Republic of Turkey
Ministry of Transport Maritime Affairs
and Communications

2016-2019
National Cyber Security Strategy

1 Introduction

Information and communication technologies have become integral components of society and economy and contribute significantly to development. The use of information and communication systems in our country have become widespread in the public and private sectors, as well as among citizens and notably in critical infrastructure sectors such as energy, water resources, health, transportation communication and financial services. Information and communication technologies, and Internet use in particular, interconnect all components in cyber space which bring with it cyber security risks and uncertainties.

As our institutions and organizations increasingly use information and communication systems in providing services, ensuring security on such information and communication systems has become an important aspect of both our national security and our economy. Security weaknesses in information and communication systems may cause such systems to become out of service or to be exploited or may lead to eventual loss of life, large scale economic loss, disturbance of public order and/or compromises to national security. Financial losses arising from cyber-attacks have reached extraordinary levels. Reports from organizations such as the World Economic Forum and various security companies clearly indicate this fact.

It is a fact that cyber space provides advantages such as anonymity and deniability for the attacks made to information systems and information/data. It is difficult to detect the financers and organizers of persistent and advanced cyber-attacks targeting information systems and data. This situation and characteristics reveal asymmetric character of risks and threats in cyber space and make it difficult to fight with these threats.

Ensuring absolute cyber security is no longer achievable in such an environment. So instead, the aim is to keep cyber security risks at manageable and acceptable levels. It is acknowledged that being in an open and connected environment such as the Internet present certain risks with increased accessibility. The objective must be being prepared for cyber incidents by managing risks with a holistic approach that includes all stakeholders and assuring continuity by mitigating these incidents with minimum loss.

1.1 National Cyber Security Strategy and 2013-2014 Action Plan

In light of this information, the Ministry of Transportation, Maritime and Communication has been given the duty of preparing the policy, strategy and action plans for providing national cyber security and ensuring coordination, pursuant to “The Council of Ministers’ Decision on the Execution, Management and Coordination of National Cyber Security Activities” that was published in

the Official Gazette Number 28447 on October 20th, 2012, and The Electronic Communication Law Number 5809.

All public institutions and organizations, as well as natural and legal persons are expected to perform assigned tasks within the framework of the policies, strategies and action plans determined by the Cyber Security Board (Annex-A) and to follow determined methods, principles and standards.

Drafted to address these issues, the National Cyber Security Strategy and 2013-2014 Action Plan was published in the Official Gazette Nr. 28683 on June 20th, 2013 and enacted. In addition to practices scheduled for the 2013-2014 period, the paper covers periodical activities that go beyond this period, such as training and awareness raising initiatives.

1.2 The Preparation Process of the 2016-2019 National Cyber Security Strategy and Action Plan

It has become imperative for the Ministry of Transportation, Maritime and Communication to update the national cyber security strategy and to determine actions that cover the 2016-2019 period in line with developing information and communication technologies, increasing security demands and gained experiences. In this context, seven evaluation meetings were held between March 10th and April 7th, 2015 with institutions considered responsible or associated in the previous action plan. Prospective assessments and actions to be realized in scope of cyber security were identified and recorded

comprehensively during the meetings, in addition to the extent of achievement of activities stated in the previous action plan and challenges.

After the meetings, a Common Mind Platform was held with the participation of 126 specialists from 73 institutions and organizations representing public institutions, critical infrastructure operators, the IT sector, universities and non-governmental organizations. The platform studies that lasted two days determined strategic objectives and actions by focusing on Turkey’s cyber security strengths and weaknesses.

Cyber Security issues have been included in the agendas of all developed countries besides international organizations such as the EU (European Union), the OECD (Organization of Economic Cooperation and Development), NATO (North Atlantic Treaty Organization), especially after 2008. The preparation of the 2016-2019 National Cyber Security Strategy and Action Plan covered several stages in addition to the works carried out with stakeholders. A background literature review investigated cyber security strategies from many countries in America, Europe and the Far East, and suggested solutions in areas like scope, objectives, priorities, organization structure, resource allocation, R&D (Research and Development) coordination, public-private cooperation and training.

The "2016-2019 National Cyber Security Strategy and 2016-2019 National Cyber Security Action Plan" was prepared as a result of accumulating, reviewing and assessing information generated within scope of such efforts.

1.3 Definitions

The terms used in this document refer to the following:

Threat: The potential cause of an incident that may cause damage to an institution or system,

Risk: The potential risk of causing damage by using vulnerabilities in one or more information entities,

Information systems: Systems included in the provision of any service, transaction and information/data through information and communication technologies,

Industrial Control Systems: Information systems in the SCADA (Supervisory Control and Data Acquisition) and Distributed Control Systems groups, which are used for industrial operations such as production, product processing and distribution controls via programmable logical controllers other than conventional information technologies,

Cyber space: The numeric environment composed of information systems spread over the entire world and space, the networks interconnecting these systems or independent information systems,

Public information systems: Information systems owned and/or operated by institutions and organizations of the Republic of Turkey,

Information systems owned by natural and legal persons: Information systems owned and/or operated by natural and legal persons who are subject to the laws of the Republic of Turkey,

National cyber space: The environment that is composed of public information systems and information systems operated/used by natural and public persons,

Confidentiality: The characteristic of preventing the use or disclosure of information to unauthorized persons, entities or processes,

Integrity: The characteristic of maintaining the accuracy and consistency of entities,

Accessibility: The characteristic of being accessible and useable when demanded by an authorized entity,

Critical Service: Services, which may cause;

- Loss of life,
- Large scale economic loss,
- National security vulnerabilities or disturbance of public order,

unless provided.

Critical Product: Information technology products that provide the confidentiality, integrity and availability of critical services,

Critical infrastructures: Infrastructures that contain information systems, which may cause

- Loss of life,
- Large scale economic loss,
- National security gaps or disturbance of public order

when the confidentiality, integrity or availability of the data they contain is compromised,

Critical infrastructure sectors: "Electronic Communication", "Energy", "Water Management", "Critical Public Services", "Transportation" and "Banking and Finance" sectors, which contain critical infrastructures pursuant to the Resolution No.2 of the Cyber Security Board dated 20/06/2013,

Institution: Public institutions and public or private sector institutions operating critical infrastructures,

Cyber incident: Violation or violation attempts of confidentiality, integrity or availability of information and industrial control systems or information/data processed by these systems,

Cyber attack: Operations carried out deliberately by a person and/or information systems at any place in cyber space for the purpose of

compromising the confidentiality, integrity or availability of information systems in national cyber space,

Border Security: Protection of information systems from potential attacks from external networks by means of access control systems such as firewalls and attack prevention systems,

Cyber security: Protection of information systems forming cyber space from attacks, assuring confidentiality, integrity and availability of information/data processed in this environment, detection of attacks and cyber security incidents, activation of counter-response mechanisms and recovering systems to conditions prior the cyber security incident,

National Cyber Security: Cyber security provided at a national scale for any hardware and software systems associated with all services, transactions, information/data provided through the information and communication technologies that constitute national cyber space.

1.4 Mission

Determining, coordinating and implementing efficient and sustainable policies to guarantee national cyber security.

1.5 Vision

Formation of an eco-system that has international competitive power in the field of cyber security, in which all stakeholders related to cyber security manage

risks at cyber space in a competent manner in cooperation with each other in order to benefit from information and communication technologies in the most efficient way for the purpose of contributing to wealth and security of society, as well as national economic growth and efficiency.

1.6 Objective

The 2016-2019 National Cyber Security Strategy and Action Plan has two main objectives. First, for all stakeholders to acknowledge the understanding that cyber security is an integral part of national security. Second, acquiring the competency that will allow taking administrative and technological precautions for maintaining the absolute security of all systems and stakeholders in national cyber space. In order to achieve this main objective, it is among the purposes of this document to determine targets and sub actions, while ensuring and supervising their implementation.

In line with these objectives:

- Ensuring the security, confidentiality and privacy of all services, transactions and information/data provided through information technologies as well as systems used for the provision of such, provided that they cover cyber space entirely,
- Determining cyber security actions to minimise the effects of cyber security incidents, recovering systems to normal functions as quickly as possible after incidents and ensuring higher efficiency in the exploration

and investigation of emerging crime by judicial authorities and law enforcement forces,

- Locally developing critical technologies and products for ensuring cyber security, confidentiality and privacy, or otherwise, taking measures to ensure that technology and products procured from abroad shall be solely and safely used for this purpose,

are addressed in this plan.

1.7 Scope

The 2016-2019 National Cyber Security Strategy and Action Plan covers all components of national cyber space on a national scale, including small and medium scaled industry, all natural and legal persons in addition to public information systems and information systems of critical infrastructures operated by public or private sector.

1.8 Update

The National Cyber Security Strategy shall be updated with national level coordination with respect to demands received from the public and privet sector, and with consideration to developing technology, changing conditions and requirements.

Actions included in this plan which cannot be accomplished by the end of 2019 will be carried on to the next action plan.

1.9 Cyber Security Strategies and Action Plans in the World

This section presents important and points from Cyber Security Strategy documents published by other countries.

Similar to the 2016-2019 National Cyber Security Strategy and Action Plan, potential cyber security risks and principles for implementing risks mitigating actions are mentioned in strategy documents of other countries and it was observed that the risks and principles did not vary significantly among countries.

Significant principles within this context are as follows:

a. Fulfilment of all legal and social responsibilities by individuals, institutions, society and state in providing cyber security,
b. Coordination, joint participation, collaboration and information sharing between the public sector, private sector, universities and non-governmental organizations,
c. Advanced cyber incident management cooperation between International Cyber Security Operation Centres.

Significant risks in the reviewed documents include:

1. Social network addiction of society,
2. Positions of critical institutions and organizations in cyber space,
3. Various cyber spying efforts and targeted attacks,
4. Lack personnel and competency,

5. Lack of coordination between institutions,
6. Economic concerns concerning sectors of varying scales operating in cyber space.

National cyber security principles, risks, strategic cyber security objectives and action plans have been determined with regard to these principles and risks.

2 Principles

The principles to be considered in ensuring national cyber security are as follows:

1. Cyber security is ensured by means of methods based on efficient and continuous assessment and improvement based on risk assessment. It is aimed that risk management methods to be created will address threats and vulnerabilities and determine new risks and to offer methods for reducing these risks to an acceptable level.

2. In order to provide cyber security, all stakeholders must know about cyber security risks and be aware that their approaches towards the management of these risks will affect not only them but also others. In order to achieve this level of awareness and competency, all stakeholders must acquire necessary trainings and experience. In addition to the technical dimension, an integrated approach including legal, administrative, economic, political and social dimensions is adopted.

3. Risk management involves rapid removal of technical vulnerabilities, preventing and responding to attacks and threats, and minimizing potential damages. Having and implementing a preparedness and continuity plan against cyber incidents is important in minimising losses.

4. Besides cooperation among all stakeholders including public, private sector, universities, non-governmental organization and individuals, achieving and sustaining cyber space security demands international cooperation and information exchange and building trust.

5. All stakeholders must pay regard to the rule of law, freedom of expression, fundamental human rights and freedoms as well as principles of protection of privacy in their efforts to ensure cyber security.

6. Stakeholders observe transparency, accountability and ethical values while performing their responsibilities in management of risks in cyber space.

7. Implemented cyber security measures must be proportional to relevant risks, positive and negative impacts must be assessed and balanced.

8. The use of national products and services is encouraged in meeting cyber security requirements; research and development projects are endorsed for developing such products and services, and innovation is regarded as essential.

3 Cyber Security Risks

Cyber security risks were assessed realistically in order to define strategic objectives within the scope of cyber security. The determined risks have been listed below:

1. Interruption of energy, transportation etc. critical services as the result of denial of service attacks and similar targeted attacks on information systems used by critical infrastructures.

2. Stealing, disclosure, modification or destruction of personal information and confidential publicly owned information by attackers as a consequence of targeted attacks towards information systems used by public and critical infrastructures.

3. Stealing, disclosure, modification or destruction of sensitive or commercially valuable data by attackers as the result of targeted attacks focused on acquiring trade secrets and know-how of institutions and organizations (private companies, research institutions and defence industry) engaging in research, development and production.

4. Harm the reputation of various institutions and organizations or the disclosure, modification or destruction of sensitive information/data as a consequence of hacker (hacktivism) attacks for propaganda purposes.

5. Material damage as a consequence of service failure due to denial of service and similar attacks on e-commerce companies, e-mail and social media service providers, creation of fake operation records; attackers acquiring, disclosing, modifying or destructing confidential information.

6. Loss of reputation by companies engaged in e-commerce, finance sector or other corporations offering online payment or money transfer services as a consequence of attackers stealing sensitive customer information, social distrust towards online transactions and material loss incurred by customers using such services.

7. Discontinuity of small and medium sized industry operations, commerce and service sector companies due to a lack of security measures in their IT systems or human error, resulting in attackers stealing, disclosing, modifying or destructing sensitive or commercial information.

8. Exposure to malware and phishing attacks, fraud and identity theft, attackers stealing, modifying or destructing personal information and devices and performing fake transactions due to reasons such as social addiction to internet and social networks, insufficient knowledge and awareness about cyber security, and failing to take personal security measures in mobile and stationary information systems.

9. Fraud at any institution and organization as the result of bulk mail, malware and similar attacks.

10. Interruption of services and operations provided via information systems at any institution and organization as the consequence of human errors or natural disasters.

4 Strategic Cyber Security Objectives and Actions

For the 2016-2019 period, strategic objectives aiming to minimise current risks in light of the determined principles are as follows:

1. Creating a national critical infrastructure inventory, meeting security requirements of critical infrastructures and supervision of these critical infrastructures by the relevant regulatory board (Annex-B).
2. Creation of a legislation conforming to international standards, which also contains cyber security auditing standards.
3. Improving the regulatory and supervisory awareness and competencies of sector regulating institutions, ministries etc. in scope of cyber security.
4. Making arrangements to protect information systems of institutions not only from attacks, but also from human errors and disasters.
5. Bringing each institution to a level of competency in operating its own information security management process.
6. Raising executives' level of awareness in the area of cyber security.
7. Training qualified personnel in cyber security and encouraging personnel, researchers and students who aim to specialize in this field.
8. Creating cyber security awareness in every level of society, implementing written and visual works in media on awareness in addition to the efforts of education institutions.

9. Providing legislative support for employing expert personnel in cyber security and improving personnel rights of the employee at public institutions.
10. Providing legislative support, making financial arrangements, hiring qualified personnel, providing IT infrastructure and improving information sharing in scope of organizing national cyber incidents responses with the aim of increasing the efficiency of Corporate and Sectorial CIRT (Cyber Incidents Response Team) (Annex C).
11. Founding a strong central public authority that will ensure coordination in the field of cyber security.
12. Forming a national cyber security eco-system with the aim of participation and coordination of public institutions, private sector, NGO's (Non-Governmental Organizations), supervisory institutions, universities, software companies and all other stakeholders.
13. Disseminating best examples within the national cyber security eco-system, offering consultancy services, sharing vulnerabilities, threats and useful practices.
14. Performing vulnerability analysis and certification works for preventing exploitation of vulnerabilities contained by domestic or foreign hardware and software products used in critical points of information systems.
15. Creating a culture of developing and supplying secure software.

16. Giving importance to R&D activities and developing national products for reducing foreign- dependency in cyber security.
17. Developing national proactive cyber defence capability for eliminating threats.
18. In order to eliminate anonymity, which is the greatest advantage of threat actors in cyber space, dissemination of efficient log management and IPv6 (Internet Protocol version 6).

Actions to be realized for reaching strategic objectives stated in previous sections are incorporated under five strategic action headings. Such strategic action headings were divided into actions and listed in the "2016-2019 National Cyber Security Action Plan" per their planned accomplishment date and responsible/relevant institutions. Strategic actions that are planned to be realized in the 2016-2019 period were grouped under the following headings:

4.1 Strengthening the Cyber Defence and Protection of Critical Infrastructures

Realization of actions towards reducing risks that may affect state and national economy, critical infrastructures and society is planned within the scope of this strategic action.

4.2 Combating Cyber Crimes

Realization of actions towards reducing risks that may affect institutions and individuals, mainly causing material loss, is planned within the scope of this strategic action.

4.3 Improvement of Awareness and Human Resources

Realization of actions for bringing cyber security culture to all segments of society from the executives of institutions to simple computer users, and raising cyber security experts is planned within the scope of this strategic action.

4.4 Developing a Cyber Security Ecosystem

Realization of actions for determining and implementing requirements from legislation to technology with coordinated contribution of public, private sector, NGO's and other stakeholders is planned within the scope of this strategic action.

4.5 Integration of Cyber Security to the National Security

Realization of actions towards reducing the loss incurred by attacks performed by well-organized threat actors that may affect state and national economy, critical infrastructures and society is planned within the scope of this strategic action.

ANNEX A: List of Cyber Security Board Member Institutions

1. Ministry of Transportation, Maritime Affairs and Communication (MoTMC)
2. Ministry of Foreign Affairs (MoFA)
3. Ministry of Interior (MoI)
4. Ministry of National Defence (MoND)
5. Undersecretariat of Public Order and Security (UoPOS)
6. National Intelligence Organization (NIO)
7. Turkish Armed Forces General Staff
8. Information and Communication Technologies Authority (ICTA)
9. Scientific and Technological Research Council of Turkey (STRCoT)
10. Financial Crimes Investigation Board
11. Presidency of Telecommunication and Communication (PoTC)

Annex B: List of Regulatory and Supervisory Institutions

1. Banking Regulation and Supervision Agency (BRSA)
2. Information and Communication Technologies Authority (ICTA)
3. Energy Market Regulatory Authority (EMRA)
4. High Council of Judges and Prosecutors (HCJP)
5. Istanbul Arbitration Centre
6. Public Oversight Accounting and Auditing Standards Authority
7. Public Procurement Authority (PRA)
8. Radio and Television Supreme Council (RTSC)
9. Turkish Competition Authority
10. Turkish Sugar Authority
11. Capital Markets Board of Turkey (CMBoT)
12. The Central Bank of the Republic of Turkey (CBRT)
13. Tobacco and Alcohol Market Regulatory Authority (TAMRA)
14. Supreme Electoral Council (SEC)
15. Council of Higher Education (CHE)

Annex C: Sector Based CIRT List

Sector Based CIRTs in Critical Public Services and Water Management Sectors

1. Ministry of Interior
2. Ministry of Justice
3. Ministry of Finance
4. Ministry of Environment and Urban Planning
5. Ministry of Labour and Social Security
6. Ministry of Food, Agriculture and Livestock
7. Ministry of Forestry and Water Works
8. Ministry of Health

Sector-Based CIRTs in the Transportation Sector

1. MoTMC, General Directorate of Highway Regulation
2. MoTMC, General Directorate of Railway Regulation
3. MoTMC, General Directorate of Maritime and Inland Waters Regulation
4. MoTMC, General Directorate of Civil Aviation

Sector-Based CIRTs in Electronic Communication, Energy and Finance Sectors

1. **Communication Sector:** Information and Communication Technologies Authority (ICTA)
2. **Finance Sector:** Banking Regulation and Supervision Agency (BRSA)
3. **Energy Sector:** Energy Market Regulatory Authority (EMRA)
4. **Finance Sector:** Capital Markets Board (CMB)