Critical Infrastructure and Cyber Security in Türkiye

Uğur Özker

Table of Content

EXECUTIVE SUMMARY

A strong cyber defense is a critical capability in today's world, where public safety on the one hand and critical infrastructure on the other are undergoing a full digital transformation. Cyber-attack methods are one of the largest and fastest growing categories of crime in the world due to the low cost of their implementation. Moreover, the magnitude of the damage they can cause when applied on critical infrastructures is another reason that makes cyber-attacks attractive to attackers.

Cyber-criminals are directly responsible for financial assets stolen online, data breaches, and the damage and loss caused to civil society by the disruption of critical infrastructure operators. Financial losses and damage to critical infrastructures cause losses of billions of US dollars each year, and in some sectors, attack attempts are increasing two to three times each year.

There are three main reasons why cyber-attacks are increasing at such a rapid pace. The first is that industrial enterprises, which include business processes in the field of operational technology, are increasingly using digital transformation based on signaling, sensor technology and the Internet of Things technologies, and their automation systems consist entirely of these arguments. A cyber-attack on these subsystems, which have become part of operational technology, brings with it many consequences that can have major impacts on the physical world.

Another reason for the increase in cyber-attacks is that financial systems are becoming more and more online every day. Financial technology makes our lives as risky as it makes our lives easier. Financial institutions especially such as banks should be very cautious when carrying out digital transformation. The slightest mistake can result in the loss of millions of US dollars in a matter of seconds. In fact, even central banks of states are frequently targeted by cyber-attackers who see the lure of this through global systems such as SWIFT.

The third and final reason that makes cyber-attacks popular is their ease. Moreover, the identity of the attackers remains mostly anonymous, which makes it as attractive as it is easy. Today, many different types of attack methods can be used in hybrid form and can leave critical infrastructure systems completely vulnerable and exposed, often due to the lack of knowledge and mistakes of the targeted victims.

When we put all these reasons together, cyber espionage is an epidemic and very widespread. Even the world's largest companies and public institutions lose terabytes of intellectual properties and financial assets through online systems every year. Anonymous and malicious attackers threaten our power grids, national financial systems, telecommunications infrastructures, healthcare organizations and even nuclear power plants. After all, when critical infrastructures are the target of cyber-attacks, the resulting threat poses a risk to the whole society beyond the public sector.

Due to its geopolitical position, Türkiye is the target of numerous cyber attacks every day. Türkiye is also very important for other countries, especially in the field of energy, due to its important energy projects such as tanap, blue stream, Baku-Ceyhan-Tbilisi pipeline. In addition, the country is an important international financial service provider, especially MEA region, with its 51 different domestic and foreign international bank institutions. In addition to all these, when we consider that the country is the connection point of the Asian and European continents and is surrounded by commercial seas on three sides, we can easily understand what a great danger it is facing in all sectors of critical infrastructure.

CYBER-ATTACK, SECURITY & CRITICAL INFRASTRUCTURE CONCEPTS

Critical Infrastructure & Its Importance Today

Cyber security and critical infrastructure is one of the key emerging issues to be discussed within the contemporary security structure. There are multiple reasons behind cyber-attacks on critical infrastructures. According to the US Department of Homeland Security, critical infrastructure (CI) consists of "assets, systems and networks, whether physical or virtual". "2030 agenda of NATO also includes increasing cyber threats.[1]

According to data of the World Economic Forum, between 2001 and 2018, the financial losses caused by cyber-attacks targeting critical infrastructure in cities reported to the Internet Crimes Complaint Center in the US increased dramatically from 17.8 million USD to 2.71 billion USD.[2] The reason for the rapid increase over the years has been the increase in online connections. Early-stage viruses were pre-installation sector viruses and could only infect a local computer restricted by floppy disks used by users of infected sharing computers. Viruses spread on floppy disks were gradually replaced by other viruses attached to part of emails as internet service became more widespread. These viruses are designed to be attached to data files, and many attacks today continue to be carried out in this way.

As of 2021, the budget allocated for the protection of critical infrastructure only within US organizations increased by 9 Billion USD compared to the previous year and reached 105.99 Billion USD,[3] and the increase is expected to continue at a high acceleration and reach 154.59 Billion USD by 2027.[4] The main reason for this increase is the security problems that the Covid-19 pandemic has brought with remote working. IT staff and other service units responsible for critical infrastructure have had to take more precautions to ensure that systems and services continue to run smoothly despite an increasingly comfortable location-independent working environment. Therefore, the ability to securely monitor and manage infrastructure operations remotely by authorized staff has become more critical today than ever before.

For the entire IT industry and stakeholders, especially in the US, the Solarwinds Orion Attack in 2020 was a turning point in prioritizing secure connectivity. According to the information shared by Solarwinds with the SEC, in this attack 18,000 Orion customers, mostly non-governmental organizations and public institutions, found their systems under attack with the update they received.[5] Even more critical was the fact that these institutions included the Pentagon and many other ministries within the US government. The scale of the intrusion through this attack clearly demonstrates how vulnerable systems can be when they have weak connections and how easily threatening actors can infiltrate once access is gained.

[1] NATO CCDOE, Cyber Threads & NATO 2030: Horizon Scanning & Analysis, https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf, 01.12.2020, Chapter 1

[2] World Economic Forum, Our Cities are Increasingly Vulnerable to heres How They Can Fight Back, https://www.weforum.org/agenda/2019/09/our-cities-are-increasingly-vulnerable-to-cyberattacks-heres-how-they-can-fight-back/ , 30.09.2019

[3] ABI Research, Cybersecurity Spending for Critical Infrastructure to Surpass US$105 Billion in 2021 [website], https://www.abiresearch.com/press/cybersecurity-spending-critical-infrastructure-surpass-us105-billion-2021/ , (10 February 2021)

[4] Fortune Business Insights, Critical Infrastructure Protection Market, https://www.fortunebusinessinsights.com/critical-infrastructure-protection-cip-market-103339 , (01 July 2020)

[5] Business Insider, Solarwinds hack explained government agencies cyber security [website], https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12 , (15 April 2021)

After the attacks, many countries started to announce their cyber security strategy plans respectively. For example, according to the UK's National Cyber Strategy 2022[6], published on 7 February 2022, the UK's aim is to become "the world's leading cyber power, a sovereign and democratic nation that is resilient to attacks".[7] On the US side, President Joe Biden's Action Plan to Improve National Cyber Security focuses on the Federal Government's collaboration with the private and public sectors.[8] In 2015, France acted much earlier than other countries and announced an action plan based on 5 main objectives. Its main objectives include protection of information systems and critical infrastructures, security of personal data, training/awareness, international collaborations and security of the information technology environment of enterprises.[9] The fact that critical infrastructures are at the forefront of the 5 main objectives clearly demonstrates the importance and priority that nations have given to the protection of critical infrastructures since early times. Likewise, Türkiye's National Cyber Security Strategy and Action Plan (2020-2023) was published on 29 December 2020.[10]

Effective Cyber-Attacks Targeting Critical Infrastructure from Past to Present

Ukraine Power Grid Cyber-Attack - 2015

On 12 December 2015, unauthorized remote access was gained to the service centers of 3 different electricity distribution companies in Ukraine and circuit breakers were applied in 30 different substations, leaving more than 230,000 subscribers in the capital Kiev and Ivano-Frisk regions without power for hours.

The first stages of such a comprehensive cyber-attack, planned to disable public services, began in the spring of 2015. A white-collar employee of one of the electricity distribution companies unwittingly fell victim to a targeted phishing attack when s/he opened an attachment to an email s/he had received, triggering a malware that was able to infect the distribution company's internal network via his/her office laptop. This malware, called BlackEnergy[11], has been used since 2014 to infiltrate energy organizations.

The electricity distribution company had two different network systems, one between the IT network and the Internet, and the other between the IT and OT (industrial) network, with separate firewalls on each network system. In order to carry out an effective attack, it was necessary to penetrate both firewalls, enter the internal network and then send circuit breaker commands to the substations on the OT network. This could not have been accomplished by a targeted phishing attack alone, but a successful first phase would have provided all the information needed for the next phase by monitoring the computers of the system participants for some time.

During the second phase of the attack, for several months, the BlackEnergy malware was remotely controlled to collect organization-specific data, step-by-step infiltrate all server systems, detect

[6] HM Government, Government Cyber Security Strategy 2022 -2030, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1049825/government-cyber-security-strategy.pdf , (7 February 2022)

[7] HM Government, Government Cyber Security Strategy 2022 – 2030, p-8 Vision & Aim section 3, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1049825/government-cyber-security-strategy.pdf [web document], (7 February 2022)

[8] The White House, Executive Order on Improving the Nation's Cyber Security, Section 1, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/, (12 May 2021)

[9] Premier Ministre, French National Digital Security Strategy [web document], https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf , (16 October 2015)

[10] Ulaştırma ve Altyapı Bakanlığı, Ulusal Siber Güvenlik Stratejisi Eylem Planı 2020 – 2023, http://www.sp.gov.tr/upload/xSPTemelBelge/files/HwolM+ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf [web document], (29 December 2020)

[11] State of New Jersey CCIC, ICS Malware Variants – BlackEnergy, https://www.cyber.nj.gov/threat-center/threat-profiles/ics-malware-variants/blackenergy [website], (10 August 2017)

vulnerabilities and perform monitoring activities by penetrating the industrial automation network where transformers are controlled. After collecting all the necessary information with advanced persistent threat (APT) and keyloggers, malware software was installed by remotely connecting to the servers to be attacked in a short period of time when employees were not at their computers and the system was prepared for the day of the attack.

On December 23, the attacker launched the final and third phase of the attack, remotely connecting to the OT servers and quickly shutting down the circuit breakers. Distribution company operators tried to disconnect the remote connection and reactivate the transformers, but in the second stage, the attacker, who captured the operators' passwords with a keylogger, changed all passwords before the attack and prevented intervention during the attack. The entire attack took place within ten minutes, and the attacker also deleted the disks on the servers, causing permanent and catastrophic data loss. In addition, by connecting to IT servers, s/he rendered the call center inoperable with a DDoS attack and prevented subscribers from contacting the distribution center. This was enough to keep the blackout in place for a longer period of time.

To briefly mention the stages of the attack; 1st phase involved sending a targeted phishing mail with the BlackEnergy app to multiple users, which took a few days for one of the employees to interact with, and gradually spread across the organization's internal network for a months-long listening phase. The 2nd phase continued for five months as a passive listening phase. The last phase is the shortest and the 3rd phase is where the attack took place. At this stage, the systems were locked down at the right time and the entire attack took place in just ten minutes.

All three phases of the attack could not be fully analyzed because the attacker deleted data that permanently erased most of the log records on the system. There are two major factors that make this attack important; first, many different cyber-attack methods were used together to maximize the damage to critical infrastructure, and second, this attack, carried out by a Russia-based hacker group, added a new aspect to the Ukraine-Russia War that erupted after the Crimea crisis.

It is also worth reminding that 91% of all electricity networks in the world have experienced at least one cyber-attack, so that we can see more clearly how much risk electricity generation networks are under[12].

NotPetya Attack 2017

In June 2017, the NotPetya Attack, which was carried out using the ransomware method, is the cyber attack with the largest economic impact to date, with a loss of 10 billion USD to its victims. Again, this attack, which initially targeted Ukraine, later became uncontrollable and spread rapidly to many countries around the world.

The source of the attack was the M.E. Doc tax calculation application belonging to the Linkos Group in Ukraine. The application was used by all entities that trade in Ukraine and are included in the tax system. The virus infected the systems thanks to an update patch to the M.E. Doc application. The hacker group, thought to be based in Russia, infiltrated this update package and planted the ransomware software, and all entities that updated quickly incorporated the virus into their systems. The main reason why the virus caused so much damage was a vulnerability in SMB, the messaging protocol used in Microsoft operating systems, which quickly spread to the entire network system of the user entity as well as the systems of third parties and organizations connected to the entities. In this respect, the NotPetya attack is the most widespread cyber-attack in the shortest period of time.

[12] Bayar, T. (2014, Oct. 14). Cybersecurity in the power sector. Power Engineering International, Vol. 22/#9.

The attack implemented a ramsomware on the infiltrated systems and irreversibly encrypted all data on the servers, causing massive data and financial losses. Global corporations such as Merck, Fedex, Saint-Gobain and Maersk are among the most vulnerable victims of the NotPetya attack. Due to the attack, processes in the logistics supply chain of many organizations, especially Maersk, became inoperable. All trade and logistics activities of Maersk in New Jersey and Mumbai trade ports, which are very important in the world, have been suspended for a while until the problem is resolved.

Estonia Attack 2007
Estonia is the first and most open attack in which a cyber-attack was applied nationwide and cyber warfare manifested itself across the country, including public resources, government agencies, banks and health services. In 2007, the country faced a massive DDoS attack that lasted for several weeks after some political turmoil in Russia. Normally, this type of DDoS attack would have been carried out in manipulations lasting only a few days or targeting only a specific organization. After weeks of intense and unremitting attacks on Estonia, which made it impossible for public life to continue, the government described it as an act of war and asked NATO for help. Another important point that makes the attack special is that after this attack, NATO accepted cyber-attack as a threat no different from other attacks and soon announced the establishment of the CCDCoE, the cyber defense unit of the alliance, in 2008 with its headquarters in Talinn, Estonia.

As the attack took on an international aspect, a team of international experts conducted an extensive investigation into the attack. According to the findings, the servers of countries such as the US, Canada, Brazil and Vietnam were used during the attack. The findiings pointed to Russia as responsible for the attack, but this has never been confirmed by the Russian authorities. Another interesting finding was the internet traffic received by Estonian institutions. Various organizations that received around 1000 visits per day before the attack received over 2000 visits per second during the attack due to DDoS attacks. This figure far exceeds the service capacity of Estonian institutions and therefore the volume of internet traffic that a small country can handle. In the face of such a high level of attacks, the server infrastructures of major organizations in the country were unable to respond to the demands and server systems crashed. As the attacks continued, the Estonian government shut down the country's internet traffic to the outside world and blocked most of the attacks, which they believed were foreign-based, to prevent further damage.

With this attack, it was concluded that cyber-attacks can reach dimensions as dangerous as weapons of mass destruction. Only when this attack happened to a NATO member country, NATO started to allocate a serious budget for cyber defense and cyber-attacks that target countries and render critical infrastructure and public resources inoperable were accepted as another aspect of war. In this context, NATO regularly organizes the cyber defense exercise called Locked Shields every year. Since 2010, the last exercise was held in April this year in Tallinn, the epicenter of cyber defense, with 2000 participants from 33 countries, 24 of which are member countries, for 3 days.[13]

Development of Artificial Intelligence & Big Data Driven Technologies

While 5.9 Zettabytes (1 ZB = 1 Billion TB) of single and unique data constitutes the data world worldwide from the moment the data is first stored until 2020, it is stated that unique data will reach 13.41

[13] NATO, Exercise Locked Shields 2022 Concludes, https://shape.nato.int/news-archive/2022/exercise-locked-shields-2022-concludes, 23 April 2022

Zettabytes with an increase of 7.51 Zettabytes in just 4 years until 2024.[14] In other words, 2.27 times more data will be stored over a 4-year period for use in various big data and artificial intelligence applications, and the necessary measures will need to be taken to prevent that much more data from being attacked. This rapid growth in data scale will increase the need for experienced and knowledgeable cyber security experts. In this case, nations will have a good opportunity to improve the education and skills of their citizens, both to gain qualified staff and to increase employment. However, high performance requirements such as increased operational workload, the emergence of new threats, brain drain, the need for automation and zero downtime in critical systems make person-independent, automated AI-powered systems attractive.

Another reason that makes the use of artificial intelligence attractive is that it can minimize damage in the event of a possible cyber security attack or data breach. As of 2021, the cost of an average data breach worldwide is considered to be 3.86 Million USD for organizations.[15] AI-powered systems reduce application dependency by using fewer security tools, while eliminating human intervention, resulting in a significant reduction in margin of error and personnel costs. These systems stand out with the automation they provide on issues such as intrusion, targeted phishing attacks[16] and fraud detection. Today, the average cost of a data breach experienced by AI-powered organizations is 25% less than other organizations (2.9 Million USD).[17] AI-powered systems are also 27% faster than conventional systems in detecting and containing an attack.[18]

Below are examples of the use of artificial intelligence in cyber-attacks that may occur in different service areas of critical infrastructure.

Banking & Finance:	Fund & Exchange Management[19] = Anomaly Detection.
Health:	Robotic Surgery[20] & Health Registration System = Anomaly & Fault Analysis.
Transportation Systems:	Traffic Control Systems & Autopilot[21] = Fault Analysis, High Availability.
Public Administration:	E-Government = Fraud, Intrusion Detection.

VARIOUS STUDIES AND REGULATIONS IN THE WORLD

Studies Carried out by the European Union

European Union Cyber Security Law
With growing cyber security concerns, the European Union adopted a Cyber Security law to develop a common vision and mission. With the enforcement of this law, the Commission and the Member States are given responsibility for the development, implementation and review of the common cyber security

[14] Statista, Share of unique data and replicated data in the global datasphere in 2020 and 2024, https://www.statista.com/statistics/1185888/worldwide-global-datasphere-unique-replicated-data/ , (1 November 2020)
[15] Statista, Cyber Crime & Security [web page], https://www.statista.com/markets/424/topic/1065/cyber-crime-security/#overview
[16] U.Ozker & O.Sahingoz, Content Based Phishing Detection with Machine Learning, https://ieeexplore.ieee.org/document/9249892 , (9 November 2020)
[17] IBM, Data Breaches Report 2021 p:35, https://www.ibm.com/downloads/cas/OJDVQGRY
[18] IBM, Data Breaches Report 2021 p:39, https://www.ibm.com/downloads/cas/OJDVQGRY
[19] Yuan Qi and Jing Xiao. "Fintech: AI powers financial services to improve people's lives." Communications of the ACM 61.11 (2018): 65-69
[20] Danny Lange, “Cognitive Robotics,” to appear in IEEE Computer, December 2019
[21] Andrew J. Hawkins, “Deadly Boeing Crashes Raise Questions About Airplane Automation,” The Verge, https://www.theverge.com/2019/3/15/18267365/boeing-737-max-8-crash-autopilotautomation, March 15, 2019

policy. The law highlights ENISA as the implementing agency and raises awareness by providing recommendations for the development of a centralized cyber defense, setting and enforcing standards and certifications. After the enforcement of the law, ENISA became the point of contact for EU institutions and bodies to obtain information on cyber security.

In addition, ENISA will be responsible for the management of incident response teams (CSIRT) at EU level and will be charged with providing assistance to Member States against cyber-attacks.

European cyber security certification schemes will be prepared and adopted under the direction of ENISA, with expert advice, the involvement and close cooperation of industry stakeholders, EU Commissioners and EU Member States.

Once the cyber security certification scheme is adopted, manufacturers of ICT products or providers of ICT services can submit applications for certification of their products or services to the conformity assessment body of their choice. The law also establishes an EU framework for cyber security certification, enhancing the cyber security of online services and consumer devices.

When a decision is taken to initiate a new certification process, the EU Cyber Security Certification Group, consisting of EU Member States, submits the certification request to the Commission and ENISA is asked to initiate the process through the Commission. ENISA brings together a collaborative group of experts, industry participants and consultants from EU Member States to work on end-to-end certification development and regulation processes. In the final stage, the program is submitted to the EU Commission, which then completes the process by adopting the program and putting it into force.

EU Cyber Security Approach under 5G Transformation

As a result of the development of today's innovation environments, 5G is coming into our lives these days to respond to the need for a service that is faster, performant and that we can carry much more processes in our daily lives to the internet environment. The EU adopted a 5G action plan with an emphasis on cyber security as one of the pillars of its Digital Single Market Strategy, which puts cyber security at the center for unlimited data and technology use among member states.[22] When 5G networks are rolled out, they will form the backbone of a wide range of services essential for the functioning of the internal market and the maintenance and operation of vital societal and economic functions such as energy, transportation, banking and healthcare. The dependence of many critical services on 5G networks will make the consequences of systemic and widespread disruption particularly severe. As a result, ensuring the cyber security of 5G networks is an issue of strategic importance for the EU at a time when cyber-attacks are increasing and more complex than ever. The interconnected and international nature of the infrastructures supporting the digital ecosystem means that any significant vulnerability or cyber security incident related to 5G networks in one Member State will affect all EU countries. Therefore, it has become imperative that measures are taken to support a common level of cyber security of 5G networks at a high scale. In addition, foreign investment in strategic sectors, the acquisition of critical assets, technologies and infrastructure, and the procurement of critical equipment by third-party providers can also pose risks.

ENISA, the European Commission, EU Member States and national regulatory authorities have developed regulations based on the risks associated with 5G.[23] In this process, market players, sector stakeholders and academics played an active role by providing consultancy services in the process of developing the guidelines under the title of temporary working groups. One of the most striking points among the

[22] European Commission, Digital Single Market Strategy Document, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52015DC0192 , 06.05.2015
[23] https://resilience.enisa.europa.eu/article-13

regulations introduced is that, within the scope of the EU General Data Security Law[24], it was mentioned that more data will be included in our lives with the increasing use of IoT and similar systems within the 5G network and the importance of personal data protection and the possible consequences of access by unauthorized persons or organizations. In environments where the protection of personal and sensitive data is more important and difficult than ever before, additional risk management and control structures need to be put in place. In this context, in order to develop a general risk assessment structure within the EU, the working group established within the scope of the EU Partnership Group Directive[25] to determine the common precaution group, supply chain risk (the effects on the supply chain were mentioned in the section where we explained the NotPetya Attack), software vulnerability risk, access control risk, other IT-related risks were evaluated and risk management processes were put forward in a way that is integrated into 5G certification processes and managed from a single center within the EU.

The Importance of Critical Infrastructure under Energy Networks

Critical energy infrastructure represents all systems used in the generation, distribution, supply and storage of energy. Critical energy infrastructure stakeholders, electricity generation, distribution and transmission, all kinds of facilities that ensure that the materials used as fuel (coal, LPG, LNG, Petroleum, nuclear energy raw materials, renewable energy resources (wind, solar, hydroelectric)) are produced in power plants, processed into end-user products and delivered to the consumer, and the systems that ensure the management and security of the processes in these facilities are the components of critical energy infrastructure. In line with this scope, EMRA defines critical energy infrastructure as "the entirety of the energy network, assets, systems and structures whose failure to fulfill their functions, in whole or in part, would adversely affect the sustainability of social order or the provision of public services".[26] In the event of a cyber-attack on critical infrastructure stakeholders in energy networks, its potential impacts and consequences can be much more effective and destructive than if critical infrastructure assets in other areas are attacked. In the event of a cyber-attack, many powerful and destructive effects can be felt at the same time, such as damage to the physical infrastructure, threat to the national security of countries, material and moral damage to citizens, inability of institutions to fulfill their obligations, large-scale financial losses of institutions or individuals, disruption of supply and demand balances in the energy market, which can be felt on an international scale.

The majority of attacks affecting critical infrastructure, 79.32%, directly target assets in the energy sector.[27] Attacks targeting the energy sector are expected to continue day by day. This is mainly because electricity, oil, gas, nuclear and other renewable services have become increasingly data dependent on automated controls to run their networks. These infrastructure systems are now managed and automated with fully automated capabilities through interconnected network systems with the support of IoT sensors. Many modern power generation plants and organizations rely on data networks to manage meters and analyze their customers' data. If we include operational processes into this, control rooms, substations, instrumentation, refineries and pipelines used to manage plants now rely entirely on digital, video-enabled and high-speed data connections.

To manage the above processes, data and analytics-centric power generation plants often use the digital capabilities and analytical tools they have gained in recent years in core processes such as resource allocation, production optimization, safety control, preventive maintenance and supply chain planning.

[24] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4.5.2016, p. 1–88.

[25] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p.1).

[26] Türkiye Official Newspaper, https://www.resmigazete.gov.tr/eskiler/2017/07/20170713-5.htm, 13.07.2017

[27] Defender, Defending the European Energy Infrastructures, CEI Security Stakeholder Group Manifest – Deliverable 6.2, P:7, 07.11.2017

Digitalization is therefore increasingly making the energy sector more and more a potential target for cyber-attacks. Primarily digital and big data-driven systems create higher volumes of data that can be subject to data breaches or theft. For example, an oil refinery generates 1 terabyte or much more of raw data per day just to maintain these processes[28]. With a possible attack or infiltration in the systems, even a small change in only 1 character of this data can cause the entire operation process to stop and lead to irreversible losses.

The Eurobarometer opinion poll[29] shows that 86% of EU citizens also agree that there should be more collaboration between EU countries on cyber security, in particular energy, to ensure access to secure energy. In this context, under the leadership of the EU Member States and the European Commission, and with the participation of the NATO Energy Security Center of Excellence (ENSEC COE), it is undertaking an important task to bring together the new threats of cyber-attacks on the critical infrastructures, especially energy, of each partner country and even private companies, with broader research and development opportunities.

As the host of NATO's Center of Excellence for Defense Against Terrorism (COEDAT), Türkiye has a broader role to play in protecting critical energy infrastructures against cyber-attacks. In addition, considering the important infrastructure projects of international importance such as TANAP, TurkAkim, Baku-Ceyhan-Tbilisi Oil Pipeline, and Iraq-Türkiye Crude Oil Pipeline, it is not surprising that Türkiye is the 11th country in the world and the 5th country among NATO countries to be most affected by cyber-attacks in the energy sector with a cyber-attack rate of 4%. Türkiye has the potential to take the lead in this field and become a role model for the world, especially the EU, through its collaboration.

The Importance of Critical Infrastructure in Healthcare Sector

Critical health infrastructure covers private/public hospitals and health institutions associated with public health today, health and care support equipment used for all purposes, pharmaceuticals, health databases, medical products, health information systems and associated industrial control systems. With the impact of digital transformation and the Covid-19 pandemic, many services in the field of health within the framework of E-Health transformation today are carried out remotely or by devices that generate raw data with the opportunities provided by developing technology and cloud services. Healthcare services currently provided by medical technology companies are becoming increasingly interconnected and common. There are more than 500,000 different types of medical devices and equipment, such as commonly used wearable devices.[30] Thanks to such rapid sectoral growth, the economic aspect of the sector also shows a rapidly increasing momentum. In 2017, the medical technology market was approximately 115 billion USD, and by the end of 2022, it is projected to quadruple in 5 years.[31]

The importance of critical infrastructure in the healthcare sector came to the fore after the WannaCry cyber-attack in 2017. It is not surprising that a healthcare service with so many elements, complex and increasingly integrated with the digital world, would be targeted or affected by cyber-attacks. The UK National Healthcare System has faced numerous challenges as a victim of the WannaCry attack. To mention the primary problems, 19,494 patient appointments and operations were canceled, many medical devices were affected by the attack and became locked and dysfunctional.[32] Many patients had

[28] Journal of Petroleum Technology, 2012: Data Mining Applications in the Oil and Gas Industry

[29] Eurobarometer 492, https://europa.eu/eurobarometer/surveys/detail/2238, 01.02.2019

[30] Deloittle, Life Sciences for Health Care, https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Life-Sciences-Health-Care/gx-lshc-medtech-iomtbrochure.pdf

[31] MedTech Europe, The European Medical Technology Industry ib Figures 2019, https://www.medtecheurope.org/wp-content/uploads/2019/04/The-European-Medical-Technology-Industry-in-figures2019-1.pdf

[32] NAO, Investigation WannaCry cyberattack and the NHS, https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf, 01.10.2017

problems with the delivery of their tests and test results. In addition, a large number of government-related organizations connected to or integrated with the National Healthcare System have experienced difficulties in data exchange and access to NHS data, and data leaks have also occurred. There were serious problems in the systems for seven days between 12 -19 May 2017 until the attack was under control. The only silver lining in these attacks may be the lack of casualties, but not all cyber attacks have the same consequences. We can say that cyber-attacks, especially in the healthcare sector, are the type closest to resulting in human deaths.

In 2020, a German woman died when a smaller ransomware targeted the servers of the Düsseldorf University Hospital, causing corruption in medical devices.[33] Especially after WannaCry, which affected the UK National Healthcare System for a week, and the cyber-attack that resulted in death in Germany, EU member states and the Commission have established protection policies against cyber-attacks that may occur in healthcare organizations by including many regulations, trainings, certifications and processes such as CERT against cyber-attacks that affect critical infrastructure in healthcare as well as in the energy field. In this process, GDPR and NISD were updated to cover the healthcare sector and MDR regulation was established and put into effect for medical devices.

The EU and its member states have categorized the sources that could be targeted in the event of a cyber-attack in the field of healthcare into ten sub-headings. The healthcare sector, which is grouped as remote care systems, identification systems, mobile patient devices, medical devices, cloud services, clinical information systems, professional services, industrial control systems, hospital information systems, and network equipment, has been evaluated and grouped in terms of impact area, size, possible damages and technical infrastructure.

Furthermore, Panacea[34] was established in March 2022 with Horizon 2020 support, with the aim of collaboration, data sharing, education and informed cyber security, recognizing that cyber security is not only financially relevant, but also socially relevant as it threatens the operational continuity of a service while putting patient safety and personal health data at risk. The organization helps healthcare organizations assess and improve their cyber security preparedness and resilience by developing a toolkit as an integrated solution for cyber security in healthcare services. These tools synchronize with each other, providing a multi-faceted, organization-wide approach to cyber security across technology, people and processes. Although the toolkit is not a long time old, 15 university hospitals from different countries across the EU are supporting the toolkit as partners and the strengthening of critical infrastructures in the field of healthcare.

Türkiye, with its higher population and wider geography compared to many EU countries, can benefit in terms of protecting the health infrastructure of its own by participating in organizations such as Panacea at the level of university hospitals in EU countries. Likewise, by supporting healthcare sector stakeholders and entrepreneurs to create such initiatives, it can ensure more active roles in cyber security and health in programs such as Horizon 2020.

The Importance of Critical Infrastructure in the Financial Sector

Critical financial infrastructure covers banking institutions, payment systems, financial technology startups, all stock exchange organizations of various scales, and cryptocurrency organizations, which have recently been used as alternative financial assets all over the world. In recent years, there has been a significant increase in cyber-attacks on financial critical infrastructure systems due to the growth of opportunities in the field of financial technology in the financial sector, the expansion of the sector volume, the emergence of new dynamics, and the replacement of traditional banking processes with

[33] NewYork Times, https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html
[34] https://www.panacearesearch.eu/

online alternatives. According to Trend Micro's report, in the first half of 2021 alone, ransomware attacks in the banking sector increased by a massive 1318%, disproportionate to other sectors.[35] With this increase in cyber-attacks, financial companies have become 300 times more targeted than other sectors[36], clearly showing how attractive this sector is for cybercriminals. Two trends that are still developing exacerbate this risk. First, the global financial system is undergoing an unprecedented digital transformation, accelerated by the COVID-19 pandemic. Banks compete with technology companies and technology companies compete with banks. Meanwhile, the pandemic has increased demand for online financial services and made working from home arrangements the norm. Central Banks are planning to introduce digital currencies under their control, while at the same time modernizing their payment systems. Second, malicious actors are taking advantage of this digital transformation, posing a growing threat to the global financial system, financial stability and confidence in its integrity.

THREATENING	MOTIVATION	OBJECTIVE	ATTACK METHOD
Nation States, Nation Supported Groups	Geopolitical, İdeological	Financial Gain, Theft, Espionage, Political Instability, Destruction of the Nation Economy, National Destruction	Permanent Data Loss Payment Systems Disruption Fraudulent Transfers Espionage
Cyber Criminals	Unjust Gain	Theft	Cash Theft Fraudulent Transfers Identity Theft
Terrorist Groups, Internal Threats	Ideological	Political Deformation Economic Destruction	DDoS Attack Infiltration Attempt Fraud

Table – 1

Table - 1[37] shows the different actors threatening critical infrastructures in the financial sector, their motivations, objectives and the classification of the attack methods they use. Today, attacks on financial systems to gain unfair gains, political and ideological results can be considered as another reason for the increase in cyber-attacks in this field.

Cyber-attacks in the financial sector have reached a very serious and dangerous size in the last ten years. Cyber-attacks in this field can go as far as targeting the SWIFT service, an interbank fund transfer service. In 2016 and 2018, attacks based in North Korea and directly targeting the Central Banks of Malaysia and India via SWIFT were detected by the system before the transactions took place and failed.[38] But a similar attack damaged the Bangladesh Central Bank.

The attack targeting the Bangladesh Central Bank on 04.02.2016 is one of the largest and most impressive cyber heists in history. What makes the heist impressive is that the attack was carried out by professionals through the SWIFT system, stealing money directly from a country's central bank. What makes the heist

[35] TrendMicro, Attacks Surge in 2021, https://newsroom.trendmicro.com/2021-09-14-Attacks-Surge-in-1H-2021-as-Trend-Micro-Blocks-41-Billion-Cyber-Threats, 14.09.2021
[36] Boston Consulting Group (2019). Global Wealth 2019: Reigniting Radical Growth.
[37] ESRB, MI5 and Cambridge Centre for Risk Studies.
[38] https://cybernews.com/editorial/here-are-the-biggest-digital-heists-of-the-last-decade/

big is that the stolen money amounted to 81 million USD. After possibly months of preparation, the attackers, using a hybrid of organizational and technical attack methods, including system penetration, passive long-term monitoring, and credential acquisition, sent 35 fraudulent requests for money transfers to the Federal Reserve. In response to a fraudulent money transfer request, the Bank of New York asked Bangladesh Bank to transfer millions of dollars from its VOSTRO account to bank accounts in the Philippines, Sri Lanka and other parts of Asia. The attackers managed to send 81 million USD to Rizal Commercial Banking Corporation (RCBC) in the Philippines through four fraudulent transfer requests and an additional 20 million USD to Sri-Lanka through a single request. The remaining 30 fraudulent transfer requests were detected by the Fed at an early stage, preventing the theft of 850 million USD. 81 million USD sent to the Philippines in four parts was transferred to three different accounts on the same day. 20 million USD intended to be sent to Sri-Lanka was detected and blocked by the intermediary Deutsche Bank during the fund transfer routing process in the post-Fed phase. Some part of the 81 million USD stolen from the Bangladesh Central Bank was converted into pesos and the money was transferred to a recipient identified as belonging to a casino.

In an environment where these examples are proliferating, Türkiye, in order to protect itself from the cyber-attacks that other countries frequently face through SWIFT and similar means, should take the necessary measures to prevent such hybrid attacks that spread over a long period of time by maximizing security measures in the CBRT and other institutions that host critical financial infrastructure services, keeping all systems up-to-date and CERT teams trained and ready, and keeping information sharing and collaboration with all stakeholders, especially the EU, at the highest level.

The Importance of Critical Infrastructure in Transportation & Port Enterprises

The transportation and shipping sector hosts both the operational burden of critical infrastructure operators and valuable customer data, making them doubly attractive targets for cybercriminals. In 2017, in the NotPetya attack in Ukraine, which later spread to other countries, malware infiltrated Maersk's IT systems and cost the global shipping company 300 million USD loss.[39] In addition to the damage Maersk suffered, the organization's entire operational activities were disrupted, and the organization lost brand and value against its customers due to problems encountered on site.

In a similar attack scenario, hackers shut down 2,000 computers belonging to the Colorado Department of Transportation in the US.[40] One of the vulnerabilities encountered in the transportation sector, unlike other sectors, is that signaling, sensors and equipment incorporate operational technologies as well as information technologies. Such sensor-based technologies are both more vulnerable to attacks and easier to manipulate, making them much riskier. Today, stakeholders in the transportation and shipping industry see this problem in operational technologies and are forced to back up or monitor their systems more. This means more costs in terms of infrastructure and hardware investment, as well as more workload.

Another risk factor inherent in operational technologies is that they can be disrupted by hacking, which can result in physical security risks for people. As such, government agencies and regulators are putting extra pressure on institutions by issuing stricter directives and legislation.

Similarly, the European Commission has published proposals to update and strengthen cyber security rules for network and information systems, including holding senior managers accountable if their companies fail to comply with the directive. However, as the burst in ransomware continues and shipping

[39] Digital Guardian, Cost of the Malware Infection, https://digitalguardian.com/blog/cost-malware-infection-maersk-300-million,
[40] CPR News, https://www.cpr.org/2018/04/06/cdot-mostly-back-online-after-ransomware-attack/, 06.04.2018

companies connect more industrial sensors and devices to the internet, cyber threats to the travel and transportation sectors are not expected to diminish, but rather are expected to proliferate.

For this reason, it is recommended that stakeholders in the transportation and shipping industry use cyber security software, train their staff to keep knowledge and awareness at the highest level, and identify potential risks with a well-calculated emergency action plan. In this way, it is aimed to minimize the damages of a breach and ensure that operational processes continue without interruption.

Studies Conducted by the US

CISA

CISA was established on 16 November 2018 to serve as the national coordinator for the cyber defense agency of the US to ensure critical infrastructure security. CISA is currently leading the efforts of US to improve its cyber security capabilities, with key tasks including understanding, managing, and mitigating risks to critical infrastructure. In addition, CISA has two other roles assigned by the US Congress. The first is to take operational leadership of cyber security across all sectors. It is also expected to work with the public and private sectors to reduce risk to cyber and physical infrastructure, including critical US infrastructures. In this regard, the US generally prefers the public – private sector partnership model for projects that pose risks to the public or require excessive resources. Establishing and managing partnership models is the second role defined by the congress.

In order for the partnership models to provide more concrete outputs, in 2019, CISA published 55 critical functions of the government and private sector that it identified as critical to the security, economy and public health of the US. According to CISA officials, the new framework aims to better assess how problems in key systems and technologies can be identified early or resolved with minimal disruption across 16 critical infrastructure sectors.

Several funds and programs administered by CISA are available to support the proposed PPP efforts to protect critical infrastructure.

Cyber Security Grant Program has a budget of 1 billion USD, managed by CISA. The study includes implementing cyber security plans and addressing cyber security threats.

The Cyber Response and Recovery Fund is an output of the CERT law with a fund budget of 100 million USD managed by CISA.

Risk Management Agencies have a 35 million USD risk management budget managed by CISA. It will help CISA coordinate with Sector Risk Management Agencies across the federal government to support cross-sector expertise.

Cyber security research fund has a budget of 14.5 million USD, managed by CISA. Academically or federally funded research centers are eligible for research and development on technology to strengthen cyber security.

On 12 September 2022, CISA published its first comprehensive cyber security action plan, the "CISA Strategic Plan 2023-2025".[41] Its strategic plan was established in response to the cyber threats facing the US and the risk environment encompassing a global cyberspace. The strategy plan includes four main

[41] CISA, 2023 – 2025 CISA Strategic Plan, https://www.cisa.gov/sites/default/files/publications/StrategicPlan_20220912-V2_508c.pdf, 12.09.2022

objectives that are planned to be implemented until 2025. We may consider them as cyber defense, risk management, operational collaboration and workforce - combining capabilities, respectively.

White House

The White House took action on critical infrastructure at a very early stage. The first public regulations in this field were issued in 1996. Pursuant to the relevant executive order, a critical infrastructure protection commission was established with experts in the field to work on the identification of critical infrastructures, and determination and implementation of protection methods. The critical infrastructures initially identified by the responsible commission included components of the telecommunications sector, power generation plants, oil storage and transportation units, banking and financial centers, public transport systems, clean water networks and services that drive vital public activities (including health, safety and fire services). In the final report of this study, it was set as a target to gain the ability to protect the identified critical infrastructure facilities completely with internal resources within 5 years and to ensure uninterrupted operation. This report also demonstrated for the first time the need to utilize cyber competencies in addition to physical competencies to protect critical infrastructures.

Just a few years after these efforts to protect critical infrastructures, one of the biggest terrorist attacks in US history, the September 11 attacks, took place. The scope of the law, which was first introduced after this terrorist attack, has been further expanded. On 8 October 2001, a new law was signed establishing for the first time the Office of Homeland Security, assigned with creating an environment of collaboration between ministries and coordination, particularly in the field of critical infrastructure security.

With a new cyber security law published in February 2013, it was decided to establish two separate National Critical Infrastructure Centers. There shall be two centers, one for physical infrastructure and one for cyber infrastructure, which will be managed by the Ministry of Homeland Security. These centers shall carry out activities primarily targeting the following topics;

1. Supporting cyber technology products developed specifically for critical infrastructure by encouraging domestic and international R&D to enable secure and resilient infrastructure systems.

2. Developing cyber-attack modeling capabilities to identify potential impacts, measuring the effects of an incident or threat scenario on critical infrastructure, aiming to back up the infrastructure and minimize the damage arising from potential risks.

3. Adhering to the Cyber Security Action Plan, prioritizing efforts to support the plan and taking the necessary actions to ensure its success.

NATO

Since the establishment of NATO with the Washington Treaty signed on 4 April 1949, the most critical and prominent article of the treaty is undoubtedly Article 5. This article was revised only once, on 22 October 1952, when the protocol to the North Atlantic Treaty relating to the accession of Greece and Türkiye was signed in London, and since then, in its current form, it has had a major influence in shaping NATO's defense and strategic cooperation policies within the alliance. To recall Article 5, it includes the provision;

> "The Parties agree that an armed attack on one or more of them in North America or Europe shall be considered an attack on all of them and that, in the event of such an attack, they shall assist the attacked party or parties by taking such action as may be deemed necessary, individually and jointly with others, including the use of armed force, to restore and maintain security in the North Atlantic region, in exercise of the right of individual or collective self-defense

> recognized in Article 51 of the UN Charter. Any such attack and all measures taken as a result thereof shall be immediately reported to the Security Council. These measures shall be terminated when the Security Council has taken the necessary measures to restore and maintain international peace and security."[42]

After decades of shaping its policies around the effects of World War II and the Cold War, NATO was prompted by the terrorist attacks in the United States on 11 September 2001 to adopt a new set of strategies to include critical infrastructure. While Article 5 has only been invoked once in the aftermath of this attack, in the following period, allied states, led by the United States, emphasized the importance of critical infrastructure and began to develop theories about the potential of cyberspace with the development of technology. While NATO's approach to cyber security was initially characterized by debates over technical terms and theory, consensus soon emerged that it was essential to the alliance's future strategies. The need to strengthen cyber capabilities was first recognized by allied leaders at their summit meeting in Prague on 21 November 2002. Article 4f of the Prague Declaration published after the summit was the first time it was officially recognized.[43]

After Estonia's public and critical infrastructure faced cyber-attacks in 2007, NATO took the issue to the next level, recognizing that a conflict between states could include a cyber aspect, and adopted its first cyber defense policy at the Bucharest Summit in 2008. Following the Bucharest Summit, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) was established and began active operations.

Since 2008, it has been conducting interdisciplinary research, training and exercises in four main areas within NATO: technology development, strategy management, cyber defense operations and legislation, with the participation of all member states. In addition to Locked Shields, the world's largest cyber security exercise, CCDCOE is involved in important projects such as CyCon, the annual cyber security conference, and the Tallinn Guide, which examines cyber operations in terms of international legislation.

On 05.09.2014, the Wales Summit recognized that international law applies in cyberspace. Thus, since the impact of a cyber-attack can be as dangerous to allies as a conventional attack, cyber security was declared to be part of NATO's collective defense strategy under Article 5 in Articles 72 and 73 of the Welsh Declaration.[44] With the inclusion of cyberspace, the concept of hybrid warfare has entered our lives.

Following Articles 70 and 71[45] of the declaration issued after NATO's Warsaw Summit on 9 July 2016, it was decided that NATO should establish a cyber operations doctrine and develop cyber capabilities in the military field without delay. The doctrine was finally published on 29 January 2020 under the name "Joint Doctrine on Cyberspace for NATO Allies."[46] This doctrine forms the basis of NATO's current cyber defense strategies. In addition, NATO's cybersecurity framework has moved to a different stage by comprehensively defining the scope of defensive and offensive cyber operations, planning of cyber activities, risk management, potential threats and roles.

After the publication of the doctrine, NATO's IT infrastructure developed rapidly. Today, NATO covers more than 60 different locations, from political headquarters in Brussels to military sites, each with local IT services integrated with the headquarters in Brussels. There has been a significant increase in cyber-attacks targeting NATO over the last decade, and they continue to grow every day. In response, NATO

[42] NATO, Collective Defence & Article 5, https://www.nato.int/cps/en/natohq/topics_110496.htm, 20.09.2022
[43] NATO, Prague Summit Declaration, https://www.nato.int/cps/en/natohq/official_texts_19552.htm?,
[44] NATO, Wales Summit Declaration, https://www.nato.int/cps/en/natohq/official_texts_112964.htm, 05.09.2014
[45] NATO, Warsaw Summit Communique, https://www.nato.int/cps/en/natohq/official_texts_133169.htm, 09.07.2016
[46] NATO, Allied Joint Doctrine for Cyberspace Operations, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf, 29.01.2020

uses its advanced IT services and cyber defense systems to monitor and record suspicious incidents every day. Any attacks or suspicious activities are automatically detected and handled. This instantaneous monitoring process alone is carried out by a specialized cyber team of 200 people, defending the network systems of 60 different regions around the clock.[47]

As NATO moves step by step towards its 2030 vision, the "NATO 2022 Strategic Concept"[48] published on 29 June 2022 summarizes the current situation and provides detailed information on the strategies to be followed in cyberspace. The eight articles in the document directly address cyber security strategies, demonstrating the importance of protecting cyberspace for NATO. Authoritarian actors challenge our interests, our values and our democratic way of life.

According to the document, regimes that pose a threat to allied states have historically invested in nuclear weapons and missile capabilities. Today, they are targeting the security of allied states with a new generation of hybrid tactics in which the cost of investing in these weapons is very high, while the cost of investing in cyber weapons is much lower. The Russian Federation has been identified as by far the most significant and direct threat to the security of NATO allies. Moreover, the People's Republic of China also challenges NATO's interests, security and values. Russia and China are practicing hybrid and cyber operations, and their aggressive rhetoric often directly targets allies and can generate serious disinformation. Often, technological and industrial sectors, critical infrastructure, strategic operators and supply chains are the first targets.

NATO's strong posture has a modern understanding. In recent years, in addition to nuclear, conventional and missile defense capabilities complemented by space, cyber defense capabilities have become the most effective arguments for the defense of allied states. Maintaining secure use and unrestricted access to space and cyberspace is critical to the current understanding. Today, it is clearly stated that any attack on allied states, including by cyber means, could lead NATO to invoke Article 5.

In recent years, dynamics are changing rapidly all over the world due to technologies such as artificial intelligence, cyber security, cloud computing, quantum computers, autonomous technologies, biotechnology, hypersonic space technologies, 5G and blockchain. The People's Republic of China, for example, aims to become the world's leading power in artificial intelligence within the next decade. As a key part of NATO's new strategies to overhaul its defense capability, a new innovation development process called DIANA, involving new technologies, has been launched by the allies.[49] The DIANA program will increase public, private and academic collaboration on critical technologies, promote interoperability and enable rapid transformation by leveraging civic innovation. DIANA will include NATO offices, IT teams and test centers around the world. The Allies also agreed to establish a multinational and broadly participatory fund under this project.

[47] NATO, Cyber Defence, https://www.nato.int/nato_static_fl2014/assets/pdf/2021/4/pdf/2104-factsheet-cyber-defence-en.pdf, 21.04.2021

[48] NATO, 2022 Strategic Concept, https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf, 29.06.2022

[49] NATO, DIANA, https://www.nato.int/cps/en/natohq/news_194587.htm , 07.04.2022

CURRENT SITUATION AND STUDIES CONDUCTED IN TÜRKIYE

Due to its geopolitical position, Türkiye is often the target of cyber-attacks by different organizations or individuals. According to the statement made by the Ministry of Transport and Infrastructure, while 118,470 Cyber-Attacks took place in 2020, this number decreased to 84,113 in 2021.[50] The fact that it faces a cyber attack every 6.24 minutes is an important sign of the seriousness of the issue. As a matter of fact, as a result of the cyber-attack on 27 October 2019, which targeted the critical infrastructure of telecommunications institutions and banks, the operational processes of many large institutions, especially Turk Telekom and Garanti Bankasi, came to a standstill and their websites were inaccessible for a while.[51] It should also be noted that public institutions in Türkiye face an average of 82 cyber-attacks per day.[52]

Thanks to the investments made and the developing infrastructure, Türkiye has risen to 11th place in the Global Cyber Security Index, which is conducted regularly every year.[53]

Regulations and Public Arrangements

With the emergence of the concept of critical infrastructure, Türkiye has also taken many steps in this field, respectively.

With the Electronic Communications Law No. 5809[54], which entered into force in November 2008, the issue of critical infrastructure officially entered Türkiye's agenda. With the law that entered into force, the sectors, institutions, locations and risks related to critical infrastructures were identified, and the goal of keeping the country's critical infrastructure under control was set by establishing and auditing cyber security centers, carrying out necessary interventions and providing trainings to responsible persons and organizations.

Following this study, in order to protect the identified critical infrastructures and related institutions and organizations, it was decided in September 2011 to establish and launch the National Cyber Incident Response Center and a large number of Cyber Incident Response Teams under the EHK in order to carry out, manage and coordinate national cyber security activities.

It took two years to develop a national strategy and action plan. Following the decision taken in 2011, the Board started working on the development of a national cyber security action plan in a short period of time and updated the first one for 2013 - 2014, the second one for 2016 - 2019 and the last one for 2020 - 2023.

The Cyber Security Action Plan announced between 2020 – 2023 has identified critical infrastructure as a top priority. In the mission section of the Action Plan:

it is understood that critical infrastructure forms the basis of the action plan with the statement: "With the awareness that cyber security is an integral part of our national security, to protect our assets in

[50] Daily Sabah, Cyber Attacks Targeting Türkiye Dropped in 2021, https://www.dailysabah.com/Türkiye/cyberattacks-targeting-Türkiye-dropped-in-2021/news, 27.02.2022
[51] TRT News, Türkiye'ye yönelik Siber Saldırılar Bertaraf Edildi, https://www.trthaber.com/haber/turkiye/turkiyeye-yonelik-siber-saldirilar-bertaraf-edildi-437841.html, 28.10.2019
[52] Kadir Has Üniversitesi, https://panorama.khas.edu.tr/kamu-kurumlari-gunde-yaklasik-olarak-82-siber-saldiriya-ugruyor-261
[53] Global Cyber Security Index, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf, p:25
[54] Ulaştırma ve Altyapı Bakanlığı, Elektronik Haberleşme Kanunu, https://www.uab.gov.tr/uploads/pages/siber-guvenlik/5809-ehb.pdf

cyberspace, especially our critical infrastructures, from threats and to carry out activities to reduce the possible effects of cyber incidents in coordination with all relevant stakeholders".

In terms of the items of the Action Plan, while critical infrastructure was identified as a target with three different references, 22 items of the action plan were associated with the strategic objective of Protecting Critical Infrastructure and Increasing Resilience;

- 24/7 protection of the cyber security of our critical infrastructures.
- Developing a cyber security approach based on regulation and supervision in critical infrastructure sectors.
- Preventing manufacturer dependency in IT products in critical infrastructure sectors.

Collaboration & Related Institutions

Digital Transformation Office of the Presidency

In line with developing technologies, social demands and reform trends in the public sector, the Digital Transformation Office of the Presidency of the Republic of Türkiye was established in the Official Gazette No. 30474 on 10 July 2018 in order to bring together the work on digital transformation, cyber security, big data and artificial intelligence, which were carried out separately under different institutions, under a single roof.

The main task of the Digital Transformation Office is to develop cyber security strategies for public institutions and critical infrastructures within the scope of the determined policies and to support stakeholders in their implementation.

While developing strategies suitable for critical infrastructure, the Office primarily focuses on directing the capacity of the private sector to critical fields in accordance with the PPP model and utilizing it in a way to achieve maximum efficiency. Every successful implementation is ensured by the development of domestic and national cyber security products in critical infrastructure fields. DTO also contributes to the promotion of the sale of successfully produced domestic and national products, provides support for exports, and conducts various activities at home to promote the use of solutions in the public sector.

The Office also provides strong support in raising awareness and establishing training programs in the field of cyber security. For this purpose, a protocol was signed between the Digital Transformation Office of the Presidency and the Council of Higher Education on 5 October 2022 for the establishment of cyber security vocational schools. With this protocol, it is aimed to build a competent and qualified workforce in the field of cyber security, to develop cyber security teaching programs, to increase the skills and competencies of trainers in the field, to enrich the existing cyber security education content in higher education, to disseminate cyber security teaching programs and to increase employment in the field of cyber security.[55]

Another stakeholder working under DTO is the Turkish Cyber Security Cluster Platform. It carries out its activities under five main headings: market access, innovation, access to talent, interaction and technological superiority. The main objectives of the platform include increasing the number of cyber security companies in Türkiye, supporting the technical, administrative and financial development of its members, improving the standards of the cyber security ecosystem, and increasing the competitiveness

[55] Yüksek Öğretim Kurulu, Siber Güvenlik Meslek Yüksek Okulları Açılıyor, https://www.yok.gov.tr/Sayfalar/Haberler/2022/siber-guvenlik-meslek-yuksekokullari-aciliyor.aspx, 05.10.2022

of member companies in the national and global market. There are 42 different teams from 38 different universities in the cyber cluster ecosystem.

TÜBITAK
Tübitak provides support to Türkiye's critical infrastructure defenders in all areas of cyber security. The Cyber Security Institute within BILGEM is the main contractor in this field. The institution, which has made a serious name for itself especially in recent years, is expanding its organizational structure and goals day by day.

Under the leadership of the TAF and with the participation of the SGE Advanced Cyber Security Research Institute Deputy Directorate Unit, Türkiye ranked 9th in the simulation of the NATO Locked Shield Exercise in 2022, a cyber warfare exercise to increase collaboration in the field of cyber defense[56]. The 10-member team of experts has managed to neutralize many different cyber-attacks.

In order to encourage initiatives in this field, the SGE also provides support to organizations on R&D issues under different headings. In this context, efforts are being made to provide initiatives with the innovations in technology and the qualifications needed in the sector, and to present business models that may be suitable. In public and private partnership activities, the facilities and experience of the Technology Transfer Office within BILGEM are utilized. The private sector's staff and knowledge resources are seen as an important advantage, especially in the productization stages of R&D projects.

Information sharing in the field of cyber security is an important factor in making existing systems more effective. For this purpose, it is especially important that data such as cyber threat factors, attack signatures and malware databases are shared with the private sector, and similarly, the information obtained by the private sector is evaluated by the SGE. With this aim, confidentiality agreements and protocols are signed that allow mutual information sharing.

The topics of joint work carried out within the scope of Public - Private Partnership are as follows;

- To create a suitable environment to develop joint projects with domestic and foreign organizations, especially TUBITAK, that provide funds for R&D studies in the field of cyber security, and to ensure that initiatives benefit from the funds provided in the most effective way.
- To include local products in cyber security projects carried out specifically for institutions.
- SGE clearly avoids commercial project opportunities, especially those involving implementation, maintenance, support, licensing and initiatives. At the same time, it shares with all relevant initiatives the opportunities that arise to ensure equal conditions of competition between initiatives.
- To ensure that all kinds of data that provide added value in the field of cyber security or that will guarantee the security of organizations are shared with those who request them based on open data principles.

In addition, SGE provides consultancy services to public and private institutions in many areas including risk analysis, penetration testing, vulnerability testing, malware analysis and certification standards.

ICTA
The Information and Communication Technologies Authority has become Türkiye's most important institution for cyber security and protection of critical infrastructure after the Electronic Communications Law No. 5809 entered into force in the Official Gazette on 5 November 2008.[57] Following the enactment

[56] NATO, Cyber Coalition, https://www.act.nato.int/cyber-coalition
[57] HGM, https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/5809.pdf, 05.11.2008

of the EHK, many responsibilities such as the preparation of national cyber security action plans, the establishment of responsible defense units, the development of legislation, the promotion of collaboration opportunities between the public and private sectors, and raising awareness were gathered under the ICTA.

In addition, the circular No. 2016/28 “Inclusion of Public Institutions and Organizations in KamuNet”[58], which has been put into effect in recent years, aims to enable public institutions to adopt the principle of collaborative work through the online environment. In line with this purpose, secure communication and data sharing between public institutions and organizations has been gathered under ICTA with a group that includes some stakeholders such as Turk Telekom. In addition to these, the Circular also assigns ICTA as the main contractor in responsibilities such as ensuring standards in inter-agency communication in accordance with the legislation, creating the appropriate infrastructure for common applications, establishing data centers for the planned public online network and ensuring its security against cyber-attacks.[59]

In addition to these, the National Cyber Incident Response Center was established on 27/05/2013 within the Information and Communication Technologies Authority (ICTA), taking into account the cyber-attacks experienced in our country and the extent of potential risks. NCIRC has 4 main fields of activity, the most important of which is “protection of critical infrastructures”.[60] In addition, in order to protect critical infrastructures, vulnerability scanning of public resources, including critical public institutions and critical infrastructures, or monitoring activities to ensure service continuity are carried out in parallel with the “Hurricane Project”. In addition to these activities, the project periodically performs vulnerability and risk scans for a total of 16 million IP addresses, which host the critical infrastructures of the public sector, and keeps them under control. Evren pointed out that electronic communications, finance, energy, water management, transportation and critical public services were identified as critical sectors in Türkiye, and noted that 14 sectoral CERTs and 2077 corporate CERTs were operating in this context. Evren pointed out that 6264 cyber security experts in CERTs continue their work to ensure national cyber security.[61]

In addition, ICTA organizes large-scale conferences[62] and cyber security exercises with the participation of a large number of CERTs to raise awareness and develop the ecosystem.[63]

Another organization operating within the ICTA is the Cyber Security Initiative. Its aim is to collect the opinions of all stakeholders and to ensure the exchange of ideas and collaboration between institutions by conducting studies in the field of cyber security.

The Cyber Security Initiative also has other tasks. They can be listed as providing cyber security awareness trainings to SMEs, creating social awareness, establishing protection measures and publishing guidelines.[64]

[58] HGM, 2016/28 KamuNet Genelgesi, https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/kamunetgenelgesi.pdf

[59] Resmi Gazete, KamuNet Ağına Bağlanma ve KamuNet Ağının Denetimine İlişkin Usül ve Esaslar Hakkında Tebliğ, Bölüm:2 Madde:4, 21.06.2017

[60] BTK, USOM & Kurumsal Siber Olaylara Müdahale Ekibi, https://www.btk.gov.tr/usom-ve-kurumsal-siber-olaylara-mudahale-ekibi, 15.12.2017

[61] Anadolu Ajansı, Siber Güvenlik Ulusal & Uluslararası Güvenlik Stratejilerinde Yerini Aldı, https://www.aa.com.tr/tr/ekonomi/gokhan-evren-siber-guvenlik-ulusal-ve-uluslararasi-guvenlik-stratejilerinde-yerini-aldi/2599110, 27.05.2022

[62] Türkiye Bilişim Derneği, 5. Siber Güvenlik Ekosisteminin Geliştirilmesi Zirvesi, https://www.siberguvenlikzirvesi.org.tr/2022/, 25.03.2022

[63] USOM, Finans Sektörü Siber Kalkan 2022 Tatbikatı, https://www.usom.gov.tr/duyurular/finans-sektoru-siber-kalkan-2022-tatbikati, 21.10.2022

[64] BTK, Siber Güvenlik İnsiyatifi, https://www.btk.gov.tr/siber-guvenlik-inisiyatifi, 15.12.2017

Some working groups have been established under the Cyber Security Initiative. These groups are as follows;

- Awareness, Training and Report Working Group
- Legislation and Coordination Working Group on Cyber Incidents
- National Cyber Incident Response Organization Working Group
- Technical Research and Standards Working Group
- Combating Cyber Threats Working Group

BRSA & CMB

In Türkiye, the institutions responsible for establishing, implementing, supervising and controlling financial standards are the CMB and the BRSA. The latest regulation[65] dated 15 March 2020, published in the Official Gazette, sets out in detail the measures, duties and responsibilities that institutions should take to protect financial and critical infrastructures in the field of electronic banking and information systems of banks. With the regulation, the security needs and requirements that prioritize the critical infrastructures of applications such as digital banking, remote identity and account management, and mobile banking, which reveal the banking understanding of today and the future, have been placed in a broad framework and their limits have been clearly defined. In this context, the CMB and the BRSA have identified the relevant financial institutions as primarily responsible and confirmed that it is the financial institutions that are obliged to protect their critical infrastructure in accordance with the relevant communiqués as responsible for the security of personal data, the uninterrupted and secure operation of the systems, ensuring that citizens are not victimized in the event of any problems, and the pecuniary and non-pecuniary damages in case of victimization. The importance and role of obtaining ISO 27001 certification, regularization and standardization of penetration checks, and minimum security measures required in system rooms, servers and network systems were underlined and emphasized pursuant to the items in the Cyber Security Strategy.

Collaboration Studies with International Organizations

Since its establishment, the EU Cyber Security Collaboration Organization has developed numerous collaboration projects with 160 organizations in 28 different countries and continues its activities uninterruptedly. Türkiye has completed 2 cyber security projects with the participation of 2 different local organizations and installations from EU countries thanks to ECSO.[66]

The NATO Cyber Defence Centre of Excellence is an international military centre established in Tallinn, Estonia, to enhance NATO's cyber defence capabilities. The Center carries out a wide range of activities in the technical, legal and international relations aspects of Cyber Security. Türkiye organizes joint exercises with the Cyber Defense Center of Excellence and continues its joint efforts to develop its cyber defense power in NATO.

TUBITAK SGE, which has been in close relations with the EU since its establishment, has started to carry out joint studies with the organization on technical issues in its field of expertise, such as Cyber Defense Exercises. It is aimed to increase and continue these collaborations in the future.

The Cyber Security Institute participates in working groups and panels operating within NATO, together with experts from different countries, in order to represent our country in meetings, exercises and

[65] Türkiye Official Newspaper, https://www.resmigazete.gov.tr/eskiler/2020/03/20200315-10.htm, 15.03.2020

[66] ENISA, Market Study of NIS Product & Services, https://www.enisa.europa.eu/events/enisa-validation-workshop-market-study-of-nis-products-and-services/3TheDSMandcPPPinitiativeLuigiRebuffi.pdf

projects before NATO, to be aware of current issues in cyber security, to be informed about technological developments, and to introduce and present our capabilities, projects and products.

FIRST is the Global Forum for Incident Response and Safety Teams. It is one of the leading organizations in this field and a world leader in incident response. The organization brings together diverse computer security incident response teams from governmental, commercial and educational organizations. It aims to prevent cyber-attacks in the fastest way possible by encouraging rapid response to incidents and information sharing among members. Türkiye actively participates in the forum with 3 different teams. TR-CERT collaborates with Turkcell CDC and Yapi Kredi Bankasi CERT teams.[67]

NATO MISP is a community of members with knowledge on malware. By sharing information, it aims to speed up the detection of malware, develop defensive methods, especially for samples not recognized by antiviruses, and uncover methods for dealing with targeted attacks. With the contributions of members, a large repository has been created that can make searches and allows for the sharing of information in multiple ways. The Cyber Security Institute actively contributes to the NATO MISP community in order to detect malware that threatens our country, monitor their activities and take necessary measures.

EVALUATIONS & RECOMMENDATIONS

In the next 5 years, with 5G, blockchain, quantum computers, cloud systems and IoT devices becoming more widespread, all sectors with critical infrastructure will be integrated with end-to-end information technologies. Much more data will be generated than today. Managing this higher volume of data will require much higher capacity power, energy, infrastructure, security and training. According to estimates, after the process matures, 80 billion devices will be connected to the internet and will be part of our daily lives[68]. This means an average of 10 online devices per person in the world. However, the data generated will continue to grow uncontrollably day by day and the current data world will evolve rapidly, doubling every 2 years. New technologies such as autonomous vehicles in the transportation sector, the Internet of Things in industry, 5G in telecommunications, and blockchain in finance will have a major impact on sectors.

With the Covid-19 pandemic, citizens having digital identities, using online shopping and payment systems more heavily, rapidly increasing the need for computing power and storage capacity has brought cloud computing to the forefront with more powerful server systems. Since the integration process with the triggered automation brought with it a serious workload and the need for know-how, artificial intelligence took over the task in operational processes.

In this environment, governments have sought to develop regulations and sanctions against the growing influence of tech giants. In addition, reducing technological dependency and localizing technology has become an even more important goal. Indeed, although not enough, as the examples from 2020 below[69] show, this is precisely why governments have started to prioritize increasing the share of R&D in GDP in recent years.

- Israel: R&D Share: 5.44% – Increase Rate: 6%

[67] FIRST, https://www.first.org/members/map#country%3ATR
[68] ENISA, Analysis of the European R&D Priorities in Cybersecurity, https://www.enisa.europa.eu/publications/analysis-of-the-european-r-d-priorities-in-cybersecurity, p:8, 01.12.2018
[69] OECD, Gross Domestic Spending on R&D, https://data.oecd.org/rd/gross-domestic-spending-on-r-d.htm

South Korea:	R&D Share: 4.81% – Increase Rate: 4%
USA:	R&D Share: 3.45% – Increase Rate: 8.5%
Japan:	R&D Share: 3.27% – Increase Rate: 2%
Finland:	R&D Share: 2.91% – Increase Rate: 4%
France:	R&D Share: 2.35% – Increase Rate: 7.5%
Norway:	R&D Share: 2.28% – Increase Rate: 6%
Estonia:	R&D Share: 1.75% – Increase Rate: 7.4%
Greece:	R&D Share: 1.51% – Increase Rate: 18%
Poland:	R&D Share: 1.39% – Increase Rate: 5.4%
Türkiye:	R&D Share: 1.09% – Increase Rate: 1.9%

The points that nations should emphasize in order to keep their cyber competencies strong in direct proportion to the developing technology are respectively;

- Introducing the systems created for security and privacy purposes by providing trainings at the public level, increasing user knowledge and experience,
- Facilitating the teaching of security principles in all computer science education programs,
- Adding relevant trainings to the curricula so that the next generation of software engineers will have security principles,
- Expanding the use of artificial intelligence in parallel with the goal of cyber security, encouraging research and production of new technology products on quantum and supercomputers, cryptography and their algorithmic applications,
- Developing a new approach for impact assessment of distributed, complex interconnected systems,
- Secure, interoperable systems should be created by ensuring integration and data sharing between critical infrastructures.

Whether a public or private sector, if a critical infrastructure organization that is late in making the above investments and breakthroughs is in danger, it can disable the supply to all institutions and organizations that depend on its infrastructure and cause losses of millions of dollars per second. This loss may be caused by different reasons such as data breach, interruption of service, physical destruction, failure to supply energy and raw materials.

The size of expenditures to protect Critical Infrastructure is expected to grow at an average annual growth rate of 3.3% over the next five years, from around 133.3 billion USD in 2021 to 157.1 billion USD by 2026.[70]

[70] Markets & Markets, Market Research Report – Critical Infrastructure, https://www.marketsandmarkets.com/Market-Reports/critical-infrastructure-protection-cip-market-988.html?utm_source=globenewswire&utm_medium=Referral&utm_campaign=paidpr, 01.06.2021

Data breaches will account for the largest share of these expenditures in the future, as they do today. The damage caused by a cyber-attack can be very high if the data provided through data breaches are used for malicious purposes (such as fraud, infiltration of corporate network systems).

According to the IBM Cost of Data Breach 2022 report, the total average cost of a data breach globally in 2022 is 4.35 million USD, up 2.6% annually. This figure is 4.82 Million USD on average for critical infrastructure breaches, while it is 3.83 Million USD on average for other organizations.[71] Accordingly, on average, critical infrastructure breaches cause 22.9% more damage than any other breach.[72]

In addition to preventing data breaches, expenditures to protect critical infrastructure include compliance with government regulations, preventing attacks from affecting physical systems, and the increasing need to secure OT networks with Industry 4.0. In addition, the development of next-generation trusted technologies such as blockchain for use in infrastructures and increasing the availability of wireless broadband in rural areas in countries with large geographies such as Türkiye may create new opportunities for sector stakeholders in terms of investments to protect critical infrastructure.

Another alternative to minimize the impact of possible cyber-attacks on critical infrastructure is to implement a “zero trust approach”. Today, critical infrastructure organizations with a “zero trust” regime are on average 1.17 Million USD less affected than those without a zero trust approach.[73]

In order to create a reliable cyber space by taking advantage of the power of this economy and proactive environment, Public Private Partnership models against cyber risks are increasing more and more in the world. The main reason for this is that many critical infrastructures targeted by cyber attacks are actually built or operated by the private sector. The know-how in these networks is usually found at specific points as components. Therefore, an effective partnership between the public sector responsible for national security protection and the private sector responsible for these infrastructures is essential for protecting cyber risks. This model has other capabilities as well. First of all, it provides more efficient protection from limited resources and ensures duplication.

Another reason why the PPP model is preferred in the field of cyber security is the need for timely information and data sharing. Information sharing between sectors and stakeholders is critical to ensure that emergency action plans are properly implemented and to minimize the damage that attacks may cause to public life and human health. The availability of early warning systems or public awareness in the event of an attack is critical to preventing chaos scenarios or surviving them with minimal damage.

A sensitive success factor in these PPP models is effective oversight of institutional collaboration. Risk analysis and continuity planning for critical information infrastructure is the responsibility of the infrastructure owners. However, the implementation of these activities should be supervised and guided by the public. Monitoring and improvement processes require long-term collaboration and coordination. In Finland, for example, the “National Emergency Security Agency” (NESA) has assumed a strategic role in planning, analyzing, developing and overseeing collaboration opportunities, particularly in cyber security. Such agency assesses vulnerabilities and analyzes the performance of key stakeholders in critical sectors

[71] IBM, Data Breach Report 2022, https://techmonitor.ai/technology/cybersecurity/cost-of-a-data-breach-2022, 27.07.2022
[72] IBM Data Breach Report 2022, The average cost of a data breach in critical infrastructure organizations https://www.ibm.com/downloads/cas/3R8N1DZJ, p:37, 27.07.2022
[73] IBM, Data Breach Costs Reach All Time High, https://newsroom.ibm.com/2022-07-27-IBM-Report-Consumers-Pay-the-Price-as-Data-Breach-Costs-Reach-All-Time-High, 27.07.2022

of the economy. Currently, it continues its collaboration activities with more than 1000 SMEs in critical sectors in the working groups it leads.[74]

An effective PPP model should place sustainable risk and crisis management processes at the center of efforts to protect critical infrastructure security by following policies in sync with the national cyber security strategy. Regardless of which sector of critical infrastructure the PPP model is applied to, the stakeholders involved in the collaboration should be familiar with these concepts and be able to apply them consistently across their respective sectors and fields of competence. When it comes to risk assessment, risk mitigation, turning risks into actions if they materialize, ensuring regular control or oversight to improve risk management, identifying changes in existing risks as they evolve, and identifying new risks should be consistently practiced by public and private stakeholders. For example, the German Federal Information Security Office (BSI), as part of its cyber security analyses, maintains an up-to-date list of the most critical risks facing industrial control systems. In order to obtain consistent results during calculations, all events are analyzed using real databases[75].

A crisis management plan should be in place in case any risk materializes. A crisis management plan in PPP practices mainly includes the following steps: identifying a crisis; planning appropriate responses to the crisis; managing the crisis and resolving it as soon as possible. Primary responsibility and authority for crisis management should be assigned to a single institution. The actions to be taken when a crisis occurs should be determined by this institution. The institution should also coordinate all actions. The "Joint Cyber Defense Cooperation" (JCDC), established by CISA in the US, has provided great benefits in crisis management regarding cyber-attacks in recent years. JCDC has helped federal agencies and private sector partners mitigate some major cyber security attacks, including the Log4J crisis in December 2021. In addition, the development of the Shields Up campaign in response to Russia's invasion of Ukraine minimized the damage of cyber-attacks and prevented another crisis by taking an active role in deciphering the Daxin malware. Following these successful outcomes, the JCDC is also working to protect the country's electronic election infrastructure from nation-state threats for future elections in the US.[76]

Considering other country examples, on the EU side, the European Cyber Security Organization (ECSO) was established in 2016 on the PPP model. ECSO brings together representatives of national public administrations and is also open to contributions from private sector initiatives. Another important objective of ECSO is to support investments in research and development with the funds it provides. To this end, cyber security projects under Horizon 2020, which finances projects in many countries, are carried out by ECSO.[77]

Looking at the above findings from Türkiye's perspective, when designing a PPP model to protect critical infrastructures against cyber-attacks in Türkiye, an institutional structure that encourages collaboration between stakeholders should be established and the role of each stakeholder should be clearly defined at the outset. In order for the PPP to be sustainable, a common point of contact for stakeholders should be defined, and the principles that will apply throughout the collaboration process should be determined in writing. There should be an open ecosystem where cyber security products produced on the basis of PPP activities can work together with the outside world without the need for customized integrations. Established joint cyber defense collaboration groups should be in line with current trends to include

[74] National Emergency Security Agency, Maritime Cyber Security Report, https://www.huoltovarmuuskeskus.fi/files/d60cfd87d66aa5321cfc9e48dc76f8b5789603b3/maritime-cybersecurity-report.pdf, 01.01.2021

75 BSI, ISM Cyber Security, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/KRITIS/ISM_Cyber_Security.pdf?__blob=publicationFile&v=1, 01.08.2020

[76] Axios, CISA director plans proactive cybersecurity for at risk companies, https://www.axios.com/2022/08/10/cisa-director-jen-easterly-vision-for-jcdc, 10.08.2022

[77] ECSO, Cyber Security Made in Europe, https://www.cyberwatching.eu/ecso

services that produce, support and deliver industrial control systems and operational technology in accordance with the requirements of new technologies. In addition, local exercises should be planned with the participation of PPP stakeholders in line with the opportunities to test the services provided. n the event of a cyber-attack against any of the PPP stakeholders, the response should be in cooperation with the relevant public institutions, CERTs, the attacked infrastructure operator and all ecosystem stakeholders.

On the other hand, Türkiye's current cyber security systematic is mainly carried out through the Cyber Security Board established within the Information and Communication Technologies Authority (ICTA) under the Ministry of Transport and Infrastructure, the National Cyber Incident Response Center (NCIRC), and corporate/sectoral Cyber Incident Response (CERT) channels. However, the implementation and development of a cyber security strategy has become a matter of national security beyond the information technology framework due to the current stage of cyber threats. In this regard, it would be beneficial for the entire cyber security structure of the country to operate through a security-centered umbrella organization with multidisciplinary sub-agencies and institutions, and to put national security at the center of its activities. In this context, an organizational structure similar to the US Department of Homeland Security can be presented as an example. In this context, the National Cybersecurity and Communications Integration Center/NICIC, which stands out as the equivalent of NCIRC, operates under the umbrella of Homeland Security.

Within Türkiye's Cyber Security structure, AFAD is one of the institutions envisaged to operate in line with the goal of ensuring the cyber security of the country's critical infrastructure and developing cyber defense and espionage capacity. In this context, AFAD has been authorized to coordinate the crisis management process in the event of a high-intensity cyber-attack on Türkiye and a possible disaster scenario resulting from the damage such an attack could cause to critical infrastructures. Although AFAD has set cyber disaster crisis management targets with the 2014-2023 Roadmap Document for the Protection of Critical Infrastructures, it has not published any report on the process of achieving the targets as of 2022. In this respect, the institutional structure of AFAD and the processes it will carry out, as well as the availability of qualified staff within the organization to coordinate such a cyber disaster situation, raise questions. Considering that the 2014-2023 Roadmap has come to an end, it would be beneficial for AFAD to publish a general report on the action plan in cyber disaster situations and the control of the targets set in the roadmap by the end of this year.

A fundamental need in the field of Cyber Security continues to be the shortage of human resources. Education policies that can be developed in this context can be addressed under two main headings. The first of these is to ensure the supply of cyber security experts through the development of a qualified workforce. On the other hand, given that cyberspace permeates every aspect of life today, it is of secondary importance that all internet users, regardless of age, rank, position or sector, reach a certain level of awareness of potential risks and threats.

Today, it is a globally accepted assumption that cyber security formation in higher education has not yet reached the desired point. The fact that companies such as Facebook, Google and Bloomberg aim to shift software developers to the field of cyber security by creating cyber security training programs within themselves in order to train cyber security experts that such programs, which lag behind both in terms of quality and quantity, cannot supply, makes the deficiency in the academy more visible. In Türkiye, large-scale companies similar to CCI apply similar methods to fill expert positions. There are already initiatives under the leadership of YÖK and Digital Transformation Office of Presidency to address this gap in academia. In this context, 11 master's programs and 1 doctoral program have been opened in the field of Cyber Security in our country for the first time. These programs are expected to be followed by 2-year associate degree programs and 4-year Cyber Security undergraduate programs.

However, when the contents of these programs are examined, it is noticeable that only one foundation and one public university graduate program provides education in English. In this context, given the borderless nature of Cyber Security threats and the nature of the field, it is natural to expect candidates who will specialize in this field to have a command of English, the most common language in the cyber field. As a result, it is beneficial to increase the share of English in the curricula of undergraduate, master's and doctoral programs, and preferably to translate the language of formation into English as much as possible.

In addition, another policy that can be implemented beyond training cyber security professionals from scratch through the new associate degree and undergraduate programs envisaged to be opened is that some incentives can be envisaged for students with existing software / developer / computer engineering education to consider Cyber Security in their career planning. This will make it possible for young people and students who are already intellectually equipped in the field of IT to become cyber security experts in a less costly and more effective way. In this context, it is thought that the inclusion of Cyber Security undergraduate and graduate programs within the scope of the Support Scholarships that YÖK provides to students in order to make critical sectors in need of qualified staff attractive will be beneficial in making the field attractive. In addition, another policy that can be implemented for the same purpose can be to inform students about the field by providing information and promotions on Cyber Security Career Opportunities within the University Career Centers (KAGEM) operating under the coordination of the Human Resources Office of the Presidency.

Cyber security is also on the agenda of multilateral international organizations. In this context, 6 Group of Governmental Experts on Information Security (GGE) have been organized at the United Nations since 2004, the most recent one took place between 2019 and 2021 and a report was prepared in 2021. Türkiye has so far not participated in any cyber security groups within the UN. Cyber security working groups within the UN do not contribute to the formation of international cyber security norms. Türkiye's lack of involvement in the formation of international norms in the field of cyber security means that it has no influence on the outcomes. Thus, Türkiye is deprived of the opportunity to support proposals that will contribute to its cyber security and oppose those it finds harmful in the process of international norm formation. Türkiye's participation in and contribution to UN working groups such as the GGE and the Open-ended Working Group on security of and in the use of information and communications technologies (2021-2025) is important in this context.

In addition to the UN, cyber security efforts are also ongoing within NATO. In this context, Türkiye is a member of NATO's Tallinn-based cyber research and think tank, the Joint Cyber Defense Center (CCD COE) and is represented by 1 military and 1 civilian representative. Another one of the cyber security projects carried out within NATO has been to make regulations on the Law of Cyber Conflict, which has the potential to be of a pioneering nature. It is expected that the Tallinn Handbook published in this context will be updated and Tallinn Handbook 2.0 will be published. Türkiye should implement a policy similar to the one recommended within the UN to influence the regulation of the law of conflict in this new field of warfare, taking into account national security principles, and work to engage in the Tallinn process. Türkiye, which contributes at a high level to all fields of the alliance, should continue this role in the field of cyber security.

At the end of our work to protect and develop Türkiye's critical infrastructure, in summary, 6 important actions come to the fore;

1 - While creating the PPP model for the protection of critical infrastructures against cyber attacks, an institutional structure that encourages cooperation between stakeholders should be established and the role of each stakeholder should be clearly defined at the initial stage.

2 - The operation of the entire cyber security structure of the country through a security-centered umbrella organization consisting of multi-disciplinary sub-institutions and organizations will be beneficial in putting national security at the center of the activities. An example of this is the Homeland Department in the USA, which provides a proactive working environment by bringing all ministries together.

3- It should be investigated at what points the institutional structure will be used for disaster management and whether there are qualified personnel within the institutions. In addition, the national disaster management plan should be updated periodically to provide guidance for the protection of critical infrastructure for public institutions.

4-Opportunities for specialization in academia should be developed. qualified workforce is gaining more and more importance day by day. Cooperation opportunities should be increased between YÖK, Presidency Digital Transformation Office and ministries in this regard. The agreement on the establishment of cyber security and network management vocational schools between YÖK and CBDDO can be a good example. A suitable environment should be provided for the development of such collaborations.

5-Join cybersecurity groups at the UN and similar places. To contribute to the formation of international cyber security norms. If Türkiye wants to have a say in this field, it should pay attention to being productive, collaborative and sharing in international platforms and increase its momentum.

6-It should take part in global legal processes by taking into account the principles of national security in the regulation of the law of conflict. Türkiye has strict data and information security laws, especially KVKK. Especially in the development of international projects and cooperation, differences between laws create obstacles. There is a new structuring in this field and a dynamic regulation process should be established by making use of important guiding documents such as NIS Directive 2, Tallinn Manual 2.0 in the international arena. In this way, laws can play a guiding and supporting role, not a hindrance, in international services to be developed in cyberspace.

Imprint

Author: Uğur Özker

Uğur Özker is a Client Engineering solution architect at IBM Middle East & Africa. Before he worked in the fields of AI, Big Data, Cyber Security and Consulting for several years.

After various R&D activities in a technology development center between 2012 - 2014, he took part as a software architect in many global projects on the topics of smart city, electronic fare collection / point of sale systems and IoT devices between 2014-2018. After that, he was responsible for many successful Cyber Security, AI & Big Data projects as a research and development expert for the development of new technologies in the field of Fintech at the technology center of Türkiye's largest public bank.

Mr. Özker graduated with a Master degree in Computer Engineering and also possesses a Master of Business Administration. He is certified by the Project Management Institute with a PMP certificate. In addition, he has successful IT project management experience with Agile / Scrum techniques.

More details about the author on LinkedIn.

This publication reflects the views of the author only.

Konrad-Adenauer-Stiftung e.V. and Centre for Economics and Foreign Policy Studies (EDAM)

Walter Glos	Tacan Ildem
Director	President
Türkiye Office	EDAM
walter.glos@kas.de	tildem@edam.org.tr

This publication of the Konrad-Adenauer-Stiftung e. V. is for information purposes only. It may not be used by parties, election canvassers or campaigners for the purpose of election canvassing. This applies to Bundestag, state and local elections as well as to elections to the European Parliament.