Sakarya University Journal of Science

ISSN : 2147-835X
Publisher : Sakarya University

Vol. 28, No. 1, 204-219, 2024
DOI: https://doi.org/10.16984/saufenbilder.1249760

Research Article

Analysis of Türkiye's Cybersecurity Strategies: Historical Developments, Scope, Content and Objectives

Hasan Çifci[1*]

[1*] İstanbul Aydın University, Faculty of Engineering, Department of Software Engineering, İstanbul, Türkiye, hasancifci@aydin.edu.tr
[*]Corresponding Author

ARTICLE INFO

Keywords:
Cybersecurity
Turkish Cybersecurity
Cybersecurity Strategy
National Cyber Strategy
Cybersecurity Objectives

Article History:
Received: 10.02.2023
Accepted: 05.12.2023
Online Available: 27.02.2024

ABSTRACT

Cybersecurity is regarded as a crucial part of overall national security. A national cybersecurity strategy (NCSS) offers direction and a framework for national cybersecurity-related concerns and initiatives. Many nations have devised their own plans to defend against attacks, reduce risks, discourage attackers, and provide a secure and accessible cyberspace to promote innovation, the economy, commerce, and wealth. In order to assist the countries in developing their plans, organizations like the ITU, ENISA, OECD, NATO, e-Governance Academy and Oxford University issued research and advice publications based on the best practices from various countries. The assessment of the scope, objective, and content of Turkish national cybersecurity strategies is limited in academic literature. The studies in the literature that gathered multinational NCSS attributes from various countries and served as a guide for the development of national cybersecurity strategies were examined through a comprehensive literature review in order to assess Türkiye's strategies in terms of scope, content, and objectives. Following the development of assessment criteria based on these studies and research, a qualitative study was carried out to evaluate and ascertain the degree of conformity of Turkish cybersecurity strategies with the criteria. The historical context of Türkiye's cybersecurity strategies was explored in this article, along with strategy revisions, evaluations of the strategies' scope, content, and objectives, and gaps that should be filled to make the strategies more effective.

1. Introduction

Information and communication technology (ICT) is becoming increasingly vital in contemporary life. Ensuring continual access to and providing integrity and confidentiality of the ICT systems and contained data is defined as “cybersecurity” [1] and it focuses on the process of protecting information by monitoring, blocking, and dealing with cyber threats [2]. Cybersecurity is provided not only by technical means but also by establishing and applying best practices, training, concepts, guidelines, policies and strategies [1]. Cybersecurity is much more complex than just computer security. Rather, it should be viewed as a national security issue since improper use of the online services might compromise national security, safety and services that are provided for the nation’s benefit [3].

Several significant cyberattacks threatened the assets and systems in cyberspace and national security [4]. For instance, in 2007, Estonia faced a series of coordinated cyberattacks that targeted wide range of the services in internet. Iran's nuclear facilities was targeted by the Stuxnet worm in 2010 [5]. Ukraine has repeatedly been targeted by Russia before and during the war. Most recently, the United States experienced a significant breach with the ransomware attack on the Colonial Pipeline in 2021, resulting in a

Cite as: H. Cifci (2024). Analysis of Türkiye's Cybersecurity Strategies: Historical Developments, Scope, Content and Objectives, *Sakarya University Journal of Science, 28*(1), 204-219. https://doi.org/10.16984/saufenbilder.1249760

temporary shutdown of the largest fuel pipeline. These incidents demonstrate the danger of cybersecurity threats, emphasizing the necessity for comprehensive national cybersecurity strategies.

Assuring the cybersecurity of a country's cyberspace, cyberspace systems, information and communication infrastructure, and the information processed therein, particularly critical infrastructures, is of critical importance [6]. Online services are used in a variety of ways, from entertainment to education, from law enforcement and military services to banking services, and from e-commerce to international logistics services. Today, the maintenance of economic life, the continuation of the public services provided by a state, the provision of social and individual safety, security and privacy are highly dependent on the uninterrupted continuation of online services.

For this reason, ensuring the cybersecurity of critical infrastructures and ICT systems in a country, including the internet infrastructure, is one of the most critical national security challenges. National cybersecurity can be defined as the establishment of particular governmental instruments and information security guidelines for important ICT systems and content within these systems [7]. National cybersecurity strategy (NCSS) is a broad and high-level strategy for identifying and prioritizing a set of national objectives that must be met within a particular time frame in order to secure cybersecurity at a national level [8].

Analyzing and evaluating cybersecurity strategies and policies in terms of content will ensure that the steps to be taken based on them are consistent and holistic. Various studies have been carried out by international organizations such as ITU (International Telecommunication Union), ENISA (The European Union Agency for Cybersecurity), OECD (Organization for Economic Co-operation and Development), NATO (North Atlantic Treaty Organization), e-GA (e-Governance Academy) and Oxford University for the creation of cybersecurity strategies. These studies cover various topics, such as guidance on how an NCSS lifecycle should be, how an NCSS should be evaluated, what its content should cover, and what objectives should be included in an NCSS.

It can be suggested that studies on the national cybersecurity strategy in Türkiye were initiated with the publication of the OECD Guidelines for the Security of Information Systems and Networks [9] with the now-abolished Prime Ministry Circular in the early 2000s, followed by the e-Transformation Türkiye Project [4]. On the other hand, the strategy document focused directly on national-level cybersecurity, was first published in 2013 and was renewed in 2016 and 2020.

In this article, scope, content and objectives of Türkiye’s cybersecurity strategies were analyzed based on the criteria drawn from international research and studies. Based on the results of the studies carried out by reputable organizations such as ITU, ENISA, OECD, NATO, e-GA and Oxford University, the contents of NCSSs and the objectives that were and should be addressed in the NCSSs of various countries in the world were determined, and evaluation criteria were established. Then, Türkiye's national cybersecurity strategies were examined, and their compatibility with the determined criteria was revealed in detail. In this circumstance, Türkiye's cybersecurity strategies were examined in the historical context, strategy changes were determined, strategies were evaluated in terms of scope, content and objectives, and gaps identified to improve the strategies.

The significance of this study comes from its evaluation criteria, which were extracted through an extensive literature survey from the research and guidance documents created by notable organizations. Another contribution is the evaluation results of the comprehensiveness of Türkiye’s cybersecurity strategies, which provides guidance to scholars and decision-makers. In addition, by using the approach in this study, it would be easier to carry out similar studies for other countries.

2. Methodology

In the first phase of the study, an extensive literature review was undertaken to gather relevant multinational NCSS attributes and

guidance on creating national cybersecurity strategies. The review included sources such as academic journals, conference papers, reports from international organizations like ITU, ENISA, OECD, NATO, e-GA, and Oxford University, and other scholarly literature. Based on these findings, specific assessment criteria were established to evaluate the content, scope, and objectives of Türkiye's national cybersecurity strategies, reflecting best practices, international standards, and widely recognized principles in the field of cybersecurity.

The next phase involved data collection and qualitative analysis. Primary data were collected from Türkiye's official national cybersecurity strategy documents, as well as associated regulations, guidelines, and related governmental publications. Secondary data were gathered from scholarly works, reports, and analyses relating to Türkiye's cybersecurity strategies. The analysis process included careful examination of the collected documents to identify key themes, patterns, and elements that align with or diverge from the assessment criteria.

The study concluded with summarizing the findings, drawing conclusions, and developing recommendations for enhancing Türkiye's cybersecurity strategies.

3. Important Guidance Documents for Creating NCSS

A nation’s welfare and the sustainability of a business have long depended on reliable ICT systems, infrastructures and services. The importance of cybersecurity to the nation as a whole is being recognized to a greater extent. An NCSS is a mechanism for enhancing the security and robustness of national infrastructure and services and offers a comprehensive and overarching approach [8]. Even though the nations develop strategies and take actions to provide cybersecurity nationwide, United States is one of the first countries which published its national cybersecurity strategy which was part of homeland security strategy [10]. Then, other nations published their strategies by highlighting the importance of national-level strategy settings.

There are various research and studies in the literature that provide guidance for developing NCSS in terms of scope and objectives. In this context, the documents in Table 1 were analyzed to create assessment criteria for Turkish national cybersecurity strategies.

National Cybersecurity Strategy Guide [3] was developed with ITU sponsorship. The document mainly focuses on the issues that should be considered when creating or reviewing national-level cybersecurity strategies. The principles in the document were gathered from the multiple stakeholders and formulated in ends-ways-means approach. The guide comprises elements of the national cybersecurity program, and it provides a template for the strategy.

The National Cyber Security Strategies document by ENISA [8] summarizes the common objectives that need to be addressed to prepare national cybersecurity strategies with sufficient content. The document also presents a brief analysis of the current state of cybersecurity strategies, common themes and differences between EU countries and the US, Canada and Japan.

ENISA's National Cyber Security Strategies-Practical Guide on Development and Execution [11] intends to provide appropriate stakeholders with practical assistance on the formulation, execution, and maintenance of cybersecurity strategies. In addition to the strategy development stages, the practices and recommendations for these stages, the basic strategic themes that need to be addressed are included.

The National Cybersecurity Framework Manual, created by NATO Cooperative Cyber Defense Center of Excellence (CCD COE) [7], highlights various aspects of national cybersecurity rather than giving the steps to follow for strategy development at the national level. Detailed information is given about the issues that need to be addressed in the strategies and the issues that need to be balanced.

Table 1. Important Guidance Documents for Creating NCSS

No	Year	Institution	Document
G1	2011	ITU	National Cybersecurity Strategy Guide
G2	2012	ENISA	National Cyber Security Strategies
G3	2012	ENISA	National Cyber Security Strategies-Practical Guide on Development and Execution
G4	2012	NATO	National Cyber Security Framework Manual
G5	2012	OECD	Cybersecurity Policy Making at a Turning Point
G6	2014	ENISA	An Evaluation Framework for National Cyber Security Strategies
G7	2016	ENISA	NCSS Good Practice Guide: Designing and Implementing National Cyber Security Strategies
G8	2018	ITU	Guide to Developing a National Cyber Security Strategy-Strategic Engagement in Cybersecurity
G9	2019	ENISA	Good Practices in Innovation Under NCSS
G10	2020	ENISA	National Capabilities Assessment Framework (NCAF)
G11	2020	e-GA	National Cyber Security in Practice
G12	2021	GCSCC	Cybersecurity Capacity Maturity Model for Nations (CMM)

Cybersecurity Policy Making at a Turning Point report, created by OECD [12], includes an analysis of a total of ten voluntary OECD countries (Australia, Canada, France, Germany, Japan, Netherlands, UK, USA, Finland and Spain) that published their cybersecurity policies between 2009 and 2011. The report provides insights on commonalities and variances between nations, as well as significant changes between policy generations.

An Evaluation Framework for National Cyber Security Strategies, developed by ENISA [13], includes the analysis of the strategies of 18 EU member states and 8 other countries and the findings obtained as a result of 11 interviews. The framework document aims to conduct an inventory of approaches used for evaluating strategies, provide recommendations on the implementation and evaluation of strategies, identify good practices, develop an evaluation framework, and support the framework with key performance indicators.

NCSS Good Practice Guide: Designing and Implementing National Cyber Security Strategies created by ENISA [14] is the updated version of the guide prepared in 2012 [11]. The original guide's various processes, objectives, and best practices were reassessed, and the strategies of EU member states and European Free Trade Association members (Norway, Switzerland, Iceland and Liechtenstein) were analyzed. The document's goal is to assist these countries in developing and updating their national cybersecurity strategies.

Guide to Developing a National Cyber Security Strategy-Strategic Engagement in Cybersecurity, created under the coordination of ITU [15], aims to establish a set of guidelines and best practices for developing, formulating, and implementing national cybersecurity strategies. In this context, the stages for all phases of the strategy were explained in detail. Additionally, general principles and the areas to focus on were specified in the document.

The main purpose of the Good Practices in Innovation Under NCSS document by ENISA [16] is to analyze the cybersecurity innovation environment in EU member states and present the challenges and good practices in innovation when implementing national cybersecurity strategies. In the document, the main objectives that should be included in the national strategies, which were determined as a result of the interviews with the member countries, are included.

In accordance with the EU Network and Information Security Directive [17], each EU member country is required to have a national cybersecurity strategy. In this context, the National Capabilities Assessment Framework (NCAF) document by ENISA [18] provides a model for member countries to measure the maturity level of strategies.

National Cyber Security in Practice [19] is a handbook developed by e-Governance Academy (e-GA) and supported by Estonian Ministry of Foreign Affairs. It defines the key elements of a country’s cybersecurity architecture.

The Cybersecurity Capacity Maturity Model for Nations (CMM) is a maturity framework developed by Oxford University's Global Cybersecurity Capacity Center (GCSCC) with over 200 experts worldwide to determine the level of cybersecurity maturity of countries [20]. The model was developed in 2014, and the most recent iteration was released in 2021. The CMM lists five factors that must be addressed at the national level in order to properly handle cybersecurity. These are legal and regulatory measures, cybersecurity policy and strategy, cybersecurity culture and society, creating cybersecurity knowledge and capabilities and technology and standards.

Academic literature is lacking regarding assessment of the content, scope and objectives of the Turkish NCSSs. Çakır and Arınmış [21] evaluated the strategies and action plans by using 11 criteria (continuity, protection of critical infrastructures, research and development supports, leadership, national and international cooperation, human resources development, education and training, legislation, budget allocation, cyber deterrence, and monitoring of action plan results) derived from the European Union and ENISA documents. The study suggested that the number of criteria can be increased but kept concise since they are sufficient to assess the strategies. On the other hand, the study lacks explanations as to why the mentioned criteria were chosen and extracted from which exact sources.

4. Important Turkish Cybersecurity Strategy Initiatives and Historical Developments

It is possible to trace the beginning of the most important studies on cybersecurity in Türkiye to the establishment of TUBITAK National Electronics and Cryptology Institute and especially to the production of the first national crypto device in 1978 [22]. On the other hand, it is seen that studies on the strategy started in the early 2000s.

The historical development of Turkish cybersecurity strategies demonstrates the country's increasing focus on protecting its citizens, businesses, and critical infrastructure from cyber threats. The first strategy document, Prime Ministry Circular No. 2003/10, was released in 2003 [4] on the security guideline [9] published by the OECD laid the foundation for the country's cybersecurity efforts. This was followed by the E-Transformation Türkiye Project [23] and its action plans [24], which aimed to create a more secure and efficient digital environment. The Information Society Strategy and Action Plan 2006-2010 [25] further advanced these efforts by defining a comprehensive framework for promoting the growth of the information society.

In 2013, the National Cybersecurity Strategy and 2013-2014 Action Plan [26] marked a new phase in the country's cybersecurity efforts, with a focus on strengthening national cybersecurity and improving the resilience of critical infrastructure. This was followed by the Information Society Strategy and Action Plan 2015-2018 [27], which continued to prioritize cybersecurity while also emphasizing the importance of access to digital services for all citizens. The National Cybersecurity Strategy and 2016-2019 Action Plan [28] further expanded on these efforts, focusing on cyber defense, cybercrime, cybersecurity ecosystem, and national security integration with cybersecurity.

In 2019, the Presidential Circular on Information Security Measures [29] reinforced the importance of cybersecurity for the country and outlined the measures necessary to protect sensitive information. The most recent strategy document, the National Cybersecurity Strategy and 2020-2023 Action Plan [30], focuses on critical infrastructures, improving national capabilities, combating cybercrime, promoting the use of secure digital technologies, and establishing international cooperation.

In conclusion, the historical development of Turkish cybersecurity strategies reflects the country's growing recognition of the importance of protecting its citizens, businesses, and critical infrastructure from cyber threats. The successive strategy documents have evolved to address changing threats and technologies, reflecting the country's commitment to staying ahead of the curve in the rapidly evolving world of cybersecurity.

Türkiye's efforts to strengthen its cybersecurity posture have been reflected in the numerous initiatives launched over the years. In the following sub-titles, brief information is given for initiatives to better understand the evolution of Türkiye's cybersecurity strategies.

4.1. Prime ministry circular no. 2003/10 (2003)

Prime Ministry Circular dated 17 February 2003 and numbered 2003/10 can be accepted as one of the first initiatives to set a strategy for communication and information security and the protection of personal privacy in Türkiye [4]. Adoption of the guidelines prepared by the OECD was adopted by the Circular.

The Guidelines recommend establishing a culture of security among users of information and communication technologies, raising awareness on this issue, establishing a general reference framework for security, developing security practices, measures and procedures, and establishing standards by performing risk management [9].

4.2. E-Transformation Türkiye project (2003)

e-Transformation Türkiye Project was initiated by the former Prime Ministry to make maximum use of ICT in the country, to provide citizens with fast and quality public service, and to rearrange the relevant legislation in line with the EU acquis [23].

In the project, the basic steps that Türkiye should take in the EU membership candidacy process were discussed. It is aimed to contribute to the transparent management of the public administration, to develop and expand the use of information and communication infrastructure and technologies, to prevent waste by carrying out investment projects in a coordinated manner and to use these technologies safely and securely.

4.3. E-Transformation Türkiye project action plans (2003 and 2005)

The first short-term action plan in the purview of e-Transformation Türkiye Project was put into practice with the Prime Ministry Circular dated 4 December 2003 and numbered 2003/48 [24]. The second short-term action plan was published on March 24, 2005 [31].

Short-term action plans are discussed under eight headings (Information Society Strategy, Information Security and Technical Infrastructure, Human Resources and Education, Legal Framework, Standards, e-Government, e-Health and e-Commerce). The topic titled “Technical Infrastructure and Information Security” is directly related to cybersecurity. However, there are action clauses on cybersecurity under other headings as well. In this context, actions for cybersecurity are listed below:

- Conducting information security risk analysis to public institutions

- Working on the use of smart cards in public

- Development of pilots for testing and ensuring network security

- Expanding the internet infrastructure and producing solutions for its security
- Examining the usage of open-source software in government

- Raising awareness in society about safe internet use

- Enactment of the law on cyber crimes

- Combating unwanted electronic communications

- To carry out legal studies in order to protect sensitive information for national security (enactment of the National Information Security Law)

- Public information systems emergency management

4.4. Information society strategy and action plan 2006-2010 (2006)

Information Society Strategy and Action Plan 2006-2010 was published in the Official Gazette on July 28, 2006, and entered into force [25]. A total of seven main themes in the strategy (Social

Transformation, Impact of ICT in the Business World, Citizen-Oriented Service Transformation, Modernization in Public Administration, Global Competitive Information Technologies Sector, Competitive, Widespread and Cheap Communication Infrastructure and Services, Development of R&D and Innovation) with 111 action items were targeted.

Among the action plans, those related to cybersecurity are listed below:

- Internet Security

- e-Commerce Security Infrastructure

- Public Website Standardization and Hosting Service

- Public Safety Net

- Public Utilization Open-Source Software

- Information Systems Disaster Management Center

- Increasing the Use of e-Signature

- Legal Regulations Regarding Information Security

- National Information Systems Security Program

Ensuring a secure internet environment, establishing a secure communication network between public institutions, safeguarding the protection of national security information, legislative efforts for the protection of personal data, establishing a central structure (Computer Emergency Response Team-CERT) under TUBITAK to respond to computer incidents across the country, determining the cybersecurity levels of public institutions and eliminating their deficiencies and determining the minimum security levels on the basis of public organizations are among the most important targets for cybersecurity.

4.5. National cybersecurity strategy and 2013-2014 action plan (2013)

The previous strategy documents mainly contain objectives for the dissemination of ICT, and cybersecurity is considered as one of the secondary steps. The National Cyber Security Strategy and 2013-2014 Action Plan is the first nationwide document on cybersecurity on its own. The Cyber Security Council was established prior to the publication of this document by a Council of Ministers Decision released in Official Gazette No. 28447 on October 20, 2012 [26].

The Cyber Security Council, in collaboration with public and non-governmental organizations (NGOs), developed the strategy and action plan, which were publicized in the Official Gazette with the resolution of the Council of Ministers dated June 20, 2013, and numbered 28683 [32].

The action plan's goal is to create the legislative foundation for cybersecurity to maintain the security of critical infrastructures run by the public or private sectors, to protect the systems used in the services provided by public organizations and the data kept here, to develop cybersecurity technologies and to train human resources in this field.

The action plan includes 29 action items and 95 sub-action items under seven main topics. The main topics in the action plan are:

1. Making legal arrangements

2. Carrying out studies to assist the judicial processes

3. Creating a national-level organization for cyber incident response

4. Increasing the resiliency of the national cybersecurity infrastructure

5. Human resource development in the field of cybersecurity

6. Development of domestic cybersecurity technologies

7. Increasing the breadth of national security safeguards

With this strategy and action plan, it has been decided to establish the National Cyber Incidents Response Center (Turkish: Ulusal Siber Olaylara Müdahale Merkezi-USOM), which works on a 7x24 basis, instead of CERT, which was decided to be established within TÜBİTAK. USOM was established under the Information and Communication Technologies Authority (Turkish: Bilgi ve İletişim Teknolojileri Kurumu-BTK) according to the Communique on the Procedures and Principles Regarding the Establishment, Duties and Operations of Cyber Incidents Response Teams dated 11 November 2013 and numbered 28818 [33].

4.6. Information society strategy and action plan 2015-2018 (2015)

Türkiye's Information Society Strategy and Action Plan covering the period of 2015-2018 was released in the Official Gazette dated 6 March 2015 and numbered 29287 [27]. In the strategy and action plan, under eight main objectives (ICT sector, Sectoral competitiveness and broadband connectivity, Skilled manpower, ICT uptake, User trust and information security, ICT-enabled innovative techniques, Digital entrepreneurship and e-commerce, Public service efficiency), a total of 72 action items were arranged. Action items with cybersecurity are:

- Enactment of the Cyber Security Law

- Enactment of personal data protection legislation

- Creation of Cybercrime Strategy and Action Plan

- Raising awareness on secure internet use

- Establishment of Specialized Computer Crimes Courts

It is seen that the action plan focuses on legal issues in terms of cybersecurity, apart from the issue of secure internet use.

4.7. National cybersecurity strategy and 2016-2019 action plan (2016)

A committee comprised of members from government organizations, academia, NGOs, and private sector officials produced the National Cybersecurity Strategy and Action Plan 2016-2019 under the direction of the defunct Ministry of Transport, Maritime Affairs, and Communications. Even though the strategy document was published, since the action plan was classified, it was not shared with the public but relevant government organizations [28].

The strategic objectives determined to minimize the risks in the cyberspace and to provide a secure national cyberspace are as follows [28]:

- Creating a national critical infrastructure catalog, achieving critical infrastructure security criteria, and having these critical infrastructures audited by the regulatory organizations with whom they are affiliated.

- Establishment of legislation in line with international standards, including the audit approach in the field of cybersecurity.

- Developing the awareness and competencies with respect to regulatory and supervisory capabilities of organizations such as sector regulatory bodies and ministries.

- Creating regulations to safeguard organizations' information systems not just from cyberattacks, but also from human mistakes and mishaps.

- The ability of any organization to conduct its own information security management procedures.

- Increasing cybersecurity awareness among business leaders.

- Educating competent individuals in cybersecurity and encouraging workers, academics, and students that desire to specialize in this sector.

- Increasing cybersecurity awareness throughout society by conducting awareness campaigns in

the written and visual media, in addition to the actions of educational institutions.

- Providing legislative support for the employment of expert personnel in cybersecurity in government institutions and improving the personnel rights of the employees.

- Increasing the efficiency of institutional and sectoral CERTs by supplying assistance, producing financial adjustments, satisfying the need for skilled staff, setting up information infrastructure, and enhancing information exchange within the purview of the national incident response institution.

- Establishing a strong central governmental power to enforce cybersecurity coordination.

- Establishing a national cybersecurity ecosystem with wide participation from all of the stakeholders.

- Dissemination of best practices across the ecosystem for national cybersecurity, establishing consultancy services, vulnerability and threat information sharing, and application sharing.

- Conducting vulnerability research and certification studies to avoid the exploitation of vulnerabilities in local or foreign software and hardware items utilized in crucial components of computer systems.

- Establishing a culture of secure software development and supply management.

- Developing domestic products by attaching importance to R&D activities in order to reduce foreign dependency in cybersecurity.

- Development of national proactive cyber defense capabilities to prevent attackers before they strike.

- Deploying effective event management and IPv6 technology to prevent anonymity.

Actions to be taken to achieve the stated strategic goals are grouped under five strategic action titles:

1.Improving Cyber Defense and Critical Infrastructure Protection: It was planned to take actions to threats that may affect society, infrastructures and national economy.

2. Fighting Against Cybercrime: It was planned to take actions aimed at eliminating the threats causing financial losses that affect citizens and organizations.

3. Awareness and Human Resources Development: It was planned to carry out actions aimed at bringing a culture of cybersecurity to all segments of society, from corporate managers to computer users, and to train cybersecurity experts.

4. Developing a Cybersecurity Ecosystem: It was planned to take actions to determine and implement the requirements for all aspects of cybersecurity with the participation of all necessary stakeholders.

5. Integration of Cybersecurity into National Security: It was planned to take actions to reduce the damage that can be caused by deliberate attacks.

4.8. Presidential circular on information security measures (2019)

The Presidential Circular on Information Security Measures was published in the Official Gazette No. 30823 on July 6, 2019, with the goal of reducing and neutralizing security risks for information and information systems in the digital environment, as well as ensuring the security of key data types that may lead to serious consequences or disrupt social stability, especially when their security is compromised [29].

The circular consists of 21 articles in total. It was decided to create an Information and Communication Security Guide. Apart from the duties and activities performed for protecting national security and confidentiality, it was obligatory to comply with the procedures and principles included in the guide in the information systems to be established in all government organizations and enterprises providing critical infrastructure services. The

systems should be audited at least once a year, and the results should be reported to the Presidency Digital Transformation Office.

4.9. National cybersecurity strategy and 2020-2023 action plan (2020)

National Cybersecurity Strategy and 2020-2023 Action Plan was enacted with the Presidential Circular No. 2020/15 and the Official Gazette dated 29 December 2020 and numbered 31349 [30]. The strategy was released under the supervision of Ministry of Transport and Infrastructure, and the action plan was shared with only accountable and relevant government entities and organizations [34]. The following eight strategic objectives have been adopted in the document:

1. Securing critical infrastructure and enhancing resiliency

2. Building national capability

3. Creating an organic cybersecurity infrastructure

4. Providing security for emerging technologies

5. Combating cybercrime

6. Creation and promotion of national cybersecurity technologies

7. Integrating cybersecurity into national security

8. Developing international cooperation

According to the strategy document, cybersecurity is accepted as an essential component of national security, it was emphasized that transparency, accountability and ethical values should be taken into account while fulfilling the responsibilities for cybersecurity. It was also stated that the services provided through critical infrastructures should be provided uninterruptedly and effectively. Providing legal framework and the principle of using national products and services have been adopted by making the necessary investments.

The objectives set in the strategy are:

- Protecting critical infrastructures continuously.

- Possessing state-of-the-art cybersecurity technology.

- Creating in-house technological opportunities to meet operational requirements.

- Adopting proactive cyber defense and taking steps against cyber incidents.

- Measuring and monitoring the competency levels of CERTs.

- Improving the capabilities of cybersecurity manpower for incident response.

- Adopting risk analysis-based planning and enhancing the institutional, sectoral and national capabilities to deal with cyber incidents.

- Providing data sharing mechanisms within the cybersecurity ecosystem.

- Keeping the traffic domestic whenever the source and target of the data are domestic.

- Development of a cybersecurity approach based on regulation and supervision in critical infrastructure sectors.

- Preventing manufacturer dependency in IT products in critical infrastructure sectors.
- Determining the requirements for ensuring the security of emerging technologies.

- Incentivizing R&D and innovation to create national technologies and products.

- Maintaining secure use of cyberspace by society.

- Increasing citizens' cybersecurity awareness.

- Creating information security culture within organizations.

- Protecting children in the online environment.

- Enhancing the skills of cybersecurity manpower.

- Expanding cybersecurity education in formal and non-formal education and enriching the educational content.

- Creating venue for national and international secure information sharing.

- Reducing cybercrime and boosting cyber deterrence.

- Creating systems to ensure the distribution of correct and up-to-date information on social media and the internet.

5. Findings and Discussion

As mentioned in the literature review, research and guidance documents from leading organizations were analyzed to determine the scope, content and objectives of the NCSSs around the world. In the analysis for Türkiye, only the documents that directly target the cybersecurity strategy were included for the comparison. These documents are National Cybersecurity Strategy and 2013-2014 Action Plan, National Cybersecurity Strategy and 2016-2019 Action Plan, and National Cybersecurity Strategy and 2020-2023 Action Plan.

In terms of scope and content of the Turkish NCSSs, 10 criteria have been extracted from the referenced sources as shown in Table 2.

Table 2. Comparison of Content and Scope of the Turkish NCSSs

No	Topic	International Guides	Str2013	Str2016	Str2020
1	Standards and Technical Measures	G2-G12	+	+	+
2	Legal and Regulatory Measures	G1-G4, G6-G8, G10, G12	+	+	+
3	Cyber Incident Response	G1-G8, G10-G12	+	+	+
4	Developing Cybersecurity Capacity	G1-G3, G5-G12	+	+	+
5	Raising Cybersecurity Awareness	G1-G3, G5-G12	+	+	+
6	Organizational Measures	G1-G4, G6-G8, G10, G12		+	
7	R&D and Innovation	G2, G3, G6-G10, G12	+	+	+
8	Cybersecurity Sector	G2-G10, G12			+
9	International Cooperation and Partnership	G1-G12	+	+	+
10	Domestic Cooperation and Partnership	G1-G10, G12	+	+	+

According to the results of the comparison, the first strategy (Str2013) covers all but organizational measures and cybersecurity sector. The second strategy (Str2016) covers all but the cybersecurity sector. The last strategy (Str2020) covers all but organizational measures and actions for cybersecurity sector were addressed in this strategy. In short, it can be suggested that Turkish NCSSs cover most of the scope and content of the contemporary NCSSs, while there are shortcomings in terms of organizational measures and cybersecurity sector-related actions.

In terms of the objectives given in the Turkish NCSSs, 28 criteria have been extracted from the referenced sources as shown in Table 3.

The objectives in Table 3 were sorted out based on the number of referenced sources. Even if the number of sources is only one for the last six objectives, it should not be overlooked that these sources contain the common objectives of many countries. Therefore, one should not be mistaken that objectives from fewer sources are less important. According to the results of the comparison, Str2013 covers 16 (57%) of the common objectives, while Str2016 covers 18 (64%) and Str2020 covers 20 (71%).

Table 3. Comparison of Objectives of the Turkish NCSSs

No	Objective	International Guides	Str2013	Str2016	Str2020
1	Raise awareness	G1-G3, G5-G11	+	+	+
2	Strengthen training and educational programs	G1-G3, G-11	+	+	+
3	Engage in international cooperation	G1-G3, G5-G10	+	+	+
4	Establish a public-private partnership	G1-G3, G5-G8, G10	+	+	+
5	Establish incident response capacity	G2, G3, G5-G8, G10, G11	+	+	+
6	Address cyber crime	G2, G3, G5-G8, G10, G11		+	+
7	Foster R&D and innovation	G2, G3, G6-G10	+	+	+
8	Protect critical infrastructures	G2, G5-G8, G10, G11	+	+	+
9	Develop cybersecurity contingency plans	G2, G3, G6-G8, G10			
10	Organize cybersecurity exercises	G3, G5, G7-G10	+		+
11	Establish baseline security measures	G3, G6-G10			
12	Develop a clear governance structure	G1-G3, G5, G8		+	
13	Follow a national risk assessment approach	G2, G3, G7, G8	+	+	+
14	Recognize and protect individual rights (Balance security with privacy)	G3, G7, G8, G10	+	+	
15	Identify and engage stakeholders	G2, G3, G5, G7		+	+
16	Support private cybersecurity sector	G5, G7, G9, G10	+	+	+
17	Respect for fundamental values	G1, G5, G6	+	+	+
18	Establish and implement legislative framework	G1, G2, G6	+	+	+
19	Increase national cooperation	G7, G8, G10	+	+	+
20	Set the vision, scope, objectives and priorities	G2, G3	+	+	+
21	Establish trusted information sharing mechanisms	G3, G8			+
22	Protect national digital information resources	G6, G10			+
23	Adjust the national cybersecurity strategy	G3	+	+	+
24	Protect children online	G5			+
25	Allocate dedicated budged and resources	G8			
26	Create compliance mechanisms	G8			
27	Improve cybersecurity supply chain	G10			
28	Evaluate security level	G3			

In Turkish NCSSs, there are some objectives that were not captured in the referenced sources but are unique and specific to Türkiye, which are given in Table 4.

As it is seen in Table 4, integrating cybersecurity into broader national security is a common unique objective of all three NCSSs, and the most recent strategy covers several unique objectives while also covering the majority of the common objectives. Even though some of the objectives were not directly mentioned in the Turkish NCSSs, there are still regulations and actions taken to address those objectives. Developing cybersecurity contingency plans [35], establishing baseline security measures [29], supply chain security, evaluation and compliance [29] are all addressed by government regulations.

It is suggested that a good strategic plan, if implemented with adequate budget and sufficient resources, provides significant benefits to organizations [35, 36]. Similarly, since the level of cybersecurity capabilities at a national level is a result of national strategies and action plans, it can be suggested that good strategies directly affect the success of the cybersecurity posture, together with the will and aspiration to perform written actions.

The Global Cybersecurity Index (GCI), developed by the ITU to assess the countries' commitment to cybersecurity, is one of the

measures to assess the success of national level cybersecurity strategies. GCI is a composite index with five pillars: 1) Legal measures, 2) Technical measures, 3) Organizational measures, 4) Capacity building, and 5) Cooperation [37]. Türkiye, which was 22nd in 2014 [38] but regressed to 43rd in 2017 [39]. It rose to the 20th rank in 2018 [40] and achieved the success of rising to the 11th rank among 194 countries in the latest GCI index, which was conducted in 2020 [41]. Since the content and scope of the common NCSSs as given in Table 2 cover the pillars of GCI, Türkiye's approach to cybersecurity strategies can be deemed successful from the scope and content perspectives.

Table 4. Unique and Specific Objectives in Turkish NCSSs

NCSS	Objectives
Str2013	Integration of the cybersecurity into national security
Str2016	Recruiting specialists in government organizations with better rights
	Creating national cybersecurity ecosystem
	Secure software development and procurement
	Improving proactive cyber defense capability
	Deployment of IPv6 protocol
	Integration of the cybersecurity into national security
Str2020	Improving proactive defense mindset
	Keeping domestic internet traffic within country
	Preventing manufacturer dependency in IT products in critical infrastructures
	Determining the requirements for ensuring the security of new generation technologies
	Minimizing cybercrime and increasing deterrence
	Organic cybersecurity network
	Security of new generation technologies
	Integration of the cybersecurity into national security
	Development and support of domestic and national technologies

6. Conclusion

National cybersecurity strategies provide guidance and framework for cybersecurity related actions and issues in countries. A lot of countries developed their strategies to prevent attacks, decrease risks, deter attackers, and provide secure and available cyberspace to foster technology, economy, business and prosperity.

Organizations such as ITU, ENISA, OECD, e-GA, NATO and Oxford University published research and guidance documents by eliciting the best practices from several countries to assist the nations in developing their strategies. Based on the criteria derived from the worldwide research and studies, the scope, content and objectives of Türkiye's cybersecurity plans were examined in this article.

Turkish cybersecurity related strategies appeared in the early 2000s under the strategies addressing e-transformation and information society. The first strategy directly dedicated to cybersecurity was published in 2013 and then updated in 2016 and 2020. All three strategies cover most of the scope and content of the common NCSSs while lacking organizational and cybersecurity sector-related measures.

From the perspective of common objectives, Turkish strategies include most of the common objectives, while some of them (establishing trusted information sharing, protecting national digital information resources, budget and resource allocation, compliance mechanisms, supply chain security and evaluation) are not directly cited in the documents. Apart from the common objectives, Türkiye has specific objectives and supplementary directives that improve the cybersecurity posture.

National cybersecurity is such a complicated subject that no single solution can be viewed as a universally applicable across all countries and all local situations [7], and therefore there isn't a single policy solution for cybersecurity that works in every circumstance [13]. Based on the comparisons in this paper and Türkiye's rankings in ITU's GCI, it can be concluded that Turkish cybersecurity strategies are among the examples of successful ones in terms of scope, content and objectives, even though there are topics, as identified in this paper, that should be addressed.

This study does not evaluate either the outcomes of the strategies and action plans or whether the actions were performed successfully or not. A further study should be conducted to find out the

success of the implementation of the actions aimed in the strategies.

Article Information Form

Funding
The author has not received any financial support for the research, authorship or publication of this study.

Authors' Contribution
This article was written by the single author.

The Declaration of Conflict of Interest/ Common Interest
No conflict of interest or common interest has been declared by the authors.

The Declaration of Ethics Committee Approval
This study does not require ethics committee permission or any special permission.

The Declaration of Research and Publication Ethics
The authors of the paper declare that they comply with the scientific, ethical and quotation rules of SAUJS in all processes of the paper and that they do not make any falsification on the data collected. In addition, they declare that Sakarya University Journal of Science and its editorial board have no responsibility for any ethical violations that may be encountered, and that this study has not been evaluated in any academic publication environment other than Sakarya University Journal of Science.

References

[1] ITU, "Definition of cybersecurity," 2022. https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

[2] NIST, "Cybersecurity," 2022. https://csrc.nist.gov/glossary/term/cybersecurity

[3] F. Wamala, "ITU National Cybersecurity Strategy Guide," 2011. [Online]. Available: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf

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

[5] E. Abdurahmanlı, "Siber İstihbarat Kapsamında: Echelon İstihbarat Sistemi," Academic Journal of History and Idea, vol. 8, no. 3, pp. 1212–1234, 2021.

[6] D. Štitilis, P. Pakutinskas, U. Kinis, and I. Malinauskaite, "Concepts and principles of cyber security strategies," Journal of Security Sustainability Issues, vol. 6, no. 2, pp. 199–210, 2016.

[7] NATO CCD COE, "National Cyber Security Framework Manual," NATO CCD COE Publications, Tallinn, 2012.

[8] ENISA, "National Cyber Security Strategies," 2012. [Online]. Available: https://www.enisa.europa.eu/publications/cyber-security-strategies-paper

[9] OECD, "OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security," 2002. [Online]. Available: https://www.oecd.org/sti/ieconomy/15582260.pdf

[10] The White House, "The National Strategy to Secure Cyberspace." 2003. [Online]. Available: https://georgewbush-whitehouse.archives.gov/pcipb/

[11] ENISA, "National Cyber Security Strategies - Practical Guide on Development and Execution," 2012. [Online]. Available: https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide

[12] OECD, "Cybersecurity Policy Making at a Turning Point - Analyzing a new generation of national cybersecurity

strategies for the internet economy," 2012. doi: 10.1787/5k8zq92vdgtl-en.

[13] ENISA, "An Evaluation Framework for National Cyber Security Strategies," 2014.

[14] ENISA, "NCSS Good Practice Guide: Designing and Implementing National Cyber Security Strategies," 2016

[15] ITU, "Guide to Developing a National Cyber Security Strategy - Strategic Engagement in Cybersecurity," Geneva, 2018. [Online]. Available: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

[16] ENISA, "Good Practices in Innovation Under NCSS," 2019.

[17] The European Parliament, Network and Information Security Directive, no. July. EU, 2016. [Online]. Available: https://www.enisa.europa.eu/topics/nis-directive

[18] ENISA, "National Capabilities Assessment Framework," The European Union Agency for Cybersecurity (ENISA), 2020.

[19] T. Vaks, E. Maaten, O. Gross, E. Neeme, L. Luht, and K. Rousku, "National Cyber Security in Practice." e-Governance Academy, Tallinn, 2020. [Online]. Available: https://ega.ee/wp-content/uploads/2020/05/Kuberturvalisuse_kasiraamat_ENG.pdf

[20] Oxford GCSCC, "Cybersecurity Capacity Maturity Model for Nations (CMM)," 2021. [Online]. Available: https://gcscc.ox.ac.uk/the-cmm

[21] H. Çakır and S. A. Uzun, "Türkiye'nin siber güvenlik eylem planlarının değerlendirilmesi," Ekon. İşletme Siyaset ve Uluslararası İlişkiler Dergisi, vol. 7, no. 2, pp. 353–379, 2021.

[22] TÜBİTAK-BİLGEM, "Tarihçe," 2022. https://uekae.bilgem.tubitak.gov.tr/tr/kurumsal/tarihce

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

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

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

[26] Council of Ministers, Decision on the Execution, Management and Coordination of National Cybersecurity Studies. 2012. [Online]. Available: https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf

[27] Ministry of Development, 2015-2018 Information Society Strategy and Action Plan. 2015. [Online]. Available: 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. [Online]. Available: https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf

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

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

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

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

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

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

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

[36] M. J. B. Kabeyi, "Organizational strategic planning, implementation and evaluation with analysis of challenges and benefits for profit and nonprofit organizations," International Journal of Applied Research, 2019.

[37] ITU, "GCI scope and framework," 2019. [Online]. Available: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv4/New_Reference_Model_GCIv4_V2.pdf

[38] ITU, "Global Cybersecurity Index (GCI) 2014," 2014. [Online]. Available: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf

[39] ITU, "Global Cybersecurity Index (GCI) 2017," 2017. [Online]. Available: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf

[40] ITU, "Global Cybersecurity Index (GCI) 2018," 2019. [Online]. Available: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

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