org/10.1353/jod.2019.0002.

Demchak, C. C. (2011). *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security*. University of Georgia Press, Athens and London.

Demirci, K. (2021). Kritik Altyapılarda Siber Güvenlik ve AFAD Üzerinden Bir Değerlendirme. *Nazilli İktisadi ve İdari Bilimler Fakültesi Dergisi*, *2*(2), 54-64.

Denning, D. E. (2017). Cyberterrorism: The Logic Bomb Versus the Truck Bomb. *In Cyberspace Crime*, pp. 217-225, Routledge.

Dubyna, M., Shchur, R., Shyshkına, O., Sadchykova, I., Panchenko, O., & Bazılınska, O. (2024). The Role of Artificial Intelligence in the Cybersecurity System of Banking Instıtutıons in the Conditions of Instability. *Journal of Theoretical and Applied Information Technology, 102*(19), 6950-6965. E-ISSN: 1817-3195.

Dunn Cavelty, M. (2008). Cyber-Security and Threat Politics: US Efforts to Secure the Information Age (1st ed.). Routledge. https://doi.org/10.4324/9780203937419.

Ercan, M. (2015). *Kritik Altyapıların Korunmasına İlişkin Belirlenen Siber Güvenlik Stratejileri* (Master's Thesis, Gebze Teknik Üniversitesi, Sosyal Bilimler Enstitüsü).

EU (2024). Critical Infrastructure and Cybersecurity. Accessed: December, 20 2024. https://energy.ec.europa.eu/topics/energy-security/critical-infrastructure-and-cybersecurity_en

Govea, J., Gaibor-Naranjo, W. & Villegas-Ch, W. (2024). Securing Critical Infrastructure with Blockchain Technology: An Approach to Cyber-Resilience. *Computers, 13*(5), 122. Accessed: November 30, 2024. https://doi.org/10.3390/computers13050122.

Gündüz, M. Z. & Daş, R. (2020). Akıllı Şebekelerde İletişim Altyapısı ve Siber Güvenlik. *Journal of the Institute of Science and Technology, 10*(2), 970-984. Accessed: December 20, 2024. https://doi.org/10.21597/jist.655990**.**

Hekim, H. & Başıbüyük, O. (2013). Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi, 4* (2), 135-158.

Holloway, M. (2015). Stuxnet Worm Attack on Iranian Nuclear Facilities. *Retrieved: April 13*, 2017, Standford University. Accessed: November, 22 2024. http://large.stanford.edu/courses/2015/ph241/holloway1/.

Jormakka, J. & Mölsä, J. V. E. (2005). Modelling Information Warfare as a Game. *Journal of Information Warfare*, *4*(2), 12–25. https://www.jstor.org/stable/26504060.

Kandır, M.O. (2025). Kritik Altyapılarda Siber Güvenlik. Yayın Tarihi: 06 Nisan 2025. Erişim Tarihi: 10 Nisan 2025. https://www.hukukvebilisimdergisi.com/kritik-altyapilarda-siber-guvenlik/.

Karabacak, B. (2011). Kritik Altyapılara Yönelik Siber Tehditler ve Türkiye İçin Siber Güvenlik Önerileri. *Siber Güvenlik Çalıştayı, Bilgi Güvenliği Derneği, Ankara*, *29*, 1-11.

KAS & EDAM (2022). *Türkiye'de Kritik Altyapı ve Siber Güvenlik. Konrad-Adenauer-Stiftung Türkiye*, 1–32. Erişim Tarihi: 10 Aralık 2024. https://edam.org.tr/wp-content/uploads/2022/08/NATO-Uluslararasi-Guvenlik-ve-Siber-Raporu.docx.pdf -2022.

Kaspersky (2023). Enerjide Var "Türkiye'de En Çok Saldırıya Uğrayan Sektörler"- Yeni Rapor!. https://www.enerjiekonomisi.com/enerjide-var-turkiye-de-en-cok-saldiriya-ugrayan-sektorler-yeni-rapor/26690/

Kaspersky (2023). *Türkiye'de Enerji ve Üretim Sektörlerine Yönelik Siber Saldırılar Arttı*. 15 Mart 2023. Erişim Tarihi: 10 Kasım 2024. https://www.kaspersky.com.tr/about/press-releases/turkiyede-enerji-ve-uretim-sektorlerine-yonelik-siber-saldirilar-artti?utm_source=chatgpt.com.

Kello, L. (2013). The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security* 2013; 38 (2): 7–40. https://doi.org/10.1162/ISEC_a_00138.

Kesan, J. P. Hayes, C. M. & Bashir, M. N. (2016) "A Comprehensive Empirical Study of Data Privacy, Trust, and Consumer Autonomy," *Indiana Law Journal*: Vol. 91: Iss. 2, Article 3. Available at: https://www.repository.law.indiana.edu/ilj/vol91/iss2/3.

Kesler, B. (2011). The Vulnerability of Nuclear Facilities to Cyber Attack; Strategic Insights: Spring 2010. Calhoun: The NPS Institutional Archive. Accessed: December, 20 2024. https://core.ac.uk/download/pdf/36718376.pdf.

Kohlmann, E. F. (2006). The Real Online Terrorist Threat. *Foreign Affairs*, *85*(5), 115–124. https://doi.org/10.2307/20032074.

Kriter Dergi. (2023). Askersiz Savaş Çağı Başladı. Türkiye'nin Siber Kalkanı Güçlendiriliyor. *Kriter Dergi*. Erişim Tarihi: 20 Mart 2025. https://kriterdergi.com/dis-politika/askersiz-savas-cagi-basladi-turkiyenin-siber-kalkani-guclendiriliyor.

Kriter Dergi (2023). Türkiye'de Siber Güvenlik Gelişmeleri. Kriter Dergi, 7(84)

Kurum, M., Bilgiç, A., & Çardak, B. (2022). *Siber Alanda Radikalleşme ve İnternetin Panoptik Gözetimi*. Güvenlik Bilimleri Dergisi, 11(2), 441-470, Accessed: 12.12.2024. https://doi.org/10.28956/gbd.1092120.

Lee, R. M., Assante, M. J., & Conway, T. (2014). German Steel Mill Cyber-Attack. *Industrial Control Systems*, *30*(62), 1-15, *Accessed*: *December 10, 2024*.

Lee, R. M. & Conway, T. (2022). The Five ICS Cybersecurity Critical Controls. *Available from. Accessed: December 10, 2024*.

Lewis, J. (2006). *Cybersecurity and Critical Infrastructure Protection*. Center for Strategic and International Studies, 1-12.

Lewis, T. G. (2019). *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*. John Wiley & Sons.

Libicki, M. C. (2009). Cyber Deterrence and Cyberwar. Published by 2009 *RAND Corporation*. ISBN: 978-0-8330-4734-2.

Lin, H. S. (2010). Offensive Cyber Operations and the Use of Force. *Journal of National Security Law & Policy, Vol.4, No.63. 2010.*

Liu, W. & Song, Z. (2020) Review of Studies on the Resillience of Urban Critical Infrastructure Networks. Reliability Engineering & System Safety, Volume 193, 2020, 106617, ISSN 0951-8320, https://doi.org/10.1016/j.ress.2019.106617**.**

Mueller, R. S. (2010) By Ellen Nakashima, "FBI Dırector Warns of Rapidly Expanding Cyberterrorism Threat". The Washington Post. 4 March 2010. Accessed: November 20, 2024. https://www.washingtonpost.com/wp-dyn/content/article/2010/03/04/AR2010030405066.html.

Nakashima, E. (2010). "FBI Dırector Warns of Rapidly Expanding Cyberterrorism Threat". The Washington Post. 4 March 2010. Accessed: 20.11.2024. https://www.washingtonpost.com/wp-dyn/content/article/2010/03/04/AR2010030405066.html.

NATO (2021). *NATO Siber Güvenlik Politikaları ve Uluslararası İşbirliği. NATO Siber Savunma Raporu,* 12.

NATO (2021). *NATO Cyber Defence Pledge. April 16, 2021.* Accessed: January 29, 2025. https://ccdcoe.org/news/2021/public-side-event-of-the-nato-cyber-defence-pledge-conference-2021-on-16-april/.

NATO (2022). *2022 NATO Strategic Concept*. Accessed: December 20, 2024. 290622-strategic-concept.pdf.

NATO (2024). *Resilience, Civil Preparedness and Article 3.* Accessed: November 29, 2024. https://www.nato.int/cps/bu/natohq/topics_132722.htm#vulnerabilities.

NATO (2024). *Cyber Defence*. July 30, 2024. Accessed December 12, 2024. https://www.nato.int/cps/de/natohq/topics_78170.htm.

NIST (2016). National Institute of Standards and Technology. Elaine Barker William C. Barker. Accessed: 25.11.2024. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

NTV (2016). Elektrik Hatlarına Siber Saldırı Girişimi. Yayın Tarihi: 31.12.2016. https://www.ntv.com.tr/turkiye/elektrik-hatlarina-siber-saldiri-girisimi,-ez-gYJG70Oqr5F-imHELg.

Nye, J. S. (2010). Cyber Power. Belfer Center for Science and International Affairs. Cambridge: Harvard Kennedy School, pp. 1-24. May 2010.

Parks, R. C. & Duggan, D. P. (2011). "Principles of Cyberwarfare," in IEEE Security & Privacy, Vol. 9, No. 5, pp. 30-35, Sept.-Oct. 2011, https://doi: 10.1109/MSP.2011.138.

Polat. D. (2020). *NATO'nun Yeni Operasyon Alanı: Siber Uzay*. Güvenlik Bilimleri Dergisi, Özel Sayı (International Security Congress Special Issue), 135-138. Accessed: December 20, 2024. https://doi.org/10.28956/gbd.695973

Pursiainen, C. (2009). The Challenges for European Critical Infrastructure Protection. *Journal of European Integration*, *31*(6), 721–739, Accessed: December 17, 2024. https://doi.org/10.1080/07036330903199846.

Pursiainen, C. (2021). Russia's Critical Infrastructure Policy: What do we Know About it?. *European Journal for Security Research,* 6(1), 21–38 (2021). https://doi.org/10.1007/s41125-020-00070-0.

Pollitt, M. M (1998). Cyberterrorism Fact or Fancy? Computer Fraud & Security, Volume 1998, Issue 2, 1998, Pages 8-10, ISSN 1361-3723, https://doi.org/10.1016/S1361-3723(00)87009-8.

RAND Corporation (2015). *Cyberterrorism: The Risks and Consequences of Digital Attacks on Critical İnfrastructure. RAND Corporation Report*, 21. Accessed: 15 December 2024. https://www.rand.org/content/dam/rand/pubs/research_reports/RRA2300/RRA2397-2/RAND_RRA2397-2.pdf.

Resmi Gazete (2025). Siber Güvenlik Kanunu. Kanun No: 7545, 12 Mart 2025, Sayı: 32846. https://www.resmigazete.gov.tr/eskiler/2025/03/20250319-1.htm

Rid, T. (2011). Cyber War Will Not Take Place. *Journal of Strategic Studies*, *35*(1), 5–32. https://doi.org/10.1080/01402390.2011.608939.

Rid, T. (2020). *Active Measures: The Secret History of Disinformation and Political Warfare*. Profile Books.

Rid, T. & Buchanan, B. (2014). Attributing Cyber Attacks. *Journal of Strategic Studies*, *38*(1–2), 4–37. https://doi.org/10.1080/01402390.2014.977382.

Robinson, P. (2025). The MOVEit Attack Explained. Erişim Tarihi: February, 16 2025. https://www.lepide.com/blog/the-moveit-attack-explained/

Saltzer, J. H., & Schroeder, M. D. (1975). "The protection of information in computer systems," in *Proceedings of the IEEE*, vol. 63, no. 9, pp. 1278-1308, Sept. 1975, doi: 10.1109/PROC.1975.9939.

Sağıroğlu, Ş. & Alkan, M. (2018). *Siber Güvenlik ve Savunma: Farkındalık ve Caydırıcılık. Ankara: Grafiker Yayınları*, 52–67.

Sağıroğlu, Ş. & Kanca, A. M. (2022). İç Siber Güvenlik Tehdit Bilgisi Paylaşımı. *Siber Güvenlik ve Savunma Kitap Serisi 6: Siber Güvenlik Ontolojisi, Tehditler ve Çözümler*, *6*, 67.

Singer, P. W. & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York, 2014; online edn. http://dx.doi.org/10.1093/wentk/9780199918096.001.0001, Accessed: January 04, 2025.

Zoli, C., Steinberg, L. J., Grabowski, M., & Hermann, M. (2018). Terrorist critical infrastructures, organizational capacity and security risk, Safety Science, Volume 110, Part C, 2018, Pages 121-130, ISSN 0925-7535, https://doi.org/10.1016/j.ssci.2018.05.021.

Şeker, E. (2020). Yapay Zekâ Tekniklerinin/Uygulamalarının Siber Savunmada Kullanımı. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, *6*(2), 108-115.

The Guardian. (2024). Germany Summons Russian Envoy Over 2023 Cyber-attacks. *The Guardian*. https://www.theguardian.com/world/article/may/03/germany-says-russians-behind-intolerable-cyber-attack-last-year.

The Wall Street Journal. (2025). How Chinese Hackers Graduated From Clumsy Corporate Thieves to Military Weapons. *The Wall Street Journal*. https://www.wsj.com/tech/cybersecurity/typhoon-china-hackers-military-weapons-97d4ef95.

Tikk, E. & Kaska, K. (2010). Legal Cooperation to Investigate Cyber Incidents: Estonian Case Study and Lessons. 9th European Conference on Information Warfare and Security, Thessaloniki, Greece, 01-02 July. Reading: Academic Publishing Limited, pp 288-294.

Tikk, E. & Kerttunen, M. (Eds.). (2020). *Routledge handbook of international cybersecurity*. The Cyber Dimension of Geopolitical Competition: Strategic Challanges in Cyperspace, London: Routledge.

Tüzün, F. (2022). *Siber Savaşın Yeni Cephesi: Kritik Altyapılar- İstihbarat ve Güvenlik Araştırmaları Merkezi*. Accessed December 28, 2024.https://igam.org.tr/siber-savasin-yeni-cephesi-kritik-altyapilar/.

UAB (2024). Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2024-2028. https://www.uab.gov.tr/uploads/pages/siber-guvenligin-yol-haritasi-yerli-ve-milli-tekno/ulusal-siber-guvenlik-stratejisi-2024-2028.pdf.

Weiss, M. & Biermann, F. (2021). Cyberspace and the Protection of Critical National Infrastructure. *Journal of Economic Policy Reform*, *26*(3), 250–267. Accessed: December 30, 2024. https://doi.org/10.1080/17487870.2021.1905530.

Yeşilyurt, H. (2015). Finansal Hizmet Sektöründe Siber Güvenlik Riskleri ve Çözüm Yolları: Ödeme Sistemleri ve Tedarik Zinciri Bütünlüğü. *Celal Bayar University Journal of Social Sciences/ Celal Bayar Üniversitesi Sosyal Bilimler Dergisi.* Cilt: 13, Sayı: 2, 97-120. Haziran 2015. Doi Number: 10.18026/cbusos.40441.

Yılmaz, S. & Sağıroğlu, Ş. (2013). Siber Saldırı Hedefleri ve Türkiye'de Siber Güvenlik Stratejisi. 6. *Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı. Ankara: ISC*, 323-331.