NATIONAL CYBER SECURITY STRATEGY

2020-2023

REPUBLIC OF TURKEY
MINISTRY OF TRANSPORT
AND INFRASTRUCTURE

NATIONAL CYBER SECURITY STRATEGY

2020 - 2023

Technological developments take an important place in our efforts towards development and growth pursued with national unity and solidarity. Those developments occur at a great pace in every field of life including public services ranging from economy to health, from education to transport.

While on one hand the information and communication technologies offer many possibilities as it continuously progresses and advances and becomes an integral part of our lives, on the other hand, it also brings along cyber security risks. Ensuring national cyber security -which is an integral part of our national security- is a priority for us; and we maintain our unrelenting efforts against cyber threats. Within this framework, taking into account the emerging national needs and technological developments and in cooperation with public institutions, private sector, non-governmental organizations and universities; the National Cyber Security Strategy and Action Plan (2020-2023) has been prepared by Ministry of Transport and Infrastructure.

In line with our 2023 objectives, we will carry our country's leading position even further in cyber security, as so we do in other fields; and we will determinedly continue our struggle against cyber threats 24/7 with our cyber security organization while employing our national and domestic technologies.

For a "Strong and Great Türkiye" who uses technology with confidence...

Congratulations to our Country and Nation on the new National Cyber Security Strategy and Action Plan (2020 – 2023).

Recep Tayyip ERDOĞAN

President of the Republic of TÜRKİYE

Information and communication technologies facilitate access to information, make daily lives more comfortable, create increasingly greater impacts on economy and social life. Many important services are delivered to our citizens through those technologies, processes and transactions are performed faster and more practically on electronic environment. Secure use of the information and communication technologies integrated in every parts of our lives, has emerged as an extremely critical matter. In this context, an efficient and strong cyber security perception plays an important role in economic growth and social wealth of countries. Significant studies have been realized within scope of the previous National Cyber Security Strategy and Action Plans covering the periods of 2013-2014 and 2016-2019 which we -Ministry of Transport and Infrastructure- have published until today. In line with the vision and objectives set forth by Mr. President of the Republic, we will perform our activities resolutely and determinedly by continuously increasing our knowledge, experience and capacity in order to further our achievements in cyber security field. In this context, National Cyber Security Strategy and Action Plan (2020-2023) has been prepared in order to support the economic development of our country, the protection of social life and the national security, as well as our Country to become an international brand in cyber security field.

Our nation's cyber security will be contributed greatly as result of completing the actions and achieving the goals of National Cyber Security Strategy and Action Plan (2020-2023) by institutions and organizations, and conducting activities with efficient communication and cooperation between all stakeholders.

I wish the efforts towards our Country's and Nation's security to be conducted within scope of National Cyber Security Strategy and Action Plan (2020-2023) to be auspicious, and want to thank everyone who contributed to the preparation of the Action Plan.

Adil KARAİSMAİLOĞLU

Minister of Transport and Infrastructure

CONTENT

1. EXECUTIVE SUMMARY **5**

2. DEFINITIONS **8**

3. INTRODUCTION **11**

4. CYBER SECURITY IN TÜRKİYE **13**

5. VISION AND MISSION **16**

6. METHOD **17**

7. PRINCIPLES **18**

8. OBJECTIVES **20**

9. STRATEGIC OBJECTIVES **22**

I. Protecting Critical Infrastructure and Increasing Resilience 23

II. National Capacity Building 24

III. Organic Cyber Security Network 25

IV. Security of New Generation Technologies 26

V. Fighting against Cybercrime 26

VI. Developing and Fostering Domestic and National Technologies 26

VII. Integrating Cyber Security into National Security 27

VIII. Improving International Cooperation 28

10. REALIZATION APPROACH **29**

10.1. Action Plan 29

10.2. Monitoring and Measurement 29

10.3. Stakeholders 30

10.4. Scope 30

10.5. Updates 30

10.6. Relation between Strategic Objectives and Actions 31

1. EXECUTIVE SUMMARY

Making the most of the advantages that the information and communication technologies offer, depends on performing the cyber security related activities in an efficient and continuous manner. The security of our citizens, institutions, sectors, namely the security of our national cyber environment against cyber threats which are structurally changing, evolving, complexifying and increasing in amount, plays a key role in our country's economic growth. During and after the global pandemic period, visible changes took place in economic and social lives and accelerated the dynamics of technological transformation; which increased the cyber security requirements in terms of infrastructure, new technologies, human resources and awareness.

Raising the bar in national cyber security each passing day is only possible through strong cyber strategies. National Cyber Security Strategy and Action Plan (2020-2023), focuses on the policies related to the next 4-year period in line with our country's cyber security vision and mission, and aims to even further the achievements realized through previous strategies. National Cyber Security Strategy and Action Plan (2020-2023) has been prepared to make the moves to carry forward our national cyber security and realize related activities. For this reason, the goals were determined by diligently taking into account the impacts of technological developments, trends in cyber threats, national needs and international practices. After determining the requirements to reach such goals and activities to be conducted, studies were completed.

The actions of continuous nature realized in 2013-2014 and 2016-2019 periods, were revisited and necessary improvements were made. In this framework, the determined strategic objectives were gathered in 8 main subjects:

I. Protecting Critical Infrastructure and Increasing Resilience

II. National Capacity Building

III. Organic Cyber Security Network

IV. Security of New Generation Technologies

V. Fighting against Cybercrime

VI. Developing and Fostering National and Domestic Technologies

VII. Integrating Cyber Security into National Security

VIII. Improving International Cooperation

In order to determine the actions to realize the achievements planned in line with strategic objectives, a preparatory workshop was held in 19 February 2020 attended by 127 participants from 67 institutions.

Action plan includes 40 actions and 75 sub-actions related to the 8 strategic objectives determined in light of the conducted activities and the Workshop, which will be implemented by institutions and organizations. It is aimed to even further raise the cyber security level by improving processes, harnessing technological components at a maximum and developing human resources. In line with this; actions were determined related to the regulation of protecting the critical infrastructure sectors, developing cyber risk management and emergency plans, ensuring that the domestic-sourced and inward bound internet traffic to remain within borders and addressing cyber security as a national security issue. Furthermore, it is aimed to increase human resources on relevant issues through realizing the actions which focus on measuring, monitoring and increasing the maturity levels of cyber emergency response teams (CERTs), developing the trainings provided by the institutions competent in the field of cyber security and enriching and disseminating the content of cyber security materials in primary, secondary and higher education. It is aimed to securely adapt and use the new generation technologies such as 5G, internet of things and cloud computing in our country. The organic cyber security network framework, planned to be created, aims to develop high-level expertise projects, and increase knowledge sharing between institutions/persons operating in this field and the National Computer Emergency Response Team of Türkiye (USOM), and expand it nationwide. The technological achievements will be increased with the actions aiming to support the efforts of the private sector to develop national and domestic cyber security technologies. Moreover, it is of great importance to develop international cooperation along with national activities considering the nature of cyber security. Within this framework, efforts will be made to increase bilateral and multilateral collaborations and develop knowledge sharing, and contributions will be made for the activities to establish international joint requirements and standards in cyberspace.

Besides, under the strategic objectives, the institutions and organizations responsible for implementing each action, sub-actions and time periods for realizing them have also been determined.

With the National Cyber Security Strategy and Action Plan (2020-2023), in which the scope of the studies related to ensure the national security defined, it is aimed to transform the 2023 vision of Türkiye into reality in this field.

2. DEFINITIONS

One of the key issues for ensuring cyber security, which is a multi-stakeholder and inter-disciplinary topic, is establishing the common terminology. Providing common definitions about cyber security, contributes to the development of communication between stakeholders. In line with that, definitions within the scope of the Strategy and Action Plan are as below:

Advanced Persistent Threat (APT): Threat which is developed with advanced knowledge and techniques and can use multiple attack vectors to reach its purpose.

Availability: Feature of data/information being available and usable on demand by an authorized entity.

CERT: Computer Emergency Response Team

Confidentiality: Feature of data/information of being unavailable, unusable, unstorable, or unrecordable in other environments or undisclosable by authorized persons, entities or processes.

Critical Infrastructure: Infrastructures that incorporates information technologies that may cause loss of life, economic harm of large-scale, national security gaps and public disorder when the confidentiality, integrity and availability of data/ information is disrupted.

Critical Infrastructure Sector: “Electronic Communications”, “Energy”, “Finance”, “Transport”, “Water Management”, and “Critical Public Services” sectors, specified as per the decision (dated 20 June 2013 numbered 2) of the repealed Cyber Security Council.

Cyber Attack: Intentional actions done by persons and/or information technologies from any point of the cyberspace, against the confidentiality, integrity or availability of information technologies, industrial control systems or the information/data processed by those systems within the cyberspace.

Cyber Incident: Violation of confidentiality, integrity or availability of information technologies and industrial control systems or the information/data which are processed by those systems.

Cyber Risk: Potential of cyber threats to create damage by using the vulnerability in one or multiple information assets. Combination of possibilities related to the negative consequences of cyber incidents.

Cyber Security: All activities that involves protecting the information technologies which constitutes the cyberspace from attacks, ensuring the confidentiality, integrity and availability of those systems, detecting attacks and cyber incidents, activating response mechanisms against those, and restoring the systems back to pre-cyber incident conditions.

Cyber Threat: Potential reason of an unwanted cyber incident that might result in the damage of an institution or a system.

Cybercrime: Crime targeting the security, related data or users of an information system, and being committed using information technologies.

Cyberspace: All systems and services directly or indirectly connected to internet, telecommunication and computer networks.

Digital Forensics: Field of science which involves the digital evidence of cybercrime to be collected, evaluated, documented, classified without being disrupted; and the mentioned data to be used in judicial process.

Honeypot: Hardware and software infrastructure which are used for detecting threats and attacks by directing them into trap systems of the same architecture with real system servers.

ICS (Industrial Control Systems): Control systems, including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) used in industrial stages (e.g. manufacturing, product processing and distribution)

Information Asset: Data that has value to individuals or organizations; and the systems, software, IT equipment and business processes through which the mentioned data is carried, stored, transmitted and processed.

Information Security: All activities conducted to prevent unauthorized use, access, disclose, erasion, change and harm of/on information technologies and information, and ensure that those systems and information are available to authorized persons and processes when necessary and with required quality.

Integrity: Feature of protecting the accuracy and completeness of information/ data.

ISMS (Information Security Management System): All systematic, planned, manageable, sustainable, documented and approved activities of the institution/ organization, which are based on the international security standards and aim to provide confidentiality, integrity and availability of information.

IXP (Internet Exchange Point): Network infrastructure that provides connection between at least two independent autonomous systems and facilitates internet traffic exchange.

KamuNet (Public Virtual Network): Private network infrastructure for public institutions and organizations to provide services, processes and data traffic.

Pentest: Test for seeking the ways to by-pass security measures of information technologies or networks, and identifying system vulnerabilities by penetrating the system.

Risk Management: According to certain standards and methodologies, identifying and evaluating the risk that may impact the business processes, activating the required controls, policies and procedures, and preventing/minimizing, monitoring and reviewing possible losses.

SCADA: Supervisory Control and Data Acquisition

SOC: Cyber Security Operation Center

USOM: National Computer Emergency Response Team of Türkiye (TR-CERT)

Vulnerability: Weaknesses of assets in cyberspace that can be used by cyber threats.

Zero-Day Vulnerability: Type of vulnerabilities on hardware, operation system or applications, for which there is no existing patch or update published, and that remains unknown until it reveals its attack method.

3. INTRODUCTION

The basic dynamic of technology is the change and development which happens fast and continuously. Those game-changer technological components/products spreading at a great pace, become an integral part of everyday life. Those developments in information and communication technologies constitutes the basis of economic and social globalization.

The point which the number of internet users has reached is a striking example to this. According to the "Measuring Digital Development: Facts and Figures (2019)" study of International Telecommunication Union (ITU); 4.1 billion people, corresponding to %53,6 of world population as of the end of 2019, are internet users. According to the national statistics, Electronic Communication Sector 2nd Quarterly Report of the year 2020 published by Information and Communication Technologies Authority (BTK) states that the number of broadband internet subscribers was 6 million in 2008, and it has reached 78,4 million as of 2nd quarter of 2020. According to Turkish Statistics Institution data, internet usage percentage of 16-74 age range was about 79 per cent in 2020.

With increasing attention, the secure use of information and communication technologies has become a necessity not only in the country but also in the whole world. Security of those technologies which has become strategic tools especially for critical sectors, increasingly become more and more important each passing day.

Cyber risks and threats also undergo changes, become complex and increase in amount at the same speed as technological developments. Those threats have reached such a potential that would cause much more comprehensive and negative consequences compared to physical attacks and they have to be given serious consideration for the public safety and the stability of the states. Today, a simple software transferred via a small portable pen drive may become a major security problem. When the critical infrastructure sectors such as finance, electronic communication, water management, energy and transport deliver their service over a secure digital environment, financial losses are prevented and threats against human lives are eliminated.

The importance of cyber security has once again shown itself during the COVID-19 pandemic. During this period, from business environment to education, from social life to individual habits, many changes occurred in many aspects of life. During the pandemic, the possibilities that the information and communication technologies such as mainly the electronic trade, remote access and video-conference applications offer, have made it possible to work remotely and get education online, and with those measures taken, economic and social lives continued. On the other hand, fighting against cyber threats targeting those applications, coronavirus-related malwares and phishing attacks and cyber threats against critical infrastructure mainly of health sector, were one of the prominent issues during the pandemic. With the spread of the pandemic, countries have been introduced to the 'new normal' concept, as they made efforts to find a way to enable controlled social life while focusing on the security of digital life.

Providing a secure digital environment depends on the security of technology, human and process components. In line with this, the security criteria of new generation technologies such as artificial intelligence, internet of things, block chain and 5G will, along with the current technologies, play a major role in cyber security planning in the near future.

Cyber threats, as they increase in number and becomes more sophisticated, may cause disruptive consequences. This makes it essential to accurately plan resources while fighting against threats. Better analysis of risks and requirements, short and long-term plans based on predictions according to technological trends, will constitute the basis of a secure cyberspace.

4. CYBER SECURITY IN TÜRKİYE

While the continuous and swift development and change in information and communication technologies facilitates the lives of individuals and societies, cyber threats that are increasingly targeting critical sectors especially electronic communications, energy, finance, transport, water management, constitute risks against individual and social security.

Within this scope, the "security" context, which is a basic human need, should be considered in individual and social scale by taking into account the risks and threats.

Within this framework, ensuring the national cyber security, has become one of the prominent issues for the country as well.

Recent studies on ensuring cyber security in the country focuses on minimizing risks, and keeping them in manageable and acceptable levels. In this context, the tasks and responsibilities of *"determining the policy, strategy and objectives to ensure national cyber security, determining the rules and procedures on ensuring cyber security for public institutions and real and legal persons, preparing the action plans, coordinating the related activities, determining the critical infrastructures and their relevant institutions and positions, establishing and overseeing the required response center or have them established, conducting studies to produce and develop any kind of cyber response tools and national solutions or outsource or promote such efforts, conducting studies on cyber security awareness and trainings, preparing the rules and procedures for real and legal persons operating in the field* *of cyber security"* have been delegated to Ministry of Transport and Infrastructure as per Article 5 of Electronic Communication Law no.5809.

Furthermore, in accordance with the Presidential Decree no.1 published in the Official Gazette dated 10 July 2018 numbered 30474, the task of *"developing projects to strengthen information security and cyber security"* has been delegated to the Digital Transformation Office. Within this framework, with the Presidential Circular no. 2019/12, Information and Communication Security Measures was published.

With the provisions[1] added to Electronic Communication Law no. 5809 on 15 August 2016, BTK has been delegated the tasks of preventing cyber attacks and ensuring deterrence, and was authorized to sanction the parties who fails to fulfill such tasks.

"National Cyber Security Strategy and 2013-2014 Action Plan", which was the first strategy document in this field, was entered into force after being published in Official Gazette no. 28683 dated 20 June 2013. In this 2-year period, many studies were conducted on such as developing cyber security legislation, ensuring the security of critical infrastructure, raising cyber security awareness and detection and prevention of cyber threats.

Moreover, in the year 2013, USOM was established to operate under BTK, and Computer Emergency Response Teams (CERTs) came into operation notably in mentioned critical infrastructure sectors. By establishing the national cyber security organization, institutional and organizational structures of the country were strengthened.

With the "2016-2019 National Cyber Security Strategy and Action Plan" published thereafter, studies were conducted on strengthening cyber defense, protection of critical infrastructure, fighting against cybercrime, raising awareness and developing human resources, developing cyber security ecosystem and integration of cyber security into national security, in order to keep the cyber security risks in a manageable and acceptable level. Within this framework;

[1] Article 60 (11) The Authority, takes, or have it taken, any kind of measures to protect public institutions and real and legal persons against cyber attacks and provide deterrence.
(12) The Authority, can receive information, document, data and recordings from relevant places and evaluate them; can benefit from or contact with archives, electronic IT centers and communication infrastructures, and take or have necessary measures taken within this context. The Authority, for the performing those tasks specified in the paragraph, works in collaboration with institutions and organizations. Therefore, any demand by the Authority for information and documents, shall be fulfilled by institutions and organizations without delay. Rules and procedures on demanding/fulfilling documents and information is determined by the Presidential Office.
(13) Real persons and private legal persons, cannot avoid fulfilling the tasks specified in this Article and relevant demands by asserting justification from legislation provision to which they are subject. Those other than Operators, who fail to fulfill their liabilities related to Authority's tasks, will be sanctioned as per the 2nd paragraph of this article.

- Activities such as trainings, camps and competitions for building capacity in CERTs within scope of national cyber security capacity building program, and cultivating human resources required in the country,
- Studies within scope of technological measures program, on developing early detection and response systems (e.g. AVCI, AZAD and KASIRGA) which integrate artificial intelligence and machine learning in cyber security,
- Bilateral information sharing and coordination studies with national and international stakeholders within scope of threat intelligence gathering, production and sharing program and,
- Monitoring activities on service continuity of critical infrastructures; vulnerability scanning and regulation & auditing activities in terms of information security

have been conducted recently.

Within scope of all those studies, Türkiye moved up 23 ranks and ranked 20th in the world and 11th in Europe, according to International Telecommunication Union's Global Cyber Security Index results published in 2019.

National cyber security studies are supported at the highest level in the country, and within this context, USOM officially launched on 10 February 2020 by the Mr. President Recep Tayyip ERDOĞAN himself, and the vision was put forth to make the country a global cyber security brand.

Due to the indispensability and constant development of technology, cyber security activities should be conducted in continuity. In line with that, National Cyber Security Strategy and Action Plan (2020-2023), was prepared with a view to further the previous achievements. It is aimed to minimize the impact of cyber threats, develop national capacities, create a more secure cyber environment and place the country at the top of the international level in the field of cyber security.

5. VISION AND MISSION

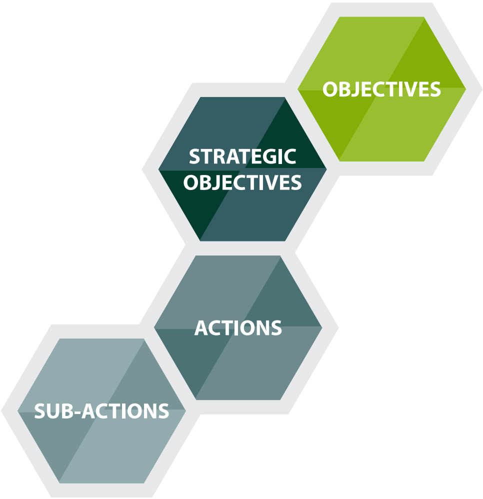
VISION

Acquire a secure cyber environment and become an international brand in the field of cyber security to support the economic development of the country, social life and national security.

MISSION

With the understanding that cyber security is an integral part of the national security, work in coordination with all stakeholders to protect the assets in cyberspace especially critical infrastructures from threats and reduce possible impacts of cyber incidents.

6. METHOD



The first step of strategic approaches is determining the correct methodology. In a field such as cyber security which involves all segments of society, to achieve the objectives easier, the approach chosen should be built on an understandable, applicable, principled basis which also includes correct and timely use of resources.

Comprehensive and planned studies are required to interiorize and address security -which is one of the basic necessities of humanity- taking technological dimensions into account. One thing that should not be disregarded while transforming the vision and mission into substantial acquisitions is presence of the principles to comply with during this transformation. The impact of strategies based on principles will reflect positively on stakeholders and makes it easier to reach the target outcomes.

National Cyber Security Strategy and Action Plan (2020-2023) aims to realize the activities and actions consisting of the activities. When those actions are entirely completed, strategic objectives will have been achieved. Therefore, National Cyber Security Strategy and Action Plan was planned in a goal-oriented structure.

7. PRINCIPLES

Building the strategy and actions aimed at ensuring national security on the principles determined in an efficient and balanced way, will contribute to the social and economic welfare of the country which is constantly developing and strengthening.

The principles on which we ground on when providing national cyber security in line with national and international norms and recent technological approaches are as below:

1. Cyber security is an integral part of national security. Full achievement of national security is only possible through reaching the goals determined in the field of cyber security.
2. Cyber security studies are conducted in accordance with corporateness, continuity and sustainability principles from past to future, in terms of all achievements, objectives, programs and projects.
3. In order for digitalization to be successful and sustainable, cyber security must be regarded as vitally significant.
4. All studies related to implementation of cyber security policies are conducted with efficient communication, coordinated cooperation between stakeholders and appropriate methodologies.

5. Stakeholders carry out their responsibilities for risk management in cyberspace with respect to transparency, accountability and ethical values.

6. Cyber security risks are determined and managed in an efficient way.

7. It is essential to deliver services especially the ones on critical infrastructures in a continuous and efficient manner.

8. Cyber security is the essential component in all phases of service and product development, from design to the distribution.

9. Adherence to basic cyber security principles such as "confidentiality-integrity-availability" balance and "need-to-know" basis is essential.

10. It is essential to build the cyber security on strong legal foundations.

11. Use of national and domestic products/services is encouraged with R&D, innovativeness and strong technological infrastructure understanding.

8. OBJECTIVES

The achievement rate of policies and strategies depends on determining the goals correctly and making the efforts continuously to reach the goals.

Cyber security can be defined as the "*Entirety of activities that involves protecting the information systems which constitutes the cyberspace from attacks, ensuring the confidentiality, integrity and availability of those systems, detection of attacks and cyber incidents, activation of response mechanisms when threats detected, and recovery of the systems back to pre-cyber incident conditions*". Within this framework, the basic goal of all stakeholders that will contribute to providing national cyber security is "minimizing the cyber threats, risks and related impacts". Optimum and efficient use of human resources in the field of cyber security, improvement of processes and technological development can be considered as the elements that are complementary to stable growth and development.

Looking from this perspective, it is considered that the goals to be determined and realized within scope of National Cyber Security Strategy and Action Plan (2020-2023) will contribute to main objectives of the country at short/mid/long-term.

NATIONAL CYBER SECURITY OBJECTIVES
determined within framework of the 2023 Vision of TÜRKİYE

To ensure the cyber security of the critical infrastructures on 24/7 basis.

To possess state-of-the-art technological means of cyber security, at the national level.

To develop domestic and national technological means within framework of operational requirements.

To continue to develop proactive cyber defense understanding with reference to the fact that cyber incident response involves pre-incident, during and post-incident works.

To evaluate and monitor the maturity levels of computer emergency response teams.

To increase the maturity levels of computer emergency response teams.

To increase the cyber incident readiness at institutional, sectoral and national levels with approaches based on risk-based analyses and plans.

To ensure the security of data sharing mechanisms between institutions and organizations.

To ensure the local data traffic (the source and the destination are both domestic) remain inside the country.

To improve the cyber security approach based on regulation and audit in critical infrastructure sectors.

To prevent possible dependencies to producers/manufacturers of IT products, within critical infrastructure sectors.

To identify requirements for the security of new generation technologies.

To realize the transformation of innovative ideas and R&D efforts into national and domestic products and services by fostering them.

To ensure the safe use of cyberspace for all segments of society.

To maintain the activities to keep the cyber security awareness at high levels in whole of society.

To incorporate information security culture in institutions and organizations.

To make sure that children are protected in cyber environment.

To strengthen human resources with projects for interested individuals who aspire to specialize in cyber security.

To make the cyber security more widespread in formal and non-formal education curricula and to enrich the educational contents.

To develop mechanisms to provide information sharing and cooperation with national and international stakeholders.

To minimize cybercrime and to increase deterrence.

To develop mechanisms for accurate and up-to-date information sharing on internet and social media.

9. STRATEGIC OBJECTIVES

As in all elements of technological development, certain focus areas come to forefront to reach determined goals in cyber security as well, which is an integral part of those technologies.

Fundamental focus areas for the period 2020-2023 are defined herewith as “strategic objectives”. The strategic objectives given below are explained in detail in order to realize cyber security vision of our country for 2023 and proceed in confidence for the way forward:

I
Protecting Critical Infrastructure and Increasing Resilience

II
National Capacity Building

III
Organic Cyber Security Network

IV
Security of New Generation Technologies

V
Fighting against Cybercrime

VI
Developing and Fostering National and Domestic Technologies

VII
Integrating Cyber Security into National Security

VIII
Improving International Cooperation

I. Protecting Critical Infrastructure and Increasing Resilience

"National Security in Cyberspace"

Critical Infrastructures are defined as the "infrastructures that contain information and communication systems that disruption of the confidentiality, integrity or availability of the data processed in which may cause loss of lives, economic harm of wide scale, national security gaps or public disorder". Cyber threats especially target those infrastructures which provide essential services for the benefit of all citizens. The main motivation of the attackers is that the negative impact of those threats can turn out to be disruptive and widescale.

Significant activities have been conducted in the country to protect critical infrastructure sectors, namely "electronic communications", "energy", "finance", "transport", "water management" and "critical public services". Those activities, as they need to be conducted in continuity, will be proceeded to be performed taking into account changing cyber threat vectors, emerging national needs and technological developments. For this purpose, critical infrastructure protection has been determined as a strategic objective. It is aimed to increase national resilience by taking measures to protect public and private sector against cyber threats.

Key points of the studies within this scope will be extending the application of international information security standards in public institutions and private sector; preventing vendor lock-in in critical infrastructures; and to protect the data of the country. Besides, the priorities also include improving sectoral regulations and creating auditing mechanisms; realizing contingency plans; and ensuring a safe technological transformation.

Overall, it is aimed to protect critical infrastructures and all national assets in cyberspace against cyber threats in an efficient way, and further strengthen the cyber incident response capabilities. In addition to that, it is aimed to minimize the threats and their negative impacts through a risk management approach at sectoral and national scales.

II. National Capacity Building

"Strengthening Human Resources"

One of the most important components of ensuring cyber security is having qualified human resources. The activities in this field aims to increase the expertise level and experience of existing human resources. Furthermore, another focus point of those activities is to cultivate qualified manpower in this field.

Within this scope, in order to develop cyber incident readiness level, it is aimed to identify the current status by evaluating the maturity levels of institutional CERTs and to further increase their competencies by focusing on the aspects which need to be improved. Competencies will also be improved by the cyber security exercises and trainings to be conducted regularly at sectoral, national and international levels.

Furthermore, activities will be carried out aimed at developing "cyber security expertise" concept into a profession, making the programs on cyber security and related fields more widespread in universities and increasing the expertise level of personnel responsible for fighting against cybercrime. In addition to those efforts, individuals aspiring to specialize in this field will be supported by organizing capture the flag competitions, summer camps and trainings thereby strengthening qualified human resources of the country in this field.

"Raising Public Awareness and Children Online Protection"

Cultivating cyber security culture in all segments of society is a necessity of this day and age and the basis of the culture is raising awareness to higher levels. When all individuals embrace the importance of safe use of technology, negative impacts of risks and threats on the life will visually diminish.

In this context, the priority goals include awareness raising activities at individual, institutional and national scales, namely all across society, and outreaching all segments with the activities aimed at families, children, students, youth, women, elderly and the disabled. Awareness raising campaigns for children online protection and activities to increase consciousness toward the responsibilities of families will be among the high priority studies.

III. Organic Cyber Security Network

"Fighting against Advanced Threats"

Cyber threats get increasingly more complex, harder to detect and become more widespread as a threat to national security. As well as ransomware and phishing, the intention to create threats difficult to predict and detect such as APTs and zero-day attacks appears as the methods usually used by the attackers to inflict larger scale damages.

To counter those threats, developing advanced-level expertise projects analyzing persistent threats and performing long-running studies depend on improving the maturity levels of the teams.

"Together We Are Stronger"

By establishing an organic cyber security network, it is aimed to develop cooperative efforts where people from all segments who are working or interested in cyber security field can share knowledge and experience.

It may not be possible to acquire information about the attack profiles which appear with a wide range of varied motivations. For this reason, sources should be diversified and increased in cyber security where the knowledge and intelligence sharing play a key role. The input to be provided for national cyber security activities acquired from those diversified sources will further strengthen USOM and the institutional CERTs which constitute the backbone of cyber incident response structure.

Within this scope, it is aimed to further the knowledge exchange and interaction between USOM and the stakeholders. It is of great importance to increase knowledge exchange between public institutions and private sector regarding cyber threats and form new connections with stakeholders, mainly the young population who have studies in the field of cyber security. In line with this, it is aimed to make contribution to national cyber security with reciprocal support and feedback mechanisms. Thus, to create a live, active and organic cyber security network at national scale by maintaining 24/7 interaction with all stakeholders is the main target.

The studies to be performed will enhance proactive defense, provide cyber deterrence and ensure that attacks are detected and prevented before they occur, thus increase the strength with the force rising from unity in cyberspace.

IV. Security of New Generation Technologies

"Reliable New Generation Technologies"

New generation technologies, which have entered into the very center of the lives of us with many applications, have been included among the priority topics in the Strategy. Secure use of technologies such as internet of things, cloud computing, and soon to roll out 5G, does support sustainable national economic development. In the meantime, it is aimed to determine the use cases for artificial intelligence and block chain technologies in the field of cyber security and create added value with the national and domestic technologies to be developed.

V. Fighting against Cybercrime

"Secure Cyber Environment"

The crime moving to cyberspace, being committed using the components there, threatening individual rights and freedoms, and the attacks targeting information systems are the issues which whole world is facing now and carries out intense efforts to find solutions. It is required to constantly develop the fighting methods against cybercrime, and to conduct preventive, deterrent and efficient studies. Within this context, it is aimed to increase the national capacity and technological means in this field in order to continue the fight against cybercrime with much more strength.

"International Efforts"

There is a need for cooperation especially at the international level for fighting against cybercrime. Non-spatial nature of cyberspace allows cyber criminals to operate beyond national borders. Therefore, the goal is to further develop the knowledge and information sharing and international cooperation in order to detect the source of the cybercrime and the criminal in the most efficient manner.

VI. Developing and Fostering Domestic and National Technologies

"Technology of Türkiye"

Increasing the number and prevalence of national and domestic cyber security solutions into which new generation technologies are integrated, will contribute to reach the targets within scope of 2023 vision of the country. Within scope of the studies conducted with the aim of making the country leader in the field of cyber security, the main goal is to enable private sector to contribute to the economy and shape the technology by boosting its development, growth and export capacity.

"Cooperation and Support Mechanisms for Technology Development"

It is aimed to develop and further enhance cooperation between public institutions-academia-private sector in order to grow and develop the cyber security ecosystem. Those cooperations will be able to directly affect domestic and national product development and ensure that the products and services are customized to the needs. It is aimed to benefit from existing mechanisms and create new mechanisms in order to support private sector especially entrepreneurship, research and development efforts, start-ups and small and medium-sized enterprises.

Ensuring the cyber security with domestic and national products, especially protecting the critical infrastructures with domestic and national security solutions, is amongst the priority goals.

"Cyber Security Test and Certification System"

The main goal is to exponentially increase the brand value of products and services produced with the national resources and make them open to global markets with increasing export. In line with this goal, it is aimed to test the performance efficiency of the domestic products and services to boost their competitiveness in international market, and aimed to establish the required national mechanism in order to certificate them. Additionally, by the mechanism, IT products of foreign origin used in the country will be able to be tested in terms of cyber security.

VII. Integrating Cyber Security into National Security

"Cyber Security for National Security"

Cyber security is an integral part of national security. Within this context, it is aimed to take the cyber security related elements into account in the high-level national security policies at maximum level; include cyber defense alongside with land, air, sea and space security in the mentioned policies; protect the country from hybrid threats involving cyber elements as well as other elements; and increase deterrence.

VIII. Improving International Cooperation

"Fighting against Transboundary Threats"

There are no definite frontiers in cyberspace. Cyberspace has an ever-expanding structure where every moment, new devices, systems and users get connected to each other. Cyber security is a very hot topic that is on the agenda of the whole world and involves efforts at international level. For this reason, in the country and in the world, international activities are carried out in order to complement cyber security efforts at national level and boost the achievements obtained by them.

There exist bilateral and multilateral efforts on cooperation initiated for policy-making in cyber security, cyber incident response and fight against cybercrime. Activities carried out within the scope of mentioned cooperation lead the efforts of international mechanisms in cyberspace and provide information and experience sharing.

Identification of the measures to increase trust in cyberspace in the eye of international organizations, and implementation of them by member states, development of joint strategies and applications, cooperation studies at technical level and increase in communication between experts, are on the agenda of cyberspace. In addition to those, events for strengthening response capabilities and increasing knowledge and preparedness levels against cyber incidents in the country and the world -such as cyber security exercises, conferences, seminars and workshops-; and capacity-building activities at international level have been organized by Türkiye.

For the future periods, it is aimed to strengthen the prominent position of the country in cyber security by the increasing contribution and attendance to international activities in this field, and increase the input provided for the national cyber security efforts by identifying the best practices in the world.

10. REALIZATION APPROACH

10.1. Action Plan

It is of great importance to realize the goals by taking the necessary steps with all stakeholders to ensure national cyber security in line with the vision and mission of National Cyber Security Strategy (2020-2023) and within framework of the principles. During the workshop attended by public institutions, private sector, academy and NGOs, feedbacks from relevant stakeholders were received regarding the required actions and activities to reach national goals within scope of strategic objectives. The draft document was opened to feedbacks of relevant institutions and organizations, accordingly revised and finalized.

The complementary document of the Strategy, National Cyber Security Action Plan (2020-2023) includes in detail; the description of an action and institutions responsible for each action, institutions with which to cooperate, goals of actions and sub-actions, methods to follow while realizing those and time periods of their realization.

National Cyber Security Strategy and Action Plan (2020-2023) covers 40 actions and 75 sub-actions under 8 strategic objectives in total.

10.2. Monitoring and Measurement

National Cyber Security Action Plan (2020-2023) is a complementary document which depends its success on the realization of the actions. Measuring the progress and completion of each action means substantializing the success of the studies performed. For that purpose, measurement criteria were determined regarding each sub-action of main actions and ensured that the achievement rate of the Action Plan is measured as per those criteria. The sub-actions of each main action and the methods to employ while realizing those sub-actions were taken into account, while determining the measurement criteria.

The monitoring and measurement of the Action Plan will be realized by the input to be received from the relevant institutions and organizations responsible for the actions, based on the sub-actions and conducted activities and measurement criteria.

10.3. Stakeholders

Deadlines and responsible institutions/organizations have been determined for each sub-action taking the characteristics of the actions, required activities, resource requirements and continuity of the activities into account. Yet in some cases there are more than one institution or organization to cooperate with. Realizing each sub-action under the coordination of the responsible institution with the cooperation of relevant institutions/organizations, is considered important for a successful delivery of the Action Plan and ensuring the national cyber security.

Public institutions, private sector institutions and organizations, mainly the ones operating critical infrastructures, universities, non-governmental organizations, research communities, individuals in the country and international stakeholders are among the stakeholders in the cyberspace. It is aimed to reach the determined targets by direct or indirect contributions from all the stakeholders.

10.4. Scope

The scope of the National Cyber Security Strategy and Action Plan (2020-2023) includes public information systems, information systems of critical infrastructures operated by public and private sector, small and medium-sized enterprises, and all components of cyberspace at national level including all natural and legal persons.

10.5. Updates

National Cyber Security Strategy and Action Plan (2020-2023), which is a visionary document of the country in the field of cyber security; will be updated, should the need arise, taking technological developments, current conditions, changing national needs and requirements into account. Furthermore, any action included in the Action Plan that may not be completed within its time period, is planned to be covered within the next National Cyber Security Strategy and Action Plan.

10.6. Relation between Strategic Objectives and Actions

Each of the 8 strategic objectives is affiliated with the 40 actions in order to achieve the objectives determined within the scope of National Cyber Security Strategy and Action Plan. Those actions consist of 75 sub-actions. The activities of the actions will be conducted by the responsible 14 different public institutions and 34 different cooperating public institutions. Moreover; all ministries, regulatory and supervisory authorities, universities and NGOs were included as the responsible and cooperating institutions for relevant sub-actions. The relation between the strategic objectives and actions are illustrated in the table below.

	*A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19	A20
I. Protecting Critical Infrastructures and Increasing Resilience	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓								✓		✓
II. Developing National Capacity							✓	✓		✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
III. Organic Cyber Security Network																		✓		✓
IV. Security of New Generation Technologies												✓								
V. Fighting against Cybercrime																	✓	✓		✓
VI. Developing and Fostering National and Domestic Technologies												✓								
VII. Integrating Cyber Security into National Security																				
VIII. Improving International Cooperation										✓								✓		

*A: Action

	A21	A22	A23	A24	A25	A26	A27	A28	A29	A30	A31	A32	A33	A34	A35	A36	A37	A38	A39	A40
I. Protecting Critical Infrastructures and Increasing Resilience		✓	✓	✓	✓	✓								✓		✓	✓	✓	✓	
II. Developing National Capacity	✓						✓	✓	✓				✓							
III. Organic Cyber Security Network	✓																			
IV. Security of New Generation Technologies		✓	✓	✓	✓	✓														
V. Fighting against Cybercrime	✓	✓			✓		✓	✓	✓	✓	✓	✓	✓							✓
VI. Developing and Fostering National and Domestic Technologies				✓		✓					✓			✓	✓	✓		✓		
VII. Integrating Cyber Security into National Security																			✓	
VIII. Improving International Cooperation												✓	✓							✓

*A: Action

REPUBLIC OF TURKEY
MINISTRY OF TRANSPORT
AND INFRASTRUCTURE

Hakkı Turayliç Street No:5
Emek / Çankaya / Ankara / Turkey
www.uab.gov.tr