SAVUNMA BİLİMLERİ DERGİSİ
The Journal of Defense Sciences

https://dergipark.org.tr/tr/pub/khosbd

Cybersecurity Maturity of Türkiye: An Assessment with ENISA's National Capabilities Assessment Framework (NCAF)

Türkiye'nin Siber Güvenlik Olgunluğu: ENISA'nın Ulusal Yetenek Değerlendirme Çerçevesi (NCAF) ile Bir Değerlendirme

Hasan ÇİFCİ [1*]

[1]*İstanbul Aydın Üniversitesi, Mühendislik Fakültesi, Yazılım Mühendisliği Bölümü, İstanbul, Türkiye*

Makale Bilgisi

Araştırma makalesi
Başvuru: 10.03.2024
Düzeltme: 16.04.2024
Kabul: 20.05.2024

Keywords

cybersecurity
maturity models
maturity assessment
National Capabilities Assessment Framework (NCAF)
Türkiye

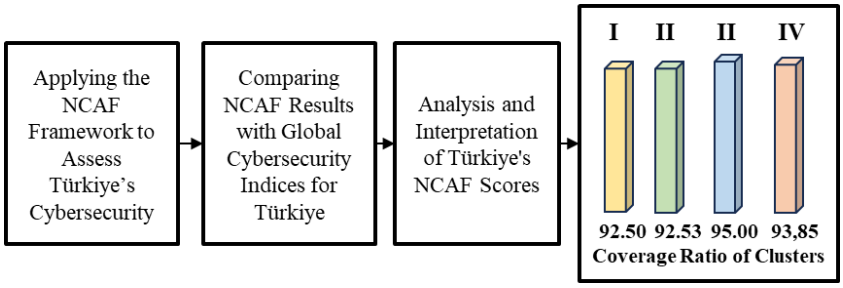
Anahtar Kelimeler

siber güvenlik
olgunluk modelleri
olgunluk değerlendirmesi
Ulusal Yetenek Değerlendirme Çerçevesi (NCAF)
Türkiye

Highlights

Türkiye's cybersecurity maturity was assessed using ENISA's NCAF and compared with global cybersecurity indices. Türkiye shows strong cybersecurity capabilities but needs improvement in some areas such as supply chain security and contingency plans. Discrepancies between Türkiye's NCAF results and global indices emphasize the complexity of cybersecurity evaluation.

Graphical Abstract



Abstract

In this study, Türkiye's cybersecurity maturity level was assessed using the European Union Agency for Cybersecurity's (ENISA) National Capabilities Assessment Framework (NCAF). To complement the NCAF findings, other global cybersecurity indices, such as the Global Cybersecurity Index (GCI), Cybersecurity Performance Index (CPI), and National Cyber Security Index (NCSI), were also given to provide a broader understanding of Türkiye's cybersecurity posture. Additionally, Türkiye's organizations, legal framework, public and private sector, academic landscape, incident response capabilities and military capabilities were presented through an extensive literature review. In this respect, this is the most up-to-date cybersecurity capability analysis of Türkiye in English. According to the findings from NCAF assessment, Türkiye has high level of cybersecurity maturity level while there are various areas that need improvement, including supply chain security, contingency strategies, education and training, security and trustworthiness of digital identity and public digital services. The comparison between Türkiye's NCAF results and global cybersecurity indices shows alignment with ITU's GCI but discrepancies with CPI and NCSI. These differences originate from different assessment criteria and emphasize the complexity of creating a universally accepted cybersecurity evaluation framework. The methodology and findings of this study can serve as a reference for researchers and policymakers to measure and enhance the cybersecurity levels of other countries.

Özet

Bu çalışmada, Türkiye'nin siber güvenlik olgunluk seviyesi, Avrupa Birliği Siber Güvenlik Ajansı'nın (European Union Agency for Cybersecurity - ENISA) Ulusal Kapasite Değerlendirme Çerçevesi (National Capabilities Assessment Framework - NCAF) kullanılarak değerlendirilmiştir. NCAF bulgularını tamamlamak amacıyla, Küresel Siber Güvenlik Endeksi (GCI), Siber Güvenlik Performans Endeksi (CPI) ve Ulusal Siber Güvenlik Endeksi (NCSI) gibi diğer küresel siber güvenlik endeksleri de ele alınarak Türkiye'nin siber güvenlik durumu hakkında daha kapsamlı bir değerlendirme sunulmuştur. Ayrıca, Türkiye'nin kurum ve kuruluşları, yasal çerçevesi, kamu ve özel sektörleri, akademik yapısı, siber olay müdahale kapasitesi ve askerî yetenekleri kapsamlı bir literatür taramasıyla ortaya konmuştur. Bu bağlamda bu çalışma, Türkiye'nin siber güvenlik kapasitesine dair İngilizce dilindeki en güncel analizdir. NCAF değerlendirmesine göre, Türkiye yüksek bir siber güvenlik olgunluk seviyesine sahipken, tedarik zinciri güvenliği, acil durum stratejileri, eğitim ve öğretim, dijital kimlik güvenliği ve kamu dijital hizmetlerinin güvenilirliği gibi iyileştirilmesi gereken muhtelif alanlar bulunmaktadır. Türkiye'nin NCAF sonuçları ile küresel siber güvenlik endeksleri arasındaki karşılaştırma, Uluslararası Telekomünikasyon Birliği'nin (ITU) GCI endeksiyle uyumluluk gösterirken, CPI ve NCSI ile bazı farklılıklar ortaya koymaktadır. Bu farklılıklar, endekslerdeki özgün değerlendirme kriterlerinden kaynaklanmakta olup, evrensel olarak kabul edilen bir siber güvenlik değerlendirme çerçevesi oluşturmanın zorluğunu ortaya koymaktadır. Çalışmanın metodolojisi ve bulguları, diğer ülkelerin siber güvenlik seviyelerini ölçmek ve geliştirmek için araştırmacılar ve politika yapıcılar için bir referans niteliği taşımaktadır.

*Corresponding author, e-mail: hasancifci@aydin.edu.tr

DOI: 10.17134/khosbd.1450078

Elektronik/Online ISSN:1303-6831
Basılı/Printed ISSN:2148-1776

1. INTRODUCTION

Increased reliance on digital technologies and a growing variety of cyber threats show the need for cybersecurity for countries [1]. Cybersecurity is a critical aspect for protecting national security, critical infrastructure, and the economy [2]. As the world becomes more interconnected and dependent on digital technology, the demand for effective cybersecurity strategies and capabilities grows.

A detailed analysis of a country's cybersecurity competence has several advantages for its long-term strategy. This assessment can provide useful information for creating a strategic plan to strengthen cybersecurity posture [3]. It can also establish a benchmark for cybersecurity capacity and assess the nation's current state of cybersecurity preparedness.

The study begins with a review of existing global cybersecurity maturity indices and models for countries including National Capabilities Assessment Framework (NCAF) tool developed by the European Union Agency for Cybersecurity (ENISA). Then, Türkiye's important initiatives, organizations, legal framework, academic landscape, public and private sector, incident response capabilities, military capabilities, and international engagement are outlined through a detailed literature review. Subsequently, findings of Türkiye's cybersecurity maturity assessment according to NCAF are presented accompanied with the results of the global cybersecurity indices.

This study is significant as it is the first to employ the NCAF tool for a country, Türkiye, which is not a member of the EU. Additionally, to the best of our knowledge, at the time of this study's preparation, there were no published journal paper in the literature that had employed this methodology. Moreover, the research stands as the most up-to-date and comprehensive analysis of Türkiye's cybersecurity stance and landscape available in English.

2. METHODOLOGY

This study employs a structured methodology to assess the cybersecurity maturity of Türkiye as of March 2024. It is primarily based on ENISA's NCAF, enhanced with an extensive literature review and analysis. The entire methodology, from data collection to data analysis, is designed to be transparent and repeatable. The steps of the methodology are as follows (Figure 1):

1. Literature Review for National-Level Cybersecurity Assessments: Widely recognized models and indices for assessing national-level cybersecurity maturity were analyzed. This was done to determine Türkiye's score and to make a comparison with the results from the NCAF assessment.

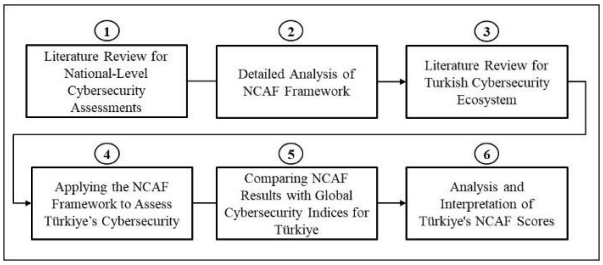


Figure 1: Main Steps of Methodology.

2. Detailed Analysis of NCAF Framework: The framework was analyzed for application. It has 472 questions addressing legislative and regulatory framework, governance, technical and operational capabilities, information sharing, incident response and capacity building domains.

3. Literature Review for Turkish Cybersecurity Ecosystem: An extensive literature review was conducted to collect the data to present cybersecurity landscape of Türkiye and to answer the questions in the NCAF. Only government resources and regulations were selected to provide correct and accurate landscape and assessment. In this study, 33 government regulations (law, strategy, decree and standard), 13 governmental web resources and 1 government-published book were used as primary data source. As it stands, this represents the most thorough compilation of data on the subject regarding Türkiye in the existing literature to date.

4. Applying the NCAF Framework to Assess Türkiye's Cybersecurity: To assess the cybersecurity level of Türkiye, the assessment tool published in ENISA's web page [4] was used. The synthesized data from the literature review was applied to the NCAF to assess Türkiye's cybersecurity maturity. Answers for the questions in the NCAF were provided by 6 of highly experienced experts some of whom held strategic positions within the Turkish government and participated in strategic initiatives.

5. Comparing NCAF Results with Global Cybersecurity Indices for Türkiye: NCAF results were compared with Türkiye's assessments in other global cybersecurity indices and models for nations.

6. Analysis and Interpretation of Türkiye's NCAF Scores: Türkiye's NCAF scores were quantitatively evaluated and qualitatively interpreted. Specific strengths and weaknesses in its cybersecurity capabilities within various categories were identified.

3. LITERATURE REVIEW

3.1. Models and Indices for Nation-Level Cybersecurity Assessment

Cybersecurity is a critical issue for nations in the current digital era [5]. To address the risks and threats, various models have been proposed to provide frameworks for mitigation at the national level [6,7]. Table 1 lists the most used models for nations in the order of last update dates.

The Cyber Power Index (CPI) was developed by The Economist Intelligence Unit in 2011 [8]. It evaluates national cyber power by considering social and economic environment, technology infrastructure, regulatory system, and industrial application. The index covers 19 of the G20 countries and scores them on a 100-point scale.

Table 1: Cybersecurity Indices and Models for Nations.

Last update	Name
2011	Cyber Power Index (CPI)
2013	The Cyber Index-International Security Trends and Realities (CI-IS)
2015	Cyber Readiness Index (CRI)
2020	National Cyber Power Index (NCPI)
2020	National Capabilities Assessment Framework (NCAF)
2021	Cyber Capabilities and National Power (CCNP)
2021	Cybersecurity Capacity Maturity Model for Nations (CMM)
2023	Global Cybersecurity Index (GCI)
2024	National Cyber Security Index (NCSI)

The Cyber Index-International Security Trends and Realities (CI-IS) study from UNIDIR (United Nations Institute for Disarmament Research) in 2013 provides information about cybersecurity trends and realities [9]. The report covers a range of topics such as cyber threats, national cybersecurity capabilities, and governance.

Potomac Institute for Policy Studies created Cyber Readiness Index (CRI) 2.0 [10] in 2015.

Index considers diplomacy and trade, national strategy, e-crime and law enforcement, information sharing, incident and crisis management, and R&D investment to evaluate national level of cybersecurity maturity.

The National Cyber Power Index (NCPI) was published by the Belfer Center for Science and International Affairs in 2020 [11]. It measures the cybersecurity capabilities and intent of 30 selected countries.

International Institute for Strategic Studies (IISS) introduced Cyber Capabilities and National Power (CCNP) report in 2021 [12]. The report presents the cybersecurity capabilities and power of 15 selected nations.

The Cybersecurity Capacity Maturity Model for Nations (CMM) is a model created by the University of Oxford to determine the cybersecurity maturity of nation-states [3]. It defines five maturity levels to define the degree of cybersecurity capacity.

The National Cyber Security Index (NCSI) is an online index developed by the e-Governance

Academy, a non-profit organization, to assess the cybersecurity readiness of nations [13]. NCSI focuses on national implementation of cybersecurity policies and programs [14].

The ITU and ABI Research launched the Global Cybersecurity Index (GCI) in 2014 to assess national level cybersecurity level [15]. The most recent report, GCI 2021, covers 180 nations [16] and is unique in the coverage of countries and geographic range [17]. GCI 5th edition was released in 2023 having metrics in five areas: technical, legal and organizational measures, capacity building, and cooperation [18].

3.2. National Capabilities Assessment Framework (NCAF)

The NCAF is a framework developed by the ENISA to assess the cybersecurity preparedness and capabilities of EU member states. There are 17 objectives that must be addressed by nations under four clusters as given in Table 2.

The NCAF provides an online platform to self-assess the cybersecurity maturity level of EU nations. It has 5 maturity levels with 472 questions addressing 17 objectives under 4 clusters.

Table 2: NCAF Clusters and Objectives.

Cluster	Cluster Name	Objectives
I	Cybersecurity Governance and Standards	1. Developing contingency plans on national cybersecurity 2. Establishing baseline cybersecurity measures 3. Securing digital identity and building trust in digital public services
II	Capacity-building and awareness	4. Establishing an incident response capability 5. Raising user awareness 6. Organizing cybersecurity exercises 7. Strengthening training and educational programs 8. Supporting Research and Development (R&D) 9. Providing incentives for the private sector 10. Enhancing the supply chain cybersecurity
III	Legal and regulatory	11. Protecting critical information infrastructure 12. Combatting cyber crime 13. Establishing incident reporting mechanisms 14. Reinforcing privacy and data protection
IV	Cooperation	15. Establishing cooperation between public agencies 16. Engaging in international cooperation 17. Establishing a public-private partnership

3.3. Cybersecurity in Türkiye

In modern society, cybersecurity has become a critical field, and Türkiye has been working to strengthen its cybersecurity infrastructure. This section presents a detailed overview of cybersecurity in Türkiye, including key strategic initiatives, governance, legal framework, academic landscape, private sector, incidence response capabilities, military capabilities, infrastructure and ICT uptake and international engagement.

3.3.1. Important Strategic Initiatives

The history of cybersecurity in Türkiye can be traced back to the establishment of the TÜBİTAK (The Scientific and Technological Research Council of Türkiye) National Electronics and Cryptology Institute and the production of the first national crypto device in 1978 [19]. In the meantime, specific cybersecurity strategies were released in the early 2000s. Main cybersecurity strategies are listed in the chronological order:

- Prime Ministry Circular No. 2003/10 (2003): This document was released by the Prime Ministry [20] and was one of the first steps to create a cybersecurity framework in the country.

- E-Transformation Türkiye Project (2003): This project was launched to transform Türkiye into an information society by utilizing the potential of information and communication technologies [21].

- E-Transformation Türkiye Project Action Plans (2003 and 2005): These action plans were released to take steps defined within E-Transformation Türkiye Project [22,23].

- Information Society Strategy and Action Plan 2006-2010 (2006): This document [24] was released to perform activities for development of an information society in Türkiye.

- National Cybersecurity Strategy and 2013-2014 Action Plan (2013): This is the first strategy document solely dedicated to cybersecurity, with a detailed action plan [25,26]. The strategy underscores the cybersecurity capabilities and resiliency of critical infrastructures.

- Information Society Strategy and Action Plan 2015-2018 (2015): This is the updated version of the previous document for the advancement of an information society in Türkiye [27]. It underscores the importance of ensuring digital service access for every citizen.

- National Cybersecurity Strategy and 2016-2019 Action Plan (2016): This is the second strategy document, which specifically focuses on cybersecurity [28]. It addresses topics, including cyber defense, cybercrime, the cybersecurity landscape, and the integration of national security with cybersecurity measures.

- Presidential Circular on Information Security Measures (2019) - This document outlines the measures to improve cybersecurity in the country [29,30]. In accordance with the Circular, an Information and Communication Security Guide was released by the Presidency Digital Transformation Office (DTO). For all public agencies, establishments, and enterprises providing critical infrastructure services, compliance with the guide is mandatory [31]. It is the responsibility of these organizations to progressively align their current IT infrastructures with the guidelines [32].

- National Cybersecurity Strategy and 2020-2023 Action Plan (2020) - The latest strategy document prioritizes protecting vital infrastructure, strengthening national capacities, combating cybercrime, encouraging the use of safe digital technologies, and fostering global cooperation [33,34].

3.3.2. Governance and Organizational Structure

Turkish government has established various policies, regulations, and institutions to deal with the cybersecurity issues. This part provides the current state of the governance and organizational structure in Turkey regarding cybersecurity. There is a wide range of cybersecurity responsibilities, ranging from formulating strategic plans to handling cyber events [35]. The main actors related to cybersecurity are (Figure 2) [20, 25, 37-46]:

- Cybersecurity Board: The Board was established in 2012 to formulate strategies and directives at the national level. The Board also has roles to evaluate and approve the plans and programs [25].

- Presidency Digital Transformation Office (DTO): The creation of this organization in 2018 aimed to consolidate various initiatives related to digital transformation, big data, national technologies, cybersecurity and artificial intelligence (AI) under one unified entity [36]. It is responsible for developing cybersecurity strategies, policies and projects for public institutions and critical infrastructures [37].

- Presidential Security and Foreign Policy Board: It is responsible for policy and strategy development on cybersecurity [37].

- Ministry of Transport and Infrastructure: This ministry creates and coordinates nationwide policies, strategies and action plans for cybersecurity [38,39].

- Information Technologies and Communications Authority (BTK): BTK is an agency for regulating and supervising the electronic communication sector. Nationwide technical solutions and controls for cybersecurity are carried out through this institution [38].

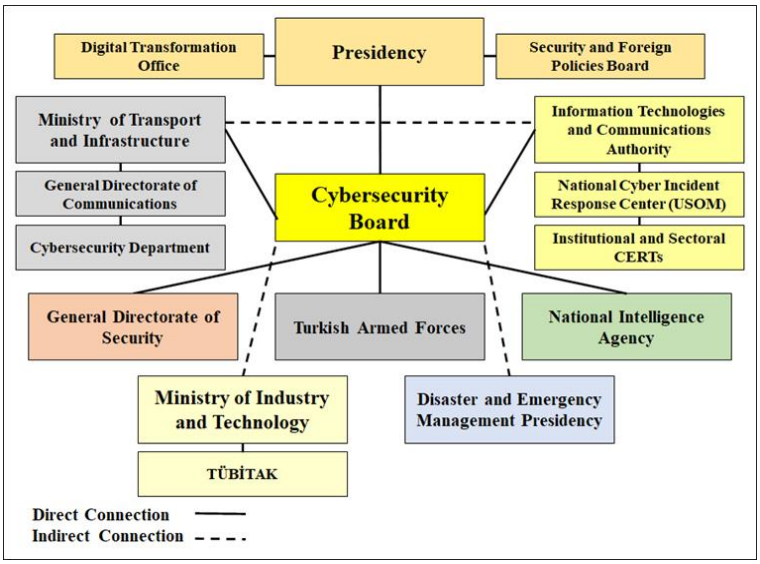


Figure 2: The Main Actors in Turkey Related to Cybersecurity.

- National Cyber Incidents Response Center (USOM, TR-CERT): It works under the BTK and is mainly responsible for country-wide cyber incident response, increasing awareness and coordination activities [25].

- Ministry of Industry and Technology: Its objective is to create plans that support the growth of R&D and the productivity of individuals and companies in critical domains such as cybersecurity, big data, and artificial intelligence (AI) [37].

- Ministry of National Defense (MND): MND is responsible for the setting strategies and overall coordination for military cybersecurity activities [20].

- Turkish Armed Forces (TAF): Responsible for the protection and security of military systems against cyber-attacks [20]. Turkish Armed Forces Cyber Defense Command is the main organization for TAF's cyber defense activities.

- General Directorate of Security (GDS): It is in charge of combating cybercrime. This task is carried out by the Department of Combating Cybercrime, which was established in 2011 [40]. Its main duties are to combat cybercrime and to raise awareness in society about cybercrime [41].

- National Intelligence Organization (MİT): It has been tasked with cyber intelligence actions since 2014 [42]. Department of Electronic and Technical Intelligence is the organization responsible for collecting the necessary intelligence to prevent cybersecurity threats for the country [43].

- Disaster and Emergency Management Presidency (AFAD): It is responsible for the protection against disaster risks in critical infrastructures in Türkiye and the management of possible disasters and emergencies [44]. It works under the Ministry of Interior [45].

- TÜBİTAK: Founded in 1963, TÜBİTAK is Türkiye's top authority for the management, funding, and application of scientific research [46]. It is responsible for scientific and technological research and development studies for cybersecurity.

3.3.3. Legal Framework

Legal framework in Türkiye was established to fight cybercrime, guarantee the protection of electronic data, communications, and personal information, and ensure a reliable and secure environment for electronic transactions.

The Electronic Signature Law No. 5070 [47], one of the important legislations in this domain, establishes the legal foundation for the use of electronic signatures in business and other transactions.

Another important law is Law No. 5651 on Regulation of Broadcasts on the Internet and Combating Crimes Committed Through These Broadcasts [48]. The law regulates the internet services and providers to combat illegal content and criminal activities.

Electronic Communications Law No. 5809 [38] creates the legal framework for electronic communications in Türkiye. Law No. 5846 on Intellectual and Artistic Works [49] protects the rights of creators and authors in the digital age. The Law No. 6563 on the Regulation of Electronic Commerce [50] and Trade Registry Regulation [51] provide the legal framework for electronic commerce in Türkiye.

The Law No. 6533 Approval of the Budapest Convention on Cybercrime [52] sets the base for combatting cybercrime while the Law No. 6698 Personal Data Protection Law [53] aims for the protection of personal information.

Decision on the Execution, Management and Coordination of National Cybersecurity Studies [25] and the Communiqué on Procedures and Principles Regarding the Establishment, Duties and Operations of Cyber Incidents Response Teams [54] are two key regulations to enhance cybersecurity governance in Türkiye [51].

Finally, the Communiqué on National Occupational Standards [55] provides the national standards for cybersecurity professionals in Türkiye to ensure a high level of expertise.

3.3.4. Academic Landscape in Terms of Cybersecurity

As of April 2024, there are 167 universities in Türkiye with departments of computer engineering, computer science, information engineering, AI engineering, and software engineering [56]. There is one university with a department of forensic information engineering and another university with a department of information security technology at the undergraduate level [56]. There are 28 universities with a master's program in cybersecurity and four universities with a doctoral program in the same field. Network security, information security, cryptology, cybersecurity, information systems security and data security are the courses commonly given in undergraduate and graduate programs of universities in Türkiye.

3.3.5. Cybersecurity Private Sector

This study examines the Turkish cybersecurity private sector, mainly from the perspective of the Turkish Cybersecurity Cluster. This cluster was acknowledged as a key component of the national cybersecurity ecosystem at the Cyber Security Ecosystem Development Summit by Ministry of Transportation and Infrastructure [57].

The Turkish Cybersecurity Cluster platform was established in 2017 under the leadership of the Defense Industry Agency (DIA) to create a cybersecurity ecosystem in Türkiye and thus create synergy by supporting companies that can produce technology and products on a global scale [58]. Aligned with a protocol signed in 2021 between the DIA and the Presidency Digital Transformation Office, it was mutually agreed to jointly undertake platform activities [59].

As of April 2024, there are 245 firms that are affiliated with the Cybersecurity Cluster, providing 373 products spanning 178 distinct categories and offering a broad range of services and training programs within 31 categories [58]. Most of the cybersecurity products by Turkish companies are related to cybersecurity event management, network security, identity and access management, application security, endpoint security, data security, web security, secure communication and cloud security.

When it comes to cybersecurity services, consultancy, network security, security audit and hardening, penetration testing and vulnerability analysis, system security, cyber incident response and application security are among the most common services.

As of April 2024, there are a total of 97 technology development zones (technoparks) in Türkiye [60]. Half of the 79 active technoparks have cybersecurity companies.

3.3.6. Incident Response Capabilities

In accordance with the National Cybersecurity Strategy and 2013-2014 Action Plan, National Cyber Incidents Response Center (USOM, TR-CERT) was established in May 2013 to respond to incidents affecting the whole country [25].

USOM appraises the alerts regarding cyber threats arising at both national and international levels and facilitates collaboration between public entities and private enterprises to identify and remediate such threats. At the same time, organizing national and international cybersecurity exercises, awareness raising, and guidance activities are among the duties of USOM [61].

Institutional CERTs and sectoral CERTs (Banking and Finance, Critical Public Services, Electronic Communications, Water Management, Transportation and Energy) are obliged to take the necessary steps to identify and prevent cyber-attacks [62] according to government regulations [54]. The coordination relationship between the USOM and CERTs is shown in Figure 3 [54].

USOM has developed projects to detect and prevent cyber threats as quickly as possible and to generate warnings.

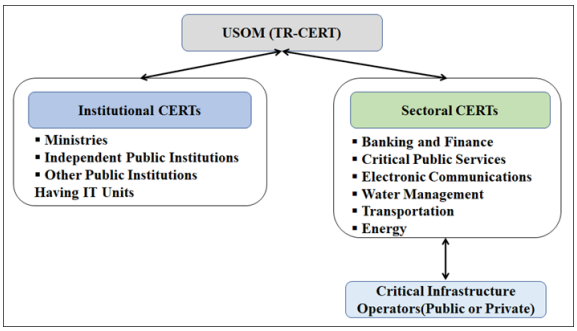


Figure 3: USOM and CERTs in Turkey.

Projects include AVCI (Hunter: Detection of infected systems and command and control centers), AZAD (Freed: Identification of AI-based, botnet member computers), KASIRGA (Hurricane: Vulnerability scan and system monitoring), ATMACA (Hawk: Vulnerability scan and detection) and KULE (Tower: Data analysis and detection). sharing) projects. USOM also has the infrastructure to forward notifications to individuals and institutions in a certain region via mobile devices [63].

3.3.7. Military Capabilities

Turkish Armed Forces (TAF) established the Cyber Defense Center in 2012 to take part in the cyberspace, which is a new operational domain. The name of the center was changed to Turkish Armed Forces Cyber Defense Command in 2013. Its scope of duty and responsibility is limited to the cyber defense of military systems [20].

The Command operates under the Turkish General Staff, Communications Electronics and Information Systems Presidency (J6), which is the member of Cybersecurity Board of Turkey, and includes personnel from all services. The aim of the command is to prevent cyber threats and gain a strong central cyber defense capability with advanced cyber defense warning and response systems.

The Command performs its operations in collaboration with other public organizations including USOM. Serving as the military CERT, it represents the supreme governing body for military cyber defense. In addition, it performs its duties in the national and international arena in coordination with NATO.

The Turkish Armed Forces Cyber Defense Center (Siber Savunma Merkezi-SİSAMER) Project was completed in 2017 to increase the strength of the command, with the aim of ensuring the security of the information systems of the TAF, enabling the TAF to react instantly on cyber defense, and reducing the effects of possible attacks [64].

3.3.8. Infrastructure and ICT Uptake

According to the ITU 2021 data, mobile-cellular network has full coverage, and 88% of the household has internet access and international bandwidth per internet user is 129 kbit/s [65].

As per the outcomes of the household survey on the usage of information technologies carried out by the Turkish Statistical Institute (TUİK), it was observed in 2023 that 95.5% of households had the capability to access the Internet from their domicile, as compared to 94.1% in the preceding year. In the 16-74 age group, the percentage of individuals who utilized internet was 85.0% in 2022, and subsequently increased to 87.1% in 2022. Furthermore, the proportion of individuals who engaged in e-commerce, either by procuring goods or services or placing orders online, was 46.2% in 2021, and rose to 49.5% in 2023 [66].

Many government services in Turkey (health, justice, environment, information, security, education, business and career, insurance, tax, fees, fines, etc.) are provided on the internet within digital transformation efforts. In 2023, the rate of individuals benefiting from public services called e-Government over the internet was 73.9% [66].

3.3.9. International Engagement

Türkiye is in the close international engagement in terms of cybersecurity through a variety of events, exercises, and membership initiatives.

Türkiye is a member of several international organizations that are dedicated to cybersecurity, including ITU, IMPACT (International Multilateral Partnership Against Cyber Threats), CAMP (Cybersecurity Alliance for Mutual Progress), and GFCE (Global Forum on Cyber Expertise). Additionally, Türkiye is a candidate for FIRST (Forum of Incident Response and Security Teams) and Trusted Introducer Membership through USOM and has participated in the ALERT (Applied Learning for Emergency Response Team). Türkiye is one of the signatory countries of Budapest Convention on Cybercrime.

Türkiye participates in international exercises such as NATO's Locked Shields, Cyber Coalition, and Trident Javelin, among others. Also, it arranges international events such as the International Cyber Warfare and Security Conference under the auspices of the government.

4. FINDINGS AND RESULTS

Findings and results from the analysis of various cybersecurity indices and the NCAF were given in this section. First, findings from cybersecurity indices and models for nations were given with the details of the scores and rankings. Then

NCAF assessment was given with the interpretation of the results. Finally, NCAF results were compared with the results of other global cybersecurity indices.

4.1. Findings from Cybersecurity Indices and Models for Nations

Over the past few decades, Türkiye has significantly improved its cybersecurity capabilities [20-33]. In this section, maturity of Türkiye's cybersecurity based on global cybersecurity indices and models are examined in the chronological order of the mentioned studies in Table 2 above. The findings provide a historical overview of the country's efforts to develop its cybersecurity capabilities.

According to CPI in 2011, Türkiye is in the 15th rank among 19 countries [8]. In Table 3, Türkiye's rankings and scores by category can be seen.

Table 3: Türkiye's Ranking and Score per CPI Category.

Nu.	Category	Türkiye's	
		Score	Ranking
1	Legal and Regulatory Framework	49.2	15
2	Economic and Social Context	24	17
3	Technology Infrastructure	29.9	10
4	Industry Application	15.9	17

UNIDIR's CI-IS gives brief information about 114 countries, including Türkiye [9]. The report only outlines the steps and actions taken by Türkiye by 2013. However, it does not contain any assessment or recommendations related to the current situation of cybersecurity in the country.

CRI by the Potomac Institute [10] is a tool that quantitatively assesses the cybersecurity posture of countries. However, the specific ranking of Türkiye is not publicly available.

According to the NCPI that was published in 2020 [11], Türkiye is in the lower capability and lower intent region, 22nd out of 29 countries, which means it has to improve cybersecurity in terms of intelligence gathering and information control.

CCNP, published in 2021 [12], provides comprehensive assessments for only 15 countries, but Türkiye is not among the countries included in this index.

The GCI created by ITU [15] provides valuable insights into the latest cybersecurity capabilities of the countries. According to GCI reports, Türkiye has been ranked consistently among the top countries in the world. In 2014, Türkiye was ranked 22nd out of 193 countries. However, Türkiye's ranking declined in 2017 to 47th out of 194 countries, but in 2018, Türkiye's ranking improved again to 20th. In 2020, Türkiye's ranking reached its highest point to date, with a ranking of 16th out of 194 countries. Despite the fluctuations in ranking, Türkiye's overall performance in the GCI demonstrates its commitment to cybersecurity. As for the reasons for fluctuations, with the help of national cybersecurity strategies and action plans [26,27], Türkiye's cybersecurity capabilities did not deteriorate between 2014 and 2017, even though Türkiye's score and ranking decreased. This fluctuation might be due to 1) Changes in the GCI methodology, as it was revised in the 2017 version to include new indicators, which led to a lack of data, 2) Relative improvement of other countries, and 3) Deficiencies in reporting

because the data collection for 2017 coincided with the coup attempt in 2016.

In Table 4, Türkiye's score per category is shown in the latest announced GCI report (GCI v4 in 2020). Note that GCI v5 report has not been announced yet at the time of writing this paper.

Table 4: Türkiye's Scores per Category in GCI v4 (2020).

Nu.	Category	Türkiye's Score
1	Legal Measures	20
2	Technical Measures	19.54
3	Organizational Measures	17.96
4	Capacity Development	20
5	Cooperative Measures	20
	Overall Score	**97.50**

Instead of a scoring or ranking system, the CMM framework by Global Cyber Security Capacity Centre provides a report that highlights the detected gaps and the present level of maturity for indicators. There is not publicly available study for Türkiye based on the CMM framework [3].

In NCSI, Türkiye ranked 65th in 2019, 45th in 2020, 49th in 2021, 57th in 2022 and 55th in 2023 [67]. Considering Türkiye's state of meeting NCSI indicators (Table 5), it is seen that it is weak in the areas of protection of digital and basic services, military cyber operations and cyber threat analysis and information, and it is successful in the areas of protection of personal data, fight against cybercrime and cybersecurity policy development.

When it comes to top countries in global indices, Table 6 lists the top 10 countries based on four different indexes: CPI, GCI (four different years), NCPI and NCSI. According to the data, none of the countries are listed in all 7 global cybersecurity indices. Türkiye is not listed in the top 10 of these indices.

Table 5: Türkiye's Percentage of Coverage of NCSI Indicators.

Nu.	Indicator	Türkiye's Coverage %
1	Protection of personal data	100
2	Fighting cybercrime	100
3	Cybersecurity policy development	100
4	E-identity and trust services	78
5	Education and professional development	78
6	Cyber crisis management	60
7	Contribution to global cybersecurity	50
8	Response to cyber incidents	50
9	Protection of digital services	20
10	Cyber threat analysis and information	20
11	Protection of essential services	17
12	Military cyber operations	17

Table 6: Top 10 Countries in Global Cybersecurity Indices.

Nu.	CPI 2011	GCI 2014	GCI 2017	GCI 2018	GCI 2020	NCPI 2020	NCSI 2023
1	UK	USA	Singapore	UK	USA	USA	Greece
2	USA	Canada	USA	USA	UK	China	Lithuania
3	Australia	Australia	Malaysia	France	S. Arabia	UK	Belgium
4	Germany	Malaysia	Oman	Lithuania	Estonia	Russia	Estonia
5	Canada	Oman	Estonia	Estonia	S. Korea	Netherlands	Czechia
6	France	N. Zealand	Mauritius	Singapore	Singapore	France	Germany
7	S. Korea	Norway	Australia	Spain	Spain	Germany	Portugal
8	Japan	Brazil	Georgia	Malaysia	Russia	Canada	Spain
9	Italy	Estonia	France	Norway	UAE	Japan	Poland
10	Brazil	Germany	Canada	Canada	Malaysia	Australia	Finland

Table 7 provides the summary of rankings of Türkiye in the mentioned global cybersecurity indices.

Table 7: Ranking of Türkiye in Global Cybersecurity Indices.

Index	Year	Number of Countries	Türkiye's	
			Ranking	Score
CPI	2011	19	15	30.40
GCI	2014	193	22	64.7
GCI	2017	194	47	58.1
GCI	2018	194	20	85.3
GCI	2020	194	11	97.49
NCPI	2020	29	22	9.00
NCSI	2023	172	55	61.04

In evaluating Türkiye's cybersecurity posture within a global context, it is insightful to compare its performance against G-20 countries (except for the European Union). G-20 nations' rankings in the latest global cybersecurity indices can be shown in Table 8. In the NCPI, Türkiye has a poor score and ranking, and it is worse in the NCSI, while it is in the top 10 in the GCI.

4.2. Findings from NCAF Assessment and Interpretation

NCAF assessment tool [4] has 472 questions (439 of them are Key Performance Indicators-KPIs) covering four clusters of cybersecurity. Questions in the tool were answered by the 6 cybersecurity experts some of whom held key positions within the Turkish government and took part in government-level strategic initiatives. Focus group and brainstorming methodologies were performed in the study.

Table 8: G-20 Rankings in Latest Global Cybersecurity Indices.

Nu.	NCPI (2020)		GCI (2020)		NCSI (2023)	
	Country	Rank	Country	Rank	Country	Rank
1	US	1	US	1	Germany	5
2	China	2	UK	2	UK	9
3	UK	3	S. Arabia	2	S. Arabia	14
4	Russia	4	S. Korea	4	France	15
5	France	6	Russia	5	Italy	23
6	Germany	7	Japan	7	Russia	30
7	Canada	8	Canada	8	Canada	33
8	Japan	9	France	9	S. Korea	34
9	Australia	10	India	10	India	36
10	S. Korea	16	Türkiye	11	Australia	42
11	India	21	Australia	12	US	46
12	Türkiye	22	Germany	13	Indonesia	49
13	S. Arabia	26	Netherlands	16	Argentina	51
14	Italy	28	Brazil	18	Japan	52
15	Indonesia	-	Italy	20	Türkiye	55
16	S. Africa	-	Indonesia	24	Brazil	71
17	Brazil	-	China	33	China	72
18	Argentina	-	Mexico	52	Mexico	92
19	Mexico	-	S. Africa	59	S. Africa	95

The results of the ENISA's NCAF assessment for Türkiye are shown in Table 9. The overall coverage ratio of 92.4% and maturity level of 4.12 out of 5 suggest that Türkiye has made significant progress in cybersecurity maturity.

The NCAF assessment results presents Türkiye's cybersecurity maturity and indicates its strong and weak areas for enhancements. The high overall coverage ratio and maturity level shows Türkiye's commitment to advancing its

cybersecurity capabilities. In terms of the four clusters, Türkiye showed strong performance in all areas. While legal and regulatory cluster has the highest and cybersecurity governance and organization has the lowest score, there is a slight and negligible difference between the clusters.

NCAF provides maturity levels for each objective from Level 1 to Level 5. The distribution of maturity levels presents vital information regarding the focus areas. 11 out of the 17 initiatives are classified at the high maturity level (Level 4). On the other hand, the presence of 2 initiatives at the low maturity level (Level 2) and 4 initiatives at a medium maturity level (Level 3) suggests that while there is a strong focus on certain objectives, there are also areas that need to be improved.

Despite the strong performance in several clusters, such as protecting critical information infrastructure, establishing baseline cybersecurity measures, organizing cybersecurity exercises, and raising user awareness, the assessment identifies specific areas where Türkiye should improve its cybersecurity posture. These include strengthening the cybersecurity supply chain, developing cybersecurity contingency plans, strengthening training and educational programs, securing digital identity and building trust in digital public services. By focusing on these specific objectives, Türkiye can improve its cybersecurity readiness and capabilities.

Table 9: NCAF Assessment Results for Türkiye.

Objective	# of Positive Answer	# of KPI	Coverage Ratio %	Maturity Level	Cluster	Coverage Ratio %	Maturity Level
1. Developing contingency plans on national cybersecurity	27	32	84,38%	3	I Cybersecurity governance and standards	92.50	3
2. Establishing baseline cybersecurity measures	27	28	96,43%	4			
3. Securing digital identity and building trust in digital public services	18	20	90,00%	2			
4. Establishing an incident response capability	22	23	95,65%	4	II Capacity-building and awareness	92.53	3.57
5. Raising user awareness	26	27	96,30%	4			
6. Organizing cybersecurity exercises	27	28	96,43%	4			
7. Strengthening training and educational programs	26	30	86,67%	3			
8. Supporting R&D	25	26	96,15%	4			
9. Providing incentives for the private sector	19	20	95,00%	4			
10. Enhancing the supply chain cybersecurity	16	20	80,00%	2			
11. Protecting critical information infrastructure	33	34	97,06%	4	III Legal and regulatory	95.00	3.75
12. Combatting cyber crime	44	47	93,62%	3			
13. Establishing incident reporting mechanisms	20	21	95,24%	4			
14. Reinforcing privacy and data protection	17	18	94,44%	4			
15. Establishing cooperation between public agencies	22	24	91,67%	3	IV Cooperation	93.85	3.67

Objective	# of Positive Answer	# of KPI	Coverage Ratio %	Maturity Level	Cluster	Coverage Ratio %	Maturity Level
16. Engaging in international cooperation	17	18	94,44%	4			
17. Establishing a public-private partnership	22	23	95,65%	4			

The NCAF assessment provides a significant roadmap to enhance cybersecurity, emphasizing the importance of a holistic approach that integrates legal, technical, organizational, and cooperative dimensions.

4.3. Comparison of Türkiye's NCAF Results with Global Cybersecurity Indices

The comparison between Türkiye's NCAF results and various global cybersecurity indices reveals mixed findings. One of the notable findings is the alignment with the ITU's GCI, which indicates that there is consistency in evaluating key elements of cybersecurity between NCAF and GCI. This shows that ITU's and ENISA's perspective to assess the cybersecurity of a country is parallel.

However, the comparison also shows discrepancies with other indices, such as the CPI, NCPI and NCSI. These variations can partly be attributed to the CPI's reliance on data from 2011, which may not accurately reflect the current state of cybersecurity. Moreover, the different evaluation criteria of the NCAF, NCSI, and NCPI illustrate the richness and variety of cybersecurity assessment methods. Each index has its unique set of criteria and methodologies, which can lead to varied interpretations and emphasis on different cybersecurity aspects. This variety shows the challenge of achieving a universally accepted framework for cybersecurity assessment and underlines the importance of understanding the specific methodologies and criteria used by each index.

By looking at these findings, it is clear that while global indices provide valuable guidelines for assessing a country's cybersecurity posture, they must be interpreted from their methodology perspectives. The differences seen in the comparison show the need for a holistic approach to cybersecurity assessment.

5. CONCLUSIONS

In this technological era, dependence on digital technologies and diversity of cyber threats require special attention on cybersecurity. To assess cybersecurity maturity levels of nations, global cybersecurity indices and maturity models are used. National Capabilities Assessment Framework (NCAF) created by the European Union Agency for Cybersecurity (ENISA) is one of the models to determine the national cybersecurity level.

In this study, Türkiye's cybersecurity maturity was assessed by using ENISA's NCAF. Findings from NCAF were supplemented and compared with the results of other global indices such as CPI, GCI, and NCSI. This research is also supported by a thorough literature review on Türkiye's cybersecurity ecosystem including national strategies, organizational structures, legal framework, public and private sector, academic landscape, and military capabilities.

The analysis reveals that Türkiye has established a solid foundation in cybersecurity, especially in terms of protecting critical information infrastructure, establishing baseline cybersecurity measures, organizing cybersecurity exercises, and raising user awareness. On the other hand, there are areas where improvements are necessary to increase Türkiye's cybersecurity maturity. These include the cybersecurity supply chain, contingency response plans, training and education, digital identity security and the reliability of digital public services.

The dynamic nature of cyber threats requires ongoing vigilance and improvement. The pursuit of higher cybersecurity maturity levels will involve not only the reinforcement of current practices but also the strategic development of new capabilities to protect against the evolving spectrum of cyber threats.

The methodology employed in this study by using NCAF combines qualitative and quantitative analysis and serves as a valuable blueprint to assess national cybersecurity maturity level. This approach and its results are expected to catalyze further academic exploration and support the formulation of better strategic cybersecurity policies.

ACKNOWLEDGMENTS

This research received no external funding.

AUTHOR CONTRIBUTIONS

Hasan ÇİFCİ: Conceptualization, writing, literature review, data collection and analysis.

CONFLICTS OF INTEREST

The author declares that he has no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

[1] L. Maglaras, I. Kantzavelou, and M. A. Ferrag, 'Digital Transformation and Cybersecurity of Critical Infrastructures', in Cyber Security of Critical Infrastructures, 2021, pp. 1–4. Accessed: Feb. 06, 2023. *https://mdpi-res.com/books/book/4750/Cyber_Security_of_Critical_Infrastructures.pdf?filename=Cyber_Security_of_Critical_Infrastructures.pdf*

[2] J. A. Lewis, 'Cybersecurity and Critical Infrastructure Protection', 2006. Accessed: Aug. 06, 2023. *http://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/0601_cscip_preliminary.pdf*

[3] Oxford GCSCC, 'Cybersecurity Capacity Maturity Model for Nations (CMM)', 2021. *https://gcscc.ox.ac.uk/the-cmm*

[4] ENISA, 'NCAF Assessment Tool'. Accessed: Nov. 11, 2023. *https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cybersecurity-assessment-framework-ncaf-tool#/*

[5] Cybersecurity Ventures, 'Cybersecurity Market Report'. Accessed: May 05, 2023. *https://cybersecurityventures.com/wp-content/uploads/2021/01/Cyberwarfare-2021-Report.pdf*

[6] CISA, 'Cybersecurity Framework'. Accessed: Oct. 05, 2023. *https://www.cisa.gov/uscert/resources/cybersecurity-framework*

[7] NIST, 'Cybersecurity Framework - Framework Documents'. Accessed: Feb. 05, 2023. *https://www.nist.gov/cyberframework/framework*

[8] EUI & Booz Allen Hamilton, 'Cyber Power Index - Findings and Methodology', pp. 1–36, 2011.

[9] UNIDIR, 'The Cyber Index-International Security Trends and Realities', 2013. *http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf*

[10] Potomac Institute for Policy Studies, 'Cyber Readiness Index 2.0', 2015. *https://potomacinstitute.org/images/CRIndex2.0.pdf*

[11] Belfer Center for Science and International Affairs, 'National Cyber Power Index 2020 - Methodology and Analytical Considerations', Belfer Center for Science and International Affairs - Harvard Kennedy School, no. September, pp. 1–71, 2020, *https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf*

[12] IISS, 'Cyber Capabilities and National Power: A Net Assessment', 2021. *https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power*

[13] eGA, 'About Us'. Accessed: Sep. 06, 2022. *https://ega.ee/about-us*

[14] eGA, 'Methodology'. Accessed: Sep. 06, 2022. *https://ncsi.ega.ee/methodology*

[15] ITU, 'Global Cybersecurity Index (GCI) 2020', 2021. *https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf*

[16] ITU, 'GCI scope and framework', 2019. *https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv4/New_Reference_Model_GCIv4_V2_.pdf*

[17] G. Acayo, 'Global Cybersecurity Index Overview'. Ispra, 2017. *https://knowledge4policy.ec.europa.eu/sites/default/files/02_-_global_cybersecurity_index_-_grace_acayo_0.pdf*

[18] ITU, 'GCI v5 Final Questionnaire'. Accessed: Oct. 22, 2023. *https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/GCIv5_E.pdf*

[19] TÜBİTAK, 'Tarihçe'. Accessed: Oct. 11, 2023. *https://uekae.bilgem.tubitak.gov.tr/tr/kurumsal/tarihce*

[20] H. Çifci, Her Yönüyle Siber Savaş, 3rd ed. Ankara, Turkey: TÜBİTAK, 2023.

[21] Prime Ministry of the Republic of Turkey, Circular No. 2003/12: e-Transformation Turkey Project. 2003. *http://www.bilgitoplumu.gov.tr/Documents/1/Mevzuatlar/BasbakanlikGenelge_2003-12.pdf*

[22] Prime Ministry of the Republic of Turkey, Circular No. 2003/48: e-Transformation Turkey Short-Term Action Plan 2003-2004. 2003. *https://www.resmigazete.gov.tr/eskiler/2003/12/20031204.htm#3*

[23] Prime Ministry of the Republic of Turkey, 2005/5 Numbered e-Transformation Turkey Project Action Plan for 2005. 2005. *https://www.resmigazete.gov.tr/Eskiler/2005/04/20050401-12.htm*

[24] Prime Ministry of the Republic of Turkey, 2006/38 Numbered Information Society Strategy and Action Plan 2006-2010. 2006. *https://www.resmigazete.gov.tr/eskiler/2006/07/20060728-7.htm*

[25] Council of Ministers, Decision on the Execution, Management and Coordination of National Cybersecurity Studies. 2012. Accessed: Feb. 03, 2023. *https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf*

[26] Council of Ministers, National Cyber Security Strategy and Action Plan 2013-2014. 2013. *https://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1.htm*

[27] Ministry of Development, 2015-2018 Information Society Strategy and Action Plan. 2015. *https://www.resmigazete.gov.tr/eskiler/2015/03/20150306M1-2.htm*

[28] Ministry of Transport Maritime and Communication, 2016-2019 National Cyber Security Strategy. 2016. *https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf*

[29] Presidency of the Republic of Turkey, Information and Communication Security Measures No. 2019/12. 2019. *https://www.mevzuat.gov.tr/MevzuatMetin/CumhurbaskanligiGenelgeleri/20190706-12.pdf*

[30] Ministry of Transport and Infrastructure, 'Minimum Information Security Criteria That Public Institutions Must Comply with', 2013. *https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/asbk.pdf*

[31] Prime Ministry of the Republic of Turkey, Circular on Inclusion of Public Institutions and Organizations in KamuNet. 2016. *https://www.resmigazete.gov.tr/eskiler/2016/12/20161203-24.pdf*

[32] DTO, 'Information and Communication Security Guide'. Accessed: Oct. 14, 2023. *https://cbddo.gov.tr/bigrehber/*

[33] Ministry of Transport and Infrastructure, 2020-2023 National Cyber Security Strategy. 2020. *https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-2020-2023.pdf*

[34] Presidency of the Republic of Turkey, National Cyber Security Strategy No. 2020/15 and Action Plan for 2020-2023. 2020. *https://www.mevzuat.gov.tr/MevzuatMetin/CumhurbaskanligiGenelgeleri/20201229-15.pdf*

[35] Presidency of the Republic of Turkey, Presidential Decree No. 4 on the Organization of Ministries, Related Institutions and Organizations and Other Institutions and Organizations. 2018. *https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=4&MevzuatTur=19&MevzuatTertip=5*

[36] DTO, 'About DTO', 2018, Accessed: Oct. 10, 2023. *https://cbddo.gov.tr/en/about-dto*

[37] Presidency of the Republic of Turkey, 1 Sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi (Presidential Decree No. 1 on the Organization of the Presidency). 2018. Accessed: Feb. 10, 2023. *https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=1&MevzuatTur=19&MevzuatTertip=5*

[38] Ministry of Transport and Infrastructure, Elektronik Haberleşme Kanunu (Electronic Communications Law). 2008. Accessed: Feb. 03, 2023. *https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5809&MevzuatTur=1&MevzuatTertip=5*

[39] Ministry of Transport and Infrastructure, Network and Information Security Regulation in the Electronic Communications Industry. 2014. *https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=19880&MevzuatTur=7&MevzuatTertip=5*

[40] EGM, 'Hakkımızda'. Accessed: Oct. 10, 2023. *https://www.egm.gov.tr/siber/hakkimizda2*

[41] Ministry of Internal Affairs, Law on Police Organization. 1937. *https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=3201&MevzuatTur=1&MevzuatTertip=3*

[42] Council of Ministers, Law Amending the Law on State Intelligence Services and the National Intelligence Organization. 2014. *https://www.resmigazete.gov.tr/eskiler/2014/04/20140426-1.htm*

[43] Presidency of the Republic of Turkey, State Intelligence Services and National Intelligence Agency Law. 1983.

https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=2937&MevzuatTur=1&MevzuatTertip=5

[44] AFAD, '2014-2023 Technological Disasters Roadmap Document', 2014. *https://www.afad.gov.tr/kurumlar/afad.gov.tr/3906/xfiles/teknolojik-afetler-son.pdf*

[45] Prime Ministry of the Republic of Turkey, Law on the Organization and Duties of the Disaster and Emergency Management Presidency. 2009. *https://www.resmigazete.gov.tr/eskiler/2009/06/20090617-1.htm*

[46] TÜBİTAK, 'Who We Are?' Accessed: Oct. 11, 2023. *https://www.tubitak.gov.tr/en/about-us/content-who-we-are*

[47] Council of Ministers, Electronic Signature Law. 2004. *https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5070&MevzuatTur=1&MevzuatTertip=5*

[48] Ministry of Transport and Infrastructure, Law on Regulation of Broadcasts on the Internet and Combating Crimes Committed Through These Broadcasts. 2007. *https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5651&MevzuatTur=1&MevzuatTertip=5*

[49] Ministry of Culture and Tourism, Intellectual and Artistic Works Law. 1951. *https://www.mevzuat.gov.tr/mevzuatmetin/1.3.5846.pdf*

[50] Ministry of Commerce, Law on the Regulation of Electronic Commerce. 2014. *https://www.mevzuat.gov.tr/mevzuatmetin/1.5.6563.pdf*

[51] Ministry of Commerce, Ticaret Sicili Yönetmeliği (Trade Registry Regulation). 2019. Accessed: Feb. 03, 2023. *https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=20124093&MevzuatTur=21&MevzuatTertip=5*

[52] Council of Ministers, Law Regarding Approval of the Agreement on Crimes Committed in the Virtual Environment. 2014. *https://www.resmigazete.gov.tr/eskiler/2014/05/20140502-12.htm*

[53] Council of Ministers, Personal Data Protection Law. 2016. *https://www.mevzuat.gov.tr/mevzuatmetin/1.5.6698.pdf*

[54] Ministry of Transport and Infrastructure, Communique on Procedures and Principles Regarding the Establishment, Duties and Operations of Cyber Incidents Response Teams. 2013. Accessed: Feb. 03, 2023. *https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=19004&MevzuatTur=9&MevzuatTertip=5*

[55] Presidency of the Republic of Turkey, Communiqué on National Occupational Standards. 2020. *https://www.resmigazete.gov.tr/eskiler/2020/02/20200209-9.htm*

[56] YÖK, 'Our Universities'. Accessed: Apr. 22, 2023. *https://www.yok.gov.tr/universiteler/universitelerimiz*

[57] Anadolu Agency, '7. Siber Güvenlik Ekosisteminin Geliştirilmesi Zirvesi başladı (EN: 7th Cyber Security Ecosystem Development Summit started)'. Accessed: Apr. 22, 2024. *https://www.aa.com.tr/tr/bilim-teknoloji/7-siber-guvenlik-ekosisteminin-gelistirilmesi-zirvesi-basladi/3155686*

[58] Siber Küme, 'Turkey Cybersecurity Cluster'. Accessed: Oct. 11, 2023. *https://siberkume.org.tr/Index*

[59] DTO, 'Cybersecurity Cluster'. Accessed: Oct. 11, 2023. *https://cbddo.gov.tr/projeler/#4800*

[60] Ministry of Industry and Technology, 'List of Technoparks in Turkey', 2023, Accessed: Oct. 11, 2023. *https://teknopark.sanayi.gov.tr/Home/TgbListesi*

[61] USOM, 'Hakkımızda'. Accessed: Oct. 10, 2023. *https://www.usom.gov.tr/hakkimizda*

[62] Energy Market Regulatory Authority, Information Security Regulation in Industrial Control Systems Used in the Energy Sector. 2017. *https://www.resmigazete.gov.tr/eskiler/2017/07/20170713-5.htm*

[63] Anadolu Agency, 'Turkey's Cyber Fortress: USOM', 2021, Accessed: Oct. 05, 2023. *https://www.aa.com.tr/tr/bilim-teknoloji/turkiyenin-siber-kalesi-usom/2439016#*

[64] MSI, 'Cyber Defense Operations Center on Duty', 2017, Accessed: Sep. 12, 2023. *https://www.savunmahaber.com/siber-savunma-harekat-merkezi-gorev-basinda/*

[65] ITU, 'Digital Development Dashboard-Türkiye'. Accessed: Feb. 13, 2023. *https://www.itu.int/en/ITU-D/Statistics/Dashboards/Pages/Digital-Development.aspx*

[66] TÜİK, 'Household Information Technologies Usage Survey'. Accessed: Apr. 22, 2024. *https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2023-49407*

[67] NCSI, 'NCSI Turkey'. Accessed: Oct. 11, 2023. *https://ncsi.ega.ee/country/tr*