ARTICLE

# National Security 2.0: The Cyber Security of Critical Infrastructure

A. Burak DARICILI * & Soner ÇELİK **

## Abstract

*Thanks to technological advancements in recent years, critical infrastructure has become both irreplaceable for modern social life—and highly vulnerable. Safe, effective and efficient management of critical infrastructure is a sign of a state's social welfare and economic development. Ensuring the security of critical infrastructure is essential for national security, and is becoming ever more dependent on network technology. Indeed, providing for the cybersecurity of critical infrastructure, i.e., protecting it from cyber attack, is the chief goal of modern states' cybersecurity strategy. The present study aims to reveal the importance of ensuring the cybersecurity of critical infrastructure within the scope of national security. First, the relationship between the concept of national security and cyber threats is scrutinized from a realist perspective. The interaction of the critical infrastructure concept and cybersecurity is then analyzed from a theoretical and technical point of view. In addition to official documents published by the United States, which has the world's most advanced cybersecurity infrastructure, the study includes definitions of related concepts published by Turkey, a country that has made significant progress in recent years in terms of the cybersecurity of its critical infrastructure.*

## Keywords

Critical infrastructure, cybersecurity, cyber attack, national security, realism.

* Associate Professor, Bursa Technical University, Department of International Relations, Bursa, Turkey. E-mail: ali.daricili@btu.edu.tr. ORCID: 0000-0002-3499-1645.

** PhD, Süleyman Demirel University, Department of International Relations, Isparta, Turkey, E-mail: sonercelik85@gmail.com. ORCID: 0000-0001-7554-5628.

Received on: 08.06.2021
Accepted on: 18.10.2021

## Introduction

Critical infrastructure refers to the physical and virtual systems that underlie modern societies, and are vital for their survival. Providing for the security of these systems is an essential part of the national security strategies of modern states. The safe and effective management of critical infrastructure is an indicator of a state's social welfare and economic development. Today, the security of critical infrastructure is heavily dependent on network technologies; accordingly, providing for the cybersecurity of a state's critical infrastructure is synonymous with national security. Protecting critical infrastructure against cyber attacks is thus crucial for maintaining daily life, as it ensures the provision of essential public services and reliable commercial and financial transactions.[1]

The process of managing critical infrastructure by means of network technologies, which are mainly operated by mechanical systems under human supervision, has accelerated since 1990, with the rapid commercialization and demilitarization of the internet under the leadership of the U.S. As a result, in the same period, cybersecurity strategies began to be developed at the national and international level. Many countries in the international system now have cyber defense and attack capacities commensurate with their developmental level and economic potential. Since the 2000s, states have endeavored to improve their cyber-attack capacities in various ways, e.g., through space espionage and counter espionage, the spread of disinformation using web-based platforms, the development of electronic warfare skills, perception management and the dissemination of propaganda. In addition to states, many international organizations and companies have developed cybersecurity plans within their fields of activity in tandem with their goals.

The importance of critical infrastructure was first emphasized in U.S. Presidential Policy Directive 63 (PPD-63), accepted by President Bill Clinton in 1998. Since that time, many countries, notably the U.S., have addressed the security of critical infrastructure in their codes, official plans and strategy papers.[2] Many measures, evaluations and recommendations with titles related to the cybersecurity of critical infrastructure have been and continue to be circulated in the realm of legal regulations, and in states' plans and strategy documents, as a result of the ongoing emergence, proliferation and diversification of cyberspace-based threats.

There have been many concrete instances of cyber attacks targeting states' critical infrastructure. Many of these occurred in the 2000s, before awareness had developed as to the nature of this kind of threat. To provide an example, at the end of the Cold War, the tension between Russia and Estonia that had begun

**There have been many concrete instances of cyber attacks targeting states' critical infrastructure. Many of these occurred in the 2000s, before awareness had developed as to the nature of this kind of threat.**

in response to Estonia's rapprochement with the North Atlantic Treaty Organization (NATO) alliance became heightened due to Estonia's decision to remove a Soviet-era statue from Tallinn Square. Immediately after this decision, a large-scale Distributed Denial of Service (DDoS) attack was launched against Estonia's critical infrastructure. The cyber attacks aimed to collapse the country's internet infrastructure by targeting the websites of Estonia's political parties, its state institutions, parliament, media organizations, banking and financial systems. The internet sector of Estonia's critical infrastructure became unserviceable for a week as a result of the attacks. Estonia recovered with the help of NATO, and the decision to close access to Estonia's national web from abroad.[3]

In another instance, a cyber attack involving the Stuxnet Virus was launched against Iran's nuclear installation in Natanz in June 2010; the installation was physically damaged and the development of its nuclear energy capacity was delayed as a result. Although Iran blamed the U.S. and Israel as the backers of the attack, no one has claimed responsibility to date.[4]

Other examples of cyber attacks targeting critical infrastructure were observed during Russia's intervention in Ukraine, which began in 2014. The use of mobile phones in Crimea in the first days of close combat in March 2014 was prevented by destroying the infrastructure of Ukrtelecom, Ukraine's official mobile phone company. Another cyber attack was carried out against a power plant in the Prykarpattyaoblenergo Region of Ukraine on December 23, 2015, causing a power outage there. According to Ukraine's allegations, these cyber attacks were conducted by Russian intelligence services and affiliated hacker groups.[5]

Another example of cyber attacks targeting a state took place in Turkey. On November 24, 2015, Turkish F-16s shot down a Russian Su-24 fighter jet for violating Turkish airspace—an incident that created significant political tension between Turkey and Russia. The tension increased in December 2015 when "DDoS" cyber attacks aimed to erode Turkey's critical infrastructure, including its banking and finance systems, public institutions and e-state, by targeting the bandwidth used by the system where ".tr" extension names are kept. The attacks had the potential to affect 400,000 websites in Turkey. Russia is alleged to have been behind those attacks, but has not recognized such claims.[6]

As these concrete cases indicate, organized cyber attacks can target the virtual/technological systems used in managing critical infrastructure. National intelligence services and/or various hacker groups may be associated with these attacks, which can be almost impossible to trace. And there are many more such examples. The remarkable point here is that today, states can organize cyber attacks against rival or adversary states by targeting critical infrastructure, rather than purely military targets. Indeed, critical infrastructure is now seen *as* a military target against which a state can organize cyber attacks. This situation is a development arising from the use of systems based on network technologies with cyber space-based technological developments to manage critical infrastructure.

It is a logical development within this context that states have begun to provide for the security of critical infrastructure as a crucial component of their national security strategies. States aim to protect their critical infrastructure by means of various plans, institutional structuring, legal regulations and strategy papers. And in addition to providing cybersecurity for their own critical infrastructure, several states have developed the capacity to carry out cyber attacks that can damage the critical infrastructure of adversary states as an important target.

Relations between the concept of national security and cyber threats will be discussed in this context from a Realist perspective in this study. Subsequently, the interaction of the critical infrastructure concept and cybersecurity will be analyzed from a technical and theoretical perspective, drawing upon definitions of these and related concepts found in official documents published by the U.S. and Turkey.

## National Security and Cyber Threats in terms of the Realist Paradigm

Although the national security concept emerged as the result of the political conditions of the 20th century, the intellectual foundations of this concept date back much farther, specifically to the era of the establishment of modern nation-states. The national security concept was first recorded in U.S.-based official documents and academic studies after WWII; U.S. national security in the period after 1950 focused on coordinating between government agencies to address the nation's threats and interests. The national security concept, as a key component of ensuring the collective security of NATO member states during the Cold War years, was fundamentally defined within the context of the struggle against Communism.[7] In studies conducted during this period, national security was defined mainly from a historical, military perspective.

Over time, it developed into a reference that countries use to determine their domestic and foreign policies. The national security concept, in its current form, includes both domestic and foreign policy elements.

**In the post-Cold War era, the national security concept was redefined in the literature in light of the disintegration of the bipolar political system and ideological point of view, along with the emergence of new-generation threats, and the desire to promote liberal values and develop free trade.**

In the post-Cold War era, the national security concept was redefined in the literature in light of the disintegration of the bipolar political system and ideological point of view, along with the emergence of new-generation threats, and the desire to promote liberal values and develop free trade. Because the national security concept developed in different states with different perspectives, it became more controversial in the post-Cold War era. Across decades, many different schools analyzed whether security is/should be individual, national or international. The modern approach tends to be critical of any security mentality that discusses national security solely from a military perspective, and a more human-centered national security mentality has come into prominence.[8] The national security concept, after moving away from its military debut, has been discussed from points of emphasis such as economic security, health safety, individual safety, food security, societal security, environmental safety and cyber safety. This new theoretical point of view has vastly extended the scope of the security concept. To provide an example, Buzan highlights the need to analyze the political, economic, social, environmental and military dimensions of security.[9]

The intellectual foundations of Realist national security policies were built on the premise that people act with motives such as interest, greed and power, contrary to Idealist approaches. Realists argue, in contrast to what the Idealists claim, that it is almost impossible to change human nature at the point of ensuring security. Instead of changing human nature, then, it should be accepted that humans are human, and the negative sides of human nature should be acknowledged and addressed by politics. Only then, we can talk about ensuring security of the people.[10]

Intellectuals such as Thomas Hobbes, Niccolò Machiavelli and Jean-Jacques Rousseau had a pessimistic perspective that can be applied to the ways in which national security needs to be understood. Those intellectuals accepted the international system as an area where states continuously fight with each other to pursue their own selfish interests. For this reason, it is impossible

to establish universal peace, as the Idealists desire. This line of reasoning is accepted by Realists such as Carr and Hans Morgenthau; in their view, the only way to prevent a state from becoming a hegemon in the international system, where there is a constant conflict of interests among states, is for states to balance each other's power.[11] The pessimistic viewpoint of classical Realists is accepted by neo-realists such as Kenneth Waltz and John Mearsheimer, according to whom security or insecurity is a result of the anarchic nature of the international system on a large scale. Therefore, international policy will continuously sustain a tendency to violence.[12]

The Realist political approach accepts states as the main actors of the international system; since the interests of each country differ from each other, there is always the possibility of war, and some kind of conflict or fighting is inevitable. The Realist approach defines the international system as anarchic, and characterizes international policy as a power struggle in which security is the main agenda item in the realm of international relations. In this respect, the security concept for Realist theoreticians is discussed through "insecurity" in general terms, and this theoretic approach is explained via themes of power, threat and insecurity.

Cyberspace-based developments, today, propose new approaches to states' threat, security and deterrence agendas. Some states have even begun to see cyber attack and cyber conflict as important methods of engaging in strategic defense and inflicting damage on their opponents. Developments in cyberspace bring along new security risks; the importance of removing these risks has thus also increased, compelling states to develop strategies to address this issue. For Realist theorists, this makes the international system even more uncertain and anarchic than before, especially given that cyber attacks can be caused not merely by states but by individuals.[13]

In Realist terms, the diversification of risks to cyberspace resources, and the inability to determine the source of these risks, deepens the anarchic structure of the international system. A cyberspace attacker can hide his or her identity by using various forms of crypto software and programs. The attacker can even conduct a "false flag"[14] operation, making it appear that the source of the cyber attack is another state or a state-sponsored hacker group by using similar software. All of these circumstances deepen the insecurity of the international system and reinforce the mutual distrust between states.

Power struggle and competition in the international system have expanded into a new dimension thanks to internet-based developments. Many states have used these technologies as an opportunity to develop their hard power. Improving military power with the help of cyber-based technology and skill has become an important goal for these states. Allocating budgets, making

investments, training experts and establishing cyber military commands in tandem with conventional army development are now essential for states in order to reach a powerful attack and defense capacity in cyberspace.[15]

All of these developments contribute to what Realists call the "security dilemma," a phenomenon whereby "many of the instruments that are used by a state to increase its security decrease the security of others."[16] And it is ongoing. When one state makes a military investment or takes a military measure, this is taken as a threat by another state, which then applies similar measures, which in turn are interpreted by other states as a threat. The threat perceptions of states vis-à-vis one another escalate, in some cases leading to an armament race with mutual measures taken back and forth.[17]

Based on the security dilemma concept, states evaluate international relations as a zero-sum game, and plan their behavior patterns in the international system based on the assumption of relative earnings. They also avoid cooperation by asking the question, "who will benefit more?" instead of, "how can we both profit?" As indicated above, the Realist approach adopts a competitive and confrontational security perspective on the axis of anarchy. Given the rigidity of this perspective, the limitations and difficulties of cooperation in the Realist paradigm come into prominence. Because the structure of the international system is anarchic, according to this approach, this insecure environment prevents states from cooperating in the long term,[18] a situation exacerbated by the anonymous structure of cyberspace and its accompanying uncertainties, which diversify and deepen risks.

Concerning all these evaluations, the mentality that has started to gain credence recently is that critical infrastructure is an inseparable part of a state's cybersecurity and thus its cybersecurity strategies. This perspective is clearly emphasized in the national cybersecurity documents of many states. For example, Turkey's National Cyber Security Strategy (2020–2023) Document states, "*Cybersecurity is an inseparable part of national security. Providing national security in an absolute manner depends on achieving [our] goals in the cybersecurity field*."[19] As mentioned above, the security of critical infrastructure and information systems that are mostly managed by internet technologies has become vital to the security of any state. States, now, are aware that cyber attacks targeting critical structures can be a serious threat, and that such attacks can negatively affect their political, economic and military security.

## The Relationship between Critical Infrastructure and Cyber Security

Critical infrastructure has two dimensions in terms of cybersecurity: defense and attack. Let us look first at the cyber defense and security dimension. Rapid development in network technologies has led to decisions to manage the critical infrastructure vital to a state's national security and public functioning by means of operating systems that rely heavily on internet technologies. Therefore, states that are in a power struggle within the international system may inflict damage on sectors of each other's critical infrastructure, accepting them as military targets. It is now a necessity for a state to protect its critical infrastructure against cyber attacks by investing in the defense capacity of these systems and endeavoring to provide security for them.

The other dimension is cyber attack capacity. A state may wish to completely or partly damage the critical infrastructure of an adversary state by seeking opportunities and improving skills in this capacity and organizing covert operations. A state may prefer this mode of attack due to the anonymous structure of cyberspace; it is almost impossible to prove allegations or to find concrete evidence of a cyberspace attack in terms of international law.

As noted above, a state's critical infrastructure might be exposed to various civil and military threats in terms of both its cyber defense and cyber attack capacity. Since critical infrastructure sectors are now evaluated within the scope of strategic systems that need to be protected at the national level, they are accepted as sensitive targets. To provide an example, Turkey's National Cyber Security Strategy (2020–2023) goals include "implementing regulations for the protection of critical infrastructure sectors; developing cyber risk management and emergency plans; ensuring that internet traffic, whose source and target is domestic, remains in the country; and discussing cybersecurity within the scope of national security."[20] Even collective security organizations, such as NATO and the European Union (EU), take measures to protect critical infrastructure against cyber risks and attacks.

**Critical infrastructure is defined differently in various approaches; the common trait of all the approaches identify it as consisting of vital systems in terms of the functioning of the state.**

Critical infrastructure is defined differently in various approaches; the common trait of all the approaches identify it as consisting of vital systems in terms of the functioning of the state. Regarding cybersecurity, each critical infrastructure system that is managed by internet technologies is a potential target of cyber attack. Critical infrastructure is defined in

Turkey's National Cyber Security Strategy and 2013–2014 Action Plan as "Infrastructures with information systems that may cause loss of life, large-scale economic damage, national security gaps or disruption of public order when the confidentiality, integrity or accessibility of the information it processes is impaired."[21] Turkey's 2016–2019 National Cyber Security Strategy specified the sectors that comprise critical infrastructure as follows: "electronic communications, energy, water management, critical public services, transportation, banking and finance sectors."[22]

Critical infrastructure as defined in terms of U.S. legislation are sectors that would result in a weakening of the country's national defense and economic security if they were to fail or collapse. An official document prepared for the U.S. in 1997 identifies these sectors as (1) telecommunication; (2) electrical power supplies and gas and oil storage and production units; (3) banking and financial institutions; (4) transport units and components; (5) units from which water is supplied; (6) emergency service units including emergency medical response units, general law enforcement, fire and search and rescue units; (7) government services and institutions.[23]

The U.S. Patriot Act, which entered into force in 2001, defines critical infrastructure as "*Vitally important physical or virtual systems and assets that can create a detrimental effect on security, national economic security, national public health, or any combination of these in case of being inadequate or destroyed.*"[24] The U.S. Presidential Policy Directive—Critical Infrastructure Security and Resilience, accepted in 2013, specifies the sectors of critical infrastructure as "chemistry, commercial activities, communication, critical production, dams, the defense industry, emergency services, energy, finance, food and agriculture, public institutions, health, information technologies, nuclear reactors, materials and waste, transportation systems, water and wastewater."[25]

The U.S. defines its current critical infrastructure sectors as "*chemical industry, trading areas, communication, critical production facilities, dams, defense industry and production areas, financial services, emergency services, energy, food and agriculture, public health and maintenance, information technologies, nuclear reactor materials and waste, public buildings and areas, transportation systems, water and wastewater systems.*"[26]

Almost all of these critical infrastructure sectors—notably energy, telecommunications, transportation and water systems—are currently managed by utilizing internet technology infrastructure. These systems can be perceived as military targets when we consider that they are strategically important for a country. It is now possible to damage the critical infrastructure of an adversary state, causing chaos or turning its economy upside-down via cyber attacks.[27]

It is possible, in cyberspace, in which all these systems are interconnected, to collapse a state's critical infrastructure, i.e., to make a system based on mutual dependence unworkable, and thus start a cyber conflict. The general run of cyber attacks toward operational targets in cyberspace starts by perforating critical infrastructure systems that are managed by internet technologies,[28] as is evident in the cyber attacks against Estonia, Iran, Turkey and Ukraine.

Considering the risks above, protecting critical infrastructure and establishing cybersecurity entails the following considerations:[29]

- Providing security against physical and cyber threats that could destroy the operation of critical infrastructure.
- Being prepared for the environmental, social, economic and political effects that could emerge in the event of the disruption or failure of critical infrastructure arising from the system itself or from natural disasters; establishing coordination and work safety plans and action steps for this purpose.
- Evaluating the law enforcement personnel, fire stations, search and rescue and medical units that are involved in ensuring the security and functionality of critical infrastructure. Precautions should be taken to ensure continuance of function, and to maintain the mobility and preparedness of units that can intervene in the event of a critical infrastructure emergency.

## Cyber Security of Critical Infrastructure

Conducting quality checks on the precautions that are taken to ensure the cyber and physical security of critical infrastructure is important, as is keeping the effectiveness of these measures up to date. Private companies and/or public enterprises apply penetration tests to specify the required measures. These tests model and simulate possible attacks against the system.

**The effect of a "third eye," i.e., having an independent contractor company assess the safety measures, is essential in providing the security of critical infrastructure.**

The effect of a "third eye," i.e., having an independent contractor company assess the safety measures, is essential in providing the security of critical infrastructure. The scope and currency of these measures is even more critical when it is considered that hackers' attack methods change day by day.

It is worth going into greater detail in regard to information systems, as these may require addition measures of protection. Information systems can be divided into two categories: data systems and communication systems. Some

critical infrastructure sectors use publicly available information systems for service, while other aspects of their functioning are managed by private information systems called Industrial Control Systems (ICS). ICSs are used in critical infrastructure sectors such as electricity transmission/generation and distribution businesses, power and nuclear power plants, chemical factories, refineries, water and treatment plants and larger industrial complexes. Providing cybersecurity to industrial companies, rather than physical security alone, has grown in importance because of the digitalization trend and increasing demand for productivity. ICSs themselves are divided into two groups based on their topology and components; Supervisory Control and Data Acquisition (SCADA) systems and Distributed Control Systems (DCS).

Critical infrastructure information systems fall into four categories:

- Information Systems: Computer systems serving an institution and its stakeholders.
- Communication Systems: Systems that provide communication services to many institutions and organizations, consisting of components geographically spread over a very wide area.
- SCADA Systems: Systems that are used to centrally monitor and control the components of a geographically dispersed system.
- Distributed Control Systems (DCS); Systems with control components spread throughout the plant to monitor and control an industrial process limited to a specific facility and location. [30]

SCADA systems have been used for many years in the management and tracking of critical infrastructure installations such as dams, steam power plants and energy distribution units. SCADA systems had no connection with other networks in the 1970s and 1980s. There were no known information and communication technologies in SCADAs in those years—only technologies developed specifically for infrastructure. In the decades that followed, SCADA systems began to include standard software, hardware, operating systems and network protocols that are widely known and used today. Currently, many SCADA systems that manage and monitor critical infrastructure systems are associated with enterprise networks and the internet. SCADA systems have thus become open to cyber attacks, and the security of those systems is seriously questioned.

Industrial infrastructure information systems generally consist of a large number of different processes that are interrelated with and mutually reliant upon each other. This is because they are topologies that include multitier rather than flat network architecture; each layer is in communication with different layers associated with it, and each layer may vary in terms of mechanisms

because of different security criteria. Therefore, a defense-in-depth mentality should be applied for multilayered topologies such as ICS. This mentality was developed based on the idea that all measures taken against cyber attacks will somehow be circumvented.

The defense-in-depth approach aims to minimize the success rate of a potential attacker by taking measures based on the requirements of each layer and its assets at the same time. The use of modern technologies in industrial infrastructure makes these systems more skillful, while the same technologies increase the potential for cyber threats by proliferating the possible attack surfaces of the systems. The "Purdue Model" layered network architecture was developed by Purdue University, Indiana, and was adapted to ICSs by the International Society of Automation (ISA)[31] both to keep the attack surfaces to a minimum and to make the management of control systems for each layer safer. There are private network security architectures for different ICS and SCADA systems, and various, modified versions of the Purdue model. The Purdue Model consists of 5 or 6 layers, depending on the reference source and notation. These layers are the Enterprise Demilitarized Zone (DMZ), Local Corporate Network, Supervisory, Control DMZ, Logical, Field and Instruments. Four main problems may be encountered in the field for each layer:

- Access Control
- Log Management
- Network Security
- Remote Access

Purdue Model layered architecture is based on the principle of separating Information Technology (IT) and Operational Technology (OT) networks into subnets. The goal is to provide controlled access (through INTER-VLAN routing or by establishing an Access Control List (ACL) or by creating isolated networks using other technologies) to subnets and restrict unnecessary access that could become a threat.[32]

With such systems, there is a need to continuously monitor and work to correct technical imperfections and deliver the required solutions. Implementing necessary precautions in a faultless manner is crucial for the security of critical infrastructure within the ongoing digitalization processes of modern life. Taking precautions that provide for the security of critical infrastructure must be seen as essential steps to be taken from the moment an organization is established, as cybersecurity precautions and applications are not components that can be added to systems later. Protecting critical infrastructure by means of software that is specially designed for SCADA systems is all-important to keeping crucial services functioning. Research and development (R&D) ac-

tivities regarding the security of critical infrastructure must be supported in order to develop national software to prevent cyber attacks from adversary states and non-state actors. Conducting and financing R&D activities to ensure cybersecurity should be basic government policy. As a result of R&D activities, cybersecurity guidelines that can be used jointly by various sectors, and that contain consistent information should be prepared for critical infrastructure; standards should be established and good practices should be specified.

Moreover, the critical infrastructure sector itself needs to be expanded, as systems based on internet technologies have become more common in recent years, and have expanded to almost all areas of life. In this regard, the critical infrastructure sectors that need to be protected for a country with a developed internet infrastructure should include all systems pertaining to the defense industry, including "all communication systems, information systems and logistics systems; air defense and command control systems; cryptosystems; navigation, approach, landing, positioning and direction-finding systems; satellite and ground systems; space systems; manned and unmanned aerial vehicle systems,"[33] as well as critical systems pertaining to the functioning of society, such as:

banks, shopping malls, education and training campuses, public buildings and enterprises, hospitals, factories, refineries, oil pipelines, natural gas lines, drinking water pipelines, treatment facilities, fixed facilities installed on pipelines, liquefied natural gas facilities and warehouses, oil wells, large pump stations, weapon and military equipment factories and facilities, railways, highways, important bridges and crossings, large ports, marinas, airfields, navigation auxiliary stations, radar stations, national monitoring, information processing system centers, radio, radio link centers, dams, power plants, transformer centers, strategic mine treatment, and operation factories.[34]

Inflicting economic damage, tarnishing the reputation of the target state by making it appear weak, creating panic and fear in society and establishing an unsafe environment are the reasons such facilities may be selected as targets by a government or government-sponsored hacker group. Critical infrastructure facilities should not only be thought of as cyber attack targets, but as the priority targets of a conventional war that could be selected to affect the will and tenacity of the adversary state—or destroy it.

Cyber threats of the asymmetric type are

**Cyber threats of the asymmetric type are on the rise; 79,790 information security violation incidents and 2,122 data leaks were reported by 70 organizations from 61 countries.**

on the rise; 79,790 information security violation incidents and 2,122 data leaks were reported by 70 organizations from 61 countries. Two-thirds of cyber attacks were concentrated on the critical infrastructure of G-7 member states, especially the U.S. The sectors most affected by the cyber attacks were public institutions, and private or public companies engaged in technology and financial activities. [35]

Cyber threat sources may be grouped into three categories: external attackers, in-house attackers and business partners. External attackers play a role in 80% of violations, and in 60% of such attacks, the attackers seize the target systems within minutes. However, determining 75% of the attacks within a few days is impossible.[36] And the scope of cyber attack risk is much greater when we consider that the statistical information given above includes only data that can be detected and reported.

Cyber attacks on critical infrastructure can cause vitally destructive/disruptive results. Those results directly affect end users, and threaten the strategic targets and national security of the countries in which they occur. It is thus essential to reduce the number of attacks on critical infrastructure and to implement and sustain effective protection methods. Moreover, it is now essential for states to create an integrated security strategy to protect critical infrastructure and to determine both cybersecurity and physical security measures, along with their requisite audit needs and methodologies.

States should adopt a comprehensive, integrated approach, in which risks and threats are evaluated from all angles and the roles of all relevant actors are defined for the periods before, during and after an attack. Such an approach should include international actors and all public and private sector stakeholders. Thinking like a hacker or a terrorist, the weakest and most sensitive points ought to be identified, the worst scenarios should be anticipated and prepared for, and the requisite practices to prevent and respond to these scenarios should be determined.

After establishing a structure that can organize all these elements, a model system is required. It must be decided who will react when and in what way, in the event of an attack. It is of great importance to consider and address these issues in detail. Priorities within this context include the determination of the steps necessary for prevention, protection and recovery.

## Conclusion

The first hacking events were performed for personal interest in the 1990s; today, the activities of government-sponsored or individual hackers have spawned a new generation of threats on a global scale. It has become very im-

portant to provide for the physical and cybersecurity of critical infrastructure sectors that render essential services for living and working within the scope of evolving security paradigms. Cyberspace is now understood as a new field of struggle on the state level.

International security approaches will continue to evolve as new technological advancements emerge. Cyber security-centered developments will play a significant role within this process. Investments in cyber defense and attack capacities will increase in the ongoing competition and power struggle within the international system, which will in turn affect states' mutual threat perceptions. Generating cybersecurity strategies and practicing them will continue to increase in importance as states develop their cyber security-oriented political approaches.

**Attacks by governments, government-sponsored hacker groups and independent hackers on digital systems are becoming more complex and sophisticated day by day.**

Attacks by governments, government-sponsored hacker groups and independent hackers on digital systems are becoming more complex and sophisticated day by day. Hackers who infiltrate and damage critical infrastructure by benefiting from system gaps have started to act like cyber warriors, receiving state support for their efforts. The scope of the threats they pose has expanded, as modern societies are much more dependent than ever before on complex and widely used internet-based technologies.

States and international organizations today focus on precautions against cyber attacks much more intensely than in the past. As a matter of course, it is hard for critical infrastructure sectors to always be prepared for asymmetric cyber attack threats. It goes without saying that there is a need for close cooperation between the government and private companies to effectively guarantee the cybersecurity of the critical infrastructure systems of the public and private sectors.

The confidentiality of the measures a state develops to ensure the cybersecurity of its critical infrastructure can be accepted as the fundamental principle. However, there is also a need for international cybersecurity alliance and cooperation based on the principle of mutual dependence when the universality of cyberspace is considered. Thus, the cybersecurity of shared, critical infrastructure is not only a national issue—it requires international cooperation.

Most cyberspace threats consist of more than one variable; the multidimensionality of the new generation of threats arising due to technological develop-

ments obliges a new and wide range of approaches in countries' national security strategies. Providing for the cybersecurity of critical infrastructure sectors that are now seen as military targets is crucial for governments to survive. Especially in the last 20 years, critical infrastructure has relied more heavily on processes dependent on network technologies; this circumstance has made the provision of cybersecurity for critical infrastructure a very important goal of states' national security strategies. Developing cyber defense and attack capacity in determining states' national defense strategies is now more necessary than ever.

Many states prepare strategies, make plans, establish special institutional structures and reform their armed forces to improve their cyber defense and attack capacity regardless of their economic size, military capacity or level of technological development. The main reason for following cyberspace-based developments so closely and trying to get involved in these processes is the power struggle and military competition among states within the scope of the Realist paradigm. States, and even collective security organizations such as NATO, have accelerated their plans to develop an effective cyber attack and defense capacity by utilizing network technology-oriented developments.

This study researched why providing security for critical infrastructure is vital for ensuring national security. We revealed that the security of critical infrastructure has become increasingly dependent on network technologies. In light of the above analysis and evaluations, the conclusion is that providing the cybersecurity of a state's critical infrastructures is of vital importance in ensuring its national security, as states have begun to accept each other's critical infrastructure as a military target within the scope of their power struggle in the international system. Thus, states are now increasing their investments in cyber defense and attack capacities. It is clear that ensuring the cybersecurity of critical infrastructure will continue to increase in importance in terms of state security as network technology-centered developments continue to evolve.

# Endnotes

1 Tarık Ak, "İç Güvenlik Yönetimi Açısından Kritik Altyapıların Korunması," *ASSAM Journal*, Vol. 7, Special Issue (2019), pp. 42–45.
2 "Presidential Decision Directive / NSC-63," *Federation of American Scientists*, 1998, https://fas.org/irp/offdocs/pdd/pdd-63.htm.
3 Ali Burak Darıcılı, "Rusya Federasyonu Kaynaklı Olduğu İddia Edilen Siber Saldırıların Analizi," *Uludağ Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, Vol. 7, No 2 (May 2014), pp. 5–7.
4 Ali Burak Darıcılı, *Siber Uzay ve Siber Güvenlik: ABD ve Rusya Federasyonu'nun Siber Güvenlik Stratejilerinin Karşılaştırmalı Analizi*, Bursa: Dora, 2017, pp. 104–105.
5 Ibid, pp. 222–223.
6 Ibid, pp. 225–228.
7 Fikret Birdişli, "Ulusal Güvenlik Kavramının Tarihsel ve Düşünsel Temelleri," *Sosyal Bilimler Enstitüsü Dergisi*, No. 31 (2011/2), p. 150.
8 Ibid, p. 152.
9 Barry Buzan, *People, States and Fear: The National Security Problem in International Relations*, Chapel Hill: University of North Carolina Press, 1983, pp. 214–242.
10 Laurie M. Johnson, *Political Thought: A Guide to the Classics*, Belmont: Wadsworth/Thomson Learning, 2002, p. 49.
11 John Baylis, "Security Concept in International Relations," *International Relations*, Vol. 5, No. 18 (Summer 2008), p. 71.
12 Ibid, p. 72.
13 Darıcılı, *Siber Uzay ve Siber Güvenlik*, pp. 40–41.
14 A false flag operation is an act committed with the intent of disguising the actual source of responsibility and pinning blame on a second party. The term "false flag" originated in the 16th century as a purely figurative expression meaning "a deliberate misrepresentation of someone's affiliation or motives." It was later used to describe a ruse in naval warfare whereby a vessel flew the flag of a neutral or enemy country in order to hide its true identity. The term today extends to include countries that organize attacks on themselves and make the attacks appear to be perpetrated by enemy nations or terrorists, thus giving the nation that was supposedly attacked a pretext for domestic repression and foreign military aggression.
15 Anthony Craig & Brandon Valeriano, "Realism and Cyber Conflict: Security in the Digital Age," *E-IR*, February 3, 2018, https://www.e-ir.info/2018/02/03/realism-and-cyber-conflict-security-in-the-digital-age/.
16 Robert Jervis, "Cooperation under the Security Dilemma," *World Politics*, Vol. 30, No. 2 (1978), p. 168.
17 Charles L. Glaser, "When are Arms Races Dangerous? Rational versus Suboptimal Arming," *International Security*, Vol. 28, No. 4 (2004), p. 44.
18 Kenneth Waltz & George H. Quester, *Uluslararası İlişkiler Kuramı ve Dünya Siyasal Sistemi*, Ankara: A.Ü. Siyasal Bilgiler Fakültesi, 1982, pp. 44–47.
19 *Ulusal Siber Güvenlik Stratejisi ve Eylem Planı* 2020–2023, Ankara: T.C. Ulaştırma ve Altyapı Bakanlığı, 2020, p. 22.
20 Ibid, p. 10.
21 "Ulusal Siber Güvenlik Stratejisi ve 2013–2014 Eylem Planı," *Haberleşme Genel Müdürlüğü*, https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/some-2013-2014-eylemplani.pdf, p. 9.
22 *Ulusal Siber Güvenik Stratejisi 2016-2019*, Ankara: T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, 2016, p. 8.
23 "The Report of the President's Commission on Critical Infrastructure Protection," *Federation of American Scientists*, October 1998, https://fas.org/sgp/library/pccip.pdf.
24 "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act," *US Congress*, 2001, https://www.congress.gov/bill/107th-congress/house-bill/3162
25 "Presidential Decision Directive / PPD 21, 2003," *Obama White House*, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

26 "Critical Infrastructure Sectors of the USA," *CISA*, 2021, https://www.cisa.gov/critical-infrastructure-sectors.
27 Seda Yılmaz & Şeref Sağıroğlu, "Siber Saldırı Hedefleri ve Türkiye'de Siber Güvenlik Stratejisi," *6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı*, Ankara, 2013, pp. 323–326.
28 Kris Hemme, "Critical Infrastructure Protection: Maintenance is National Security," *Journal of Strategic Security*, Vol. 5, No. 8 (2015), p. 25.
29 "Critical Foundations Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection," *Federation of American Scientists*, 1997, p. B-1, https://sgp.fas.org/library/pccip.pdf.
30 "TÜBİTAK Kritik Bilgi Sistem Altyapıları için Asgari Güvenlik Önlemleri Dokümanı," *Haberleşme Genel Müdürlüğü*, https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/kritik-bilgi-sistem-altyapilari-i-c-in-asgari-gu-venlik-o-nlemleri-6445b90e-b2ad-4e5e-9c13-6ae19ba10e37.pdf.
31 The ISA is an institution that makes improvements in areas such as engineering and technology, and also sets standards for industrial automation and control systems.
32 See http://www.pera.net.
33 Hülya Kınık & Vahit Güntay, "Siber Güvenlik Temelinde Kritik Altyapılar ve Hazar Havzası," *Journal of International Social Research*, Vol. 9, No. 47 (December 2016), p. 254.
34 Ibid.
35 "Data Breach Investigations Report," *Idaho Cybersecurity Awareness*, 2015, https://cybersecurity.idaho.gov/wp-content/uploads/sites/87/2019/04/data-breach-investigation-report_2015.pdf.
36 Ibid.