CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

National Cybersecurity Organisation: TURKEY

Emre Halisdemir

National Cybersecurity Governance Series

Tallinn 2021

About this study

This publication is part of a series of country reports offering a comprehensive overview of national cybersecurity governance by nation. The aim is to improve awareness of cybersecurity management in the various national settings, support nations enhancing their own cybersecurity governance, encourage the spread of best practice and contribute to the development of interagency and international cooperation.

Primarily focusing on NATO Nations that are Sponsoring Nations of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), each country report outlines the division of cybersecurity roles and responsibilities between agencies, describes their mandate, tasks and competencies and the coordination between them. In particular, it covers the mandates of political and strategic management; operational cybersecurity capabilities and cyber incident management; military cyber defence; and cyber aspects of crisis prevention and management. It offers an introduction to the broader digital ecosystem of the country and outlines national cybersecurity strategy objectives to clarify the context for the organisational approach in a particular nation.

CCDCOE

The NATO CCDCOE is a NATO-accredited cyber defence hub focusing on research, training and exercises. It represents a community of 29 nations providing a 360-degree look at cyber defence, with expertise in the areas of technology, strategy, operations and law. The heart of the Centre is a diverse group of international experts from military, government, academia and industry backgrounds.

The CCDCOE is home to the Tallinn Manual, the most comprehensive guide on how international law applies to cyber operations. The Centre organises the world's largest and most complex international live-fire cyber defence exercise, Locked Shields. Every spring the Centre hosts the International Conference on Cyber Conflict, CyCon, a unique event bringing together key experts and decision-makers of the global cyber defence community. Since January 2018, CCDCOE has been responsible for identifying and coordinating education and training solutions in the field of cyber defence operations for all NATO bodies across the Alliance.

The Centre is staffed and financed by the following NATO nations and partners of the Alliance: Austria, Belgium, Bulgaria, Canada, Croatia, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Montenegro, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, South Korea, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. NATO-accredited centres of excellence are not part of the NATO Command Structure.

www.ccdcoe.org
publications@ccdcoe.org

Disclaimer

Reports in this series

National Cybersecurity Organisation in Czechia

National Cybersecurity Organisation in Estonia

National Cybersecurity Organisation in France

National Cybersecurity Organisation in Germany

National Cybersecurity Organisation in Hungary

National Cybersecurity Organisation in Italy

National Cybersecurity Organisation in Lithuania

National Cybersecurity Organisation in Luxembourg

National Cybersecurity Organisation in the Netherlands

National Cybersecurity Organisation in Poland

National Cybersecurity Organisation in Romania

National Cybersecurity Organisation in Slovakia

National Cybersecurity Organisation in Slovenia

National Cybersecurity Organisation in Spain

National Cybersecurity Organisation in Turkey

National Cybersecurity Organisation in the United Kingdom

National Cybersecurity Organisation in the United States

China and Cyber: Attitudes, Strategies, Organisation

National Cybersecurity Organisation in Israel

Series editors: Kadri Kaska and Keiko Kono (CCDCOE)

Information in this document has been checked for accuracy as of June 2021.

A previous version of this report was authored by Ensar Seker and Ihsan Burak Tolga in 2018.

Table of Contents

1. Digital society and cybersecurity assessment

E-government services enable efficient, easy and reliable interaction with government agencies, facilitating access to accurate and up-to-date information about all public services provided by public institutions and organisations. Turkey's e-government portal (e-Devlet) enables quick and easy sharing of information and documents between institutions. This service aims to spare citizens from commuting and losing time between institutions, while reducing the institutions' workload. Reliability of transactions via e-government is ensured by means such as private codes, mobile signatures and mobile electronic signatures. Such authentication and security systems are mostly incorporated in official transactions including finance, purchases of valuable items, notary services, tax systems, signing official documents and government-to-individual communications.

Country indicators

83.2 million	Population[1]
79%	Internet users (% of the population[2])
783.562	Area (km^2)
13.600	GDP per capita (USD)

International rankings*

67th	ICT Development Index (ITU 2017)
53th	E-Government Development Index (UN 2018)
20th	Global Cybersecurity Index (ITU 2018)
46th	National Cybersecurity Index (eGA 2019)

1.1 Digital infrastructure availability and take-up

In 2020, nearly half the adult population (51.5% among 16-74 years-olds) used the internet to interact with government agencies and organisations and to use government services for personal purposes. The figure has grown quickly from the previous year's 42%. In recent years, the most-used services of e-government were provided by public organisations such as Social Security Institution, Revenue Administration, Ministry of Justice, National Police and the General Directorate of Land Registry and Cadastre.[3] Over half of those online interactions with government organisations involved seeking information about government services. Some of the most popular facilities included queries to the national health database for individual uses, tax reports and billing, mobile communications service inquiries, court and legal record inquiries and statistics, social security transactions, road administration services and personal information updates.

[1] Türkiye İstatistik Kurumu - Turkish Statistical Institute, 2020, Adrese Dayalı Nüfus Kayıt Sistemi Sonuçları 2019, Nr: 33705, http://www.tuik.gov.tr/HbGetirHTML.do?id=33705

[2] Türkiye İstatistik Kurumu - Turkish Statistical Institute, 2020, Hanehalkı Bilişim Teknolojileri Kullanım Araştırması 2020. Nr: 33679, http://www.tuik.gov.tr/PreHaberBultenleri.do?id=33679

[3] Resmî kurumların sunduğu e-hizmetler, 2020 – e-services provided by the government units, 2020 https://www.turkiye.gov.tr/hizmetler

1.2 Digital public services

As of 2020, Turkey's e-government services primarily cover:

- Various **administrative and justice system services** – document tracking, taxation and customs affairs, government contracts and public procurements, queries related to court proceedings;
- **Official registries** – individual record services such as the address of residence, personal records, family or dependent records, conscription information, payrolls etc.;
- **Social and welfare services** – retirement plans and pension tracking, labour union services, medical appointments, records and queries related to government insurance plans;
- Services related to the **education system** such as educational records, applications and tracking, National Educational Eligibility Exam records and queries, scholarship tracking, permalinks to educational institutions;
- **Business and property services** – business activity and records, vehicle records and services, personal debt, mobile device records queries, certifications and theft reporting;
- **Agricultural and farming** records – **cadastral** tracking and information; and
- **Voting** records.

The **Ministry of Transport and Infrastructure (UAB)** is responsible for the installation, implementation and administration of the government services hub (e-government).[4] It oversees the regular operation of entire e-government services from a supervisory position, delegates cybersecurity-related responsibilities to other government organisations and sustains coordination between the related services of other ministries and government agencies.

According to 2019 data, public sector information technology investments amount to 4.5% of all public sector investments.[5]

As an important step in the efforts of digitalisation of public services, in a circular dated 3 December 2016, it was announced that the information networks of all government organisations and institutions would be incorporated into KamuNet (government-use virtual network) to sustain more secure communication across different government bodies.[6]

1.3 Digitalisation in business

Online commerce is steadily gaining popularity in Turkey and 36.5% of people between 16 and 74 years old used online commercial services to purchase products or services for personal purposes in 2020. This was 2.4% higher than in the previous year. The most popular articles purchased through e-services were clothing, books, periodicals and food.[7]

The volume of online commerce has also been on a steady rise over the last few years. In the first six months of 2020, the total online commerce market volume in Turkey reached $13.4 billion. E-commerce volume increased by 64% in the first 6 months of 2020 compared to the same period in 2019.[8]

[4] Official Gazette of the Republic of Turkey, 2006, Bakanlar Kurulu Kararı 24.03.2006, Year: 2006, Issue: 10316 http://www.resmigazete.gov.tr/eskiler/2006/04/20060420-3.htm

[5] T.C. Kalkınma Bakanlığı, Kamu Bilgi ve İletişim Teknolojileri Yatırımları, 2019, http://www.bilgitoplumu.gov.tr/wp-content/uploads/2016/09/Kamu_BIT_Yatirimlari_2016.pdf, http://www.edevlet.gov.tr/e-devlet-icin-genel-gorunum8

[6] T.C. Ulaştırma ve Altyapı Bakanlığı, 2016, Incorporating Governmental Organisations and Institutions into KamuNet, Circular, http://www.udhb.gov.tr/doc/siberg/KamuNetgenelgesi.pdf

[7] Türkiye İstatistik Kurumu - Turkish Statistical Institute, 2020, Hanehalkı Bilişim Teknolojileri Kullanım Araştırması 2020. Nr: 33679, http://www.tuik.gov.tr/PreHaberBultenleri.do?id=33679

[8] Türkiye'nin 2020 E-Ticaret Verileri (İlk 6 Aylık), 2020, https://worldef.net/blog/turkiyenin-2020-e-ticaret-verileri-ilk-6-aylik/

Electronic commerce activities are regulated by the Law on Regulation of Electronic Commerce passed by the Grand National Assembly of Turkey (TBMM) in 2014.[9] All public regulatory activities and secondary legislation on e-commerce were tasked to the Ministry of Trade. [10] Two regulations, one on commercial communication and commercial electronic communications and the other on service providers and intermediary service providers in electronic commerce, both adopted in 2015, detail the responsibilities of service providers and the content of advertisements.[11]

By August 2020, over 95% of Turkish enterprises and practically all enterprises with 250 or more employees had internet access. The vast majority of new companies have broadband internet access and nine out of ten have a company website. Paid cloud computing use was 40.8% in companies with 250 or more employees. The rate of enterprises using robot technology was 5.1%.[12]

1.4 Cyber threat landscape and cybersecurity assessment

Like many other countries, Turkey has been experiencing a rapid digital transformation in recent years. This transformation brings along many information security risks. Approximately 136,000 cyber-attacks were identified in Turkey in 2019.[13] As a result of the adoption of digital technologies at a local and national level, cybersecurity has become as important as physical security for the country. Given the increasing threat, sufficient investment has been made in the field of cybersecurity in government and the private sector. Many coordinated projects have been carried out in public, private and military fields; serious investments have been made by important defence industry organisations; cybersecurity specific institutes have been established in the academic field; and new products and technologies have been developed with national means. As a result of these efforts, Turkey has recently become one of the most successful countries in the field of cybersecurity.

2. National cybersecurity strategy and legal framework

2.1 National cybersecurity foundation

The *National Cybersecurity Strategy and Action Plan 2013-2014* was the first comprehensive strategic planning document in the field of cybersecurity in Turkey and was published in the Official Gazette in June 2013. During those 2 years, studies were carried out to increase the level of cybersecurity

[9] Official Gazette of the Republic of Turkey, 23 October 2014 Law No: 29166, "Bill regarding regulating electronic commerce in Turkey", http://www.resmigazete.gov.tr/eskiler/2014/11/20141105-1.htm

[10] Ministry of Economy, Türkiye'de e-Ticaretin Tarihçesi Law No: 6563 2017, Regulation on Electronic Commerce, https://www.ekonomi.gov.tr/portal/content/conn/UCM/path/Contribution%20Folders/web/Hizmet%20Ticareti/Elektronik%20Ticaret/T%C3%BCrkiyede%20eticaret%20tarih%C3%A7esi%20devam%C4%B1.pdf?lve

[11] Ministry of Commerce, 2015, Regulations on Commercial Communication and Commercial Electronic Communications on 15/07/2015, Regulations on Service Provider and Intermediary Service Providers in Electronic Commerce on 26/08/2015, http://www.resmigazete.gov.tr/main.aspx?home=http://www.resmigazete.gov.tr/eskiler/2015/07/20150715.htm&main=http://www.resmigazete.gov.tr/eskiler/2015/07/20150715.htm, http://www.resmigazete.gov.tr/main.aspx?home=http://www.resmigazete.gov.tr/eskiler/2015/08/20150826.htm&main=http://www.resmigazete.gov.tr/eskiler/2015/08/20150826.htm

[12] Türkiye İstatistik Kurumu - Turkish Statistical Institute, 2020, Girişimlerde Bilişim Teknolojileri Kullanım Araştırması, http://www.tuik.gov.tr/PreHaberBultenleri.do?id=33677

[13] Presidency of The Republic of Turkey, 2020, https://www.tccb.gov.tr/haberler/410/116592/-turkiye-yi-bilgi-ve-iletisim-teknolojilerinde-dunyanin-en-onde-gelen-ulkeleri-arasina-sokacagiz-

legislation, to ensure the security of critical infrastructures, to encrypt the cybersecurity awareness in the society and to detect and prevent cyber threats. [14]

In 2013, the National Cyber Incident Response Centre (Ulusal Siber Olaylara Müdahale Merkezi - USOM) was established and Cyber Incident Response Teams (SOME) started their activities in institutions and organisations, especially in identified critical infrastructure sectors. With the establishment of the national cybersecurity organisation, institutional and organisational structures were constituted and strengthened in the country.

A new plan, the *National Cybersecurity Strategy and Action Plan 2016-2019,* was published in 2016. To keep cybersecurity risks at manageable and acceptable levels, new targets such as strengthening cyber defence, protecting critical infrastructures, combating cybercrimes, developing awareness and human resources, improving the cybersecurity ecosystem were defined. Thanks to the efforts of government and public sector actors to achieve these goals, Turkey has risen 23 ranks compared to the previous year and was ranked 20th in the world and 11th in Europe in 2018, according to the International Telecommunication Union's *Global Cybersecurity Index* published in 2019. [15]

2.2 National cybersecurity strategy

To protect and improve the gains of previous years' strategy plans and efforts, a preparation workshop for a new national cybersecurity strategy plan was held in February 2020 with 127 participants from 67 organisations.[16] As the result of the workshop and additional studies, the *National Cybersecurity Strategy and Action Plan 2020-2023* was published by the Transport and Infrastructure Ministry on 28 December 2020.[17] The document will serve as a guideline for all government organisations, agencies, officials and legal entities for the next three years.

The new strategy aims to improve previous strategies and targets to achieve new goals in seven areas: protecting critical infrastructure, developing national capacity, organic cybersecurity network, security of new generation technologies, combating cybercrime, developing and supporting local and national technologies, integration of cybersecurity within national security and development of international cooperation. To achieve these goals, 40 actions and 75 implementation steps to be taken by institutions and organisations were set out in the strategic plan.

2.3 Cybersecurity legislation

To designate the structure and responsibilities of the Transport and Infrastructure Ministry, the Telegram and Telephone Law of 2000[18] distributed policymaking, regulation and operation functions in the communications domain, amending the basic laws of the telecommunications sector – the 1924 Law of

[14] Ulaştırma ve Altyapı Bakanlığı, Haberleşme Genel Müdürlüğü - Transport and Infrastructure Ministry, 2013, National Cybersecurity Strategy and 2013-2014 Action Plan, https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/some-2013-2014-eylemplani.pdf

[15] International Telecommunication Union's Global Cybersecurity Index, 2019, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

[16] Information Technology and Communication Institution (BTK), 2020, https://www.btk.gov.tr/haberler/2020-2023-siber-guvenlik-stratejileri-btk-da-belirlendi

[17] Ulaştırma ve Altyapı Bakanlığı, Haberleşme Genel Müdürlüğü - Transport and Infrastructure Ministry, 2020, National Cybersecurity Strategy and 2020-2023 Action Plan, https://hgm.uab.gov.tr/haberler/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-2020-2023-yayimlandi?PageSpeed=noscript

[18] Official Gazette of the Republic of Turkey, 2000, Law No 4502 dated 27 January 2000, http://www.mevzuat.gov.tr/MevzuatMetin/1.5.4502.pdf

Telegram and Telephone[19] and the 1983 Law on Establishing Information and Communication Technologies Authority.[20]

The Telecommunications Authority, established in 2000, is the first sectoral regulatory body in Turkey. To improve legislative clarity, create competition in the sector, reduce uncertainty for operators and allocate resources to R&D, the Electronic Communications Law came into force in November 2008.[21]

An important law protecting the individual's personal information, the Personal Data Protection Law[22] adopted by the Turkish Parliament in March 2016, came into force in April 2016. The law covers all data processing personnel and institutions within the framework of basic purposes such as ensuring the confidentiality of personal data, protecting it and preventing unauthorised use. All institutions are obliged to comply with the law and all personal data processes conducted by these institutions are within its scope.

Turkey has also signed and ratified the 2001 Budapest Convention on Cybercrime [23] (with a few reservations) which addresses internet and computer crime by harmonising national laws, improving investigative techniques and increasing cooperation between states. It has also passed national laws in accordance with the provisions of the Convention.

3. National cybersecurity governance

3.1 Strategic leadership and policy coordination

Implementation, administration and coordination of national cybersecurity actions, and preparation and coordination of policy, strategy and action plans regarding the governance of national cybersecurity were given to the **Transport and Infrastructure Ministry** by Cabinet[24] decision of October 2012.

The Ministry acts as the responsible government agency and oversees all other cybersecurity entities throughout the state.[25] It has been overseeing and conducting cybersecurity activities at the strategic level through the Turkish National CERT (USOM). The Ministry is also able to form councils and working groups to conduct best practices for fulfilling its given responsibility regarding national cybersecurity.[26]

The Transport and Infrastructure Ministry is also responsible for:

- Preparing strategy and action plans to maintain national cybersecurity;
- Constructing procedures and principles to ensure security and privacy of the information belonging to public and private institutions;

[19] Official Gazette of the Republic of Turkey, 2008, Telgraf ve Telefon Kanunu 1924 Law No: 406, http://www.mevzuat.gov.tr/MevzuatMetin/1.3.406.pdf

[20] Official Gazette of the Republic of Turkey, 2011, Information and Communication Technologies Authority Establishment Law (Bilgi Teknolojileri ve İletişim Kurumunun Kuruluşuna İlişkin Kanun 1983), Law No: 2813 / 1983, http://www.mevzuat.gov.tr/MevzuatMetin/1.5.2813.pdf

[21] Information and Communication Technologies Authority, 2015, Information and Communication Technologies Authority (BTK) Establishment, https://www.btk.gov.tr/en-US/Pages/Establishment

[22] Personal Data Protection Authority, 2016, Personal Data Protection Law No 6698 dated 7 April 2016, https://www.kisiselverilerinkorunmasi.org/kanunu-6698-sayili/

[23] Budapest Convention on Cybercrime, 2001, Council of Europe - Convention on Cybercrime (ETS No. 185) (europa.eu)

[24] According to the Constitution of Turkey; the Cabinet of Turkey, or Council of Ministers, is the body that regularly assembles under the leadership of President and possesses the supreme executive authority in Turkey.

[25] Official Gazette of the Republic of Turkey, 2012, Cabinet Decision number 2012/3842 on 20 October 2012 of 'Cabinet Decision on Implementing, Administering and Coordination of National Cybersecurity Actions', http://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18.htm

[26] Official Gazette of the Republic of Turkey, 2012, Turkish Cabinet's Decision number 2012/3842 on 11 June 2012, http://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf

- Assuring the cybersecurity of national information technology and communications infrastructure, systems and databases;
- Determining critical infrastructures and strengthening these systems against cyber threats and attacks by monitoring intervention and prevention systems via establishing related centres and supervising/operating them constantly;
- Promoting the development and production of national cybersecurity tools;
- Planning cybersecurity human resources, coordinating personnel training and monitoring their developments;
- Cooperating with other countries and international organisations;
- Increasing cybersecurity awareness amongst citizens; and
- Issuing security certifications to natural and legal persons working in the field of cybersecurity.

In addition to the Transportation and Infrastructure Ministry, the Digital Transformation Office (Dijital Dönüşüm Ofisi -DDO) established by Presidential Decree in July 2018, has been given the task of developing projects that increase information security and cybersecurity. In this context, Presidential Circular No. 2019/12 and Information and Communication Security Measures were published. [27]

In July 2020, the Presidency of the Republic of Turkey Digital Transformation Office published an *Information and Communication Security Guide* which includes information and communication security measures to be taken by public institutions and businesses offering critical infrastructure services. The guide is the first national reference document published in the field. [28]

3.2 Cybersecurity authority and cyber incident response

While policymaking is the responsibility of the Transportation and Infrastructure Ministry, the regulatory function has been assigned to the **Information and Communication Technologies Authority (Bilgi Teknolojileri Kurumu -BTK)**. Established in 2000 as the Telecommunications Authority by the Telegram and Telephone Law of 2000, as amended by the 2008 Electronic Communications Law, it is the first sectoral regulatory body of Turkey.[29]

Even though the Ministry of Transport and Infrastructure acts as the responsible government agency and oversees all other cybersecurity entities, there is a range of government agencies that contributes to ensuring the security of cyberspace in Turkey. The most relevant of these are mentioned below.

The **Presidency of National Intelligence Organisation** (Milli İstihbarat Teşkilatı Başkanlığı -MİT) Department of Electronic and Technical Intelligence is responsible for the surveillance of telecommunications as authorised by law to analyse and store communications information for counter-intelligence purposes and the prevention of terrorist activities. The organisation functions under the State Intelligence Services and National Intelligence Organisation Law of 2014.[30] It engages in image and sound analysis, produces image intelligence (IMINT), deciphers encrypted data and conducts activities against cyber threats.[31]

---

[27] Official Gazette of the Republic of Turkey, 2018, 10/7/2018 - 30474, https://www.mevzuat.gov.tr/mwg-internal/de5fs23hu73ds/progress?id=DHJFxRZke6x92mVzCu2GjMOkXfzkurGtxHNySbcyINw

[28] Information and Security Guide Published, 2020, https://cbddo.gov.tr/en/news/4850/bilgi-ve-iletisim-guvenligi-rehberi-yayimlandi. The Guide is available at https://www.cbddo.gov.tr/en/icsguide.

[29] Information and Communication Technologies Authority, 2015, Information and Communication Technologies Authority (BTK) Establishment, https://www.btk.gov.tr/en-US/Pages/Establishment

[30] Official Gazette of the Republic of Turkey, 2014, "Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununda Değişiklik Yapılmasına Dair Kanun" Law Number: 6532 of 17/04/2014, updating the law "Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu", Law Number: 2937 of 01/11.1983, http://www.resmigazete.gov.tr/eskiler/2014/04/20140426-1.htm

[31] The Presidency of National Intelligence Organisation, 2017, Structure and Departments, http://mit.gov.tr/eng/teskilat.html

The **Turkish National Police** Department of Cyber Crime Prevention provides support for the investigation of crimes committed using information technology and examines and manages digital evidence to ensure that the dispersed structure of provincial law enforcement units does not have any negative effect. It gathers forensic data under a single organisation to prevent duplicating investment and to fight cybercrime effectively and efficiently. The Department was established within the Turkish National Police General Directorate (Emniyet Genel Müdürlüğü -EGM) by Cabinet Decision of 2011.[32]

The **Personal Data Protection Authority** (Kişisel Verileri Koruma Kurulu - KVKK) protects personal data and develops awareness of the issue in the public eye in line with the fundamental rights related to privacy and freedom stated in the Constitution and to establish an environment to enhance the capability of public and private organisations in a data-driven economy. It has nine board members, five of whom are selected by the Grand National Assembly of Turkey and four by the President.[33]

Other Institutions Related to Cybersecurity

The **Presidency of Defence Industries** (Savunma Sanayii Başkanlığı -SSB) was founded in 1985 as the Defence Industry Development and Support Administration Office (Savunma Sanayii Geliştirme ve Destek Başkanlığı -SaGeB) under the Ministry of National Defence.[34] SaGeB's tasks were to set policies regarding the establishment of the infrastructure of the defence industry with the authority and responsibility to apply these policies. Subsequently, it was restructured as the Undersecretariat for Defence Industries (Savunma Sanayii Müsteşarlığı -SSM) in 1989.[35] Since 2017, this organisation has been under and reporting to the Presidency of the Turkish Republic.[36] By legislative decree in 2018,[37] the structure has gone through a reorganisation and has been renamed as the Presidency of the Republic of Turkey Presidency of Defence Industries (T.C. Cumhurbaşkanlığı Savunma Sanayii Başkanlığı – SSB). The cyber defence industry is considered a part of the national defence industry, thus defence projects in the cyber domain are overseen and contracted by SSB with respect to the requirements and strategic plan of Turkish armed forces and national security.

SSB, along with other government bodies like the BTK, holds annual cybersecurity conferences with a different area of focus each year. The International Cyber Warfare and Security Conference (ICWC), which is organised by SSB, and the International Conference on Information Security and Cryptology organised by BTK are two examples of large periodic conferences in the cybersecurity domain in Turkey.

The Scientific and Technological Research Council of Turkey's (Türkiye Bilimsel ve Teknolojik Araştırma Kurumu -TUBITAK) Informatics and Information Security Research Centre (Bilişim ve Bilgi Güveliği İleri Teknolojiler Araştırma Merkezi – BILGEM) operates on information technology, information security and advanced electronics. TUBITAK BILGEM aims to support national R&D activities and simultaneously exercise in-house R&D. It has more than 1,600 personnel to sustain the technological independence of the nation. Institutions within TUBITAK BILGEM have attained hundreds of project achievements in the fields of information security, software and telecommunications. These are the National Research Institute of Electronics and Cryptology (Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü -UEKAE), the Information Technologies Institute (Bilgi Teknolojileri Enstitüsü -BTE), the Advanced Technologies

[32] Official Gazette of the Republic of Turkey, 2013, Cabinet Decision No: 2011/2025, HAKKIMIZDA - EGM Siber Suçlarla Mücadele Daire Başkanlığı (*Name changed to current version by the Ministry of Interior's approval of 28.02.2013*), http://www.siber.pol.tr/Sayfalar/hakkimizda.aspx

[33] Personal Data Protection Authority - KVKK - Kişisel Verileri Koruma Kurumu Başkanlığı, 2017, About Us. http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf

[34] Official Gazette of the Republic of Turkey, 1985, Law No. 3238, Law Regarding Various Regulations of Defence Industry - 07/11/1985 http://www.mevzuat.gov.tr/MevzuatMetin/1.5.3238.pdf

[35] The Presidency of Defence Industries – Savunma Sanayii Başkanlığı, About Us, http://www.ssm.gov.tr/WebSite/contentlist.aspx?PageID=39&LangID=2

[36] Official Gazette of the Republic of Turkey, 2017, Decree-Law No: 696 http://www.resmigazete.gov.tr/eskiler/2017/12/20171224-22.htm

[37] Official Gazette of the Republic of Turkey, 2018, Decree-Law No: 703, http://www.resmigazete.gov.tr/eskiler/2018/07/20180709M3.pdf

Research Institute (İleri Teknolojiler Araştırma Enstitüsü -İLTAREN), the Cybersecurity Institute (Siber Güvenlik Enstitüsü -SGE) and the Software Technologies Research Institute (Yazılım Teknolojileri Enstitüsü -YTE).[38]

Cybersecurity Awareness-Raising Events

Cybersecurity awareness-raising events play an important role in Turkey to maintain information security awareness. By conducting these events, institutions and citizens are informed about cybersecurity threats, general security precautions and policies. Many different means are used to raise cybersecurity awareness, and a few examples are depicted in the following table.

Areas	Events	Responsible Organisations
Training	Cybersecurity Training Programmes, Executive Cyber Training, Cyber Forensics Training, Malware Analysis Training, Master of Science in Cyber/Information Security	Universities, TUBITAK, TAF Cyber Defence Command, Defence Industry Companies
Conferences	Government Cybersecurity Summit,[39] International Cyber Warfare and Security Conference[40]	Transport and Infrastructure Ministry, Presidency of Defence Industries
National Cyber Defence Exercises	National Cyber Defence Exercise,[41] Phishing Exercise, Capture the Flag Exercise, Cyber Shield Exercises	Communications General Directorate, Ministry of Transport and Infrastructure, TAF Cyber Defence Command, TUBİTAK
International Cyber Defence Exercises	NATO Cyber Coalition, Locked Shields, NATO Trident Javelin	TAF Cyber Defence Command, TUBİTAK

Table 1. Awareness-raising activities by various organisations

Cyber crisis management

Under the *National Cybersecurity Strategy and Action Plan 2013-2014*, National CERT and sectoral and institutional sub-CERTs were established within the top government and sectoral agencies and organisations. The official announcement for establishing the National CERT (**USOM**) and sectoral and institutional CERTs (**SOME**) was published in November 2013 and provided guidelines and details to the agencies to form cybersecurity response teams.[42]

USOM was established under BTK and constantly monitors and provides warnings and announcements for cybersecurity incidents. It also establishes national and international coordination for the prevention of cyber-attacks against critical sectors. Additionally, to assist the organisations responsible for forming their own sub-CERTs (SOME), *Guidelines for Establishing and Management of Institutional CERTs* was released.

USOM splits into two subgroups: government CERTs and private sector CERTs. Institutional Cyber Events Response Teams are responsible for the main government institutions and bodies (see Figure

[38] TUBİTAK, BILGEM Informatics and Information Security Research Centre, 2017, Information, http://bilgem.tubitak.gov.tr/en/kurumsal/bilgem-informatics-and-information-security-research-center

[39] Kamu Siber Güvenlik Zirvesi - Government Cybersecurity Summit, 2018, http://www.kamusiberguvenlik.com/

[40] T.C. Cumhurbaşkanlığı, Savunma Sanayii Başkanlığı – The Presidency of Defence Industries, 2018, 3. Uluslararası Siber Savaş ve Güvenlik Konferansı - 3rd International Cyber Warfare and Sacurity Conference, https://www.ssb.gov.tr/Website/contentList.aspx?PageID=1068&LangID=1

[41] Haberleşme Genel Müdürlüğü, 2017, Ulusal Siber Güvenlik Tatbikatı - National Cyber Defence Exercise http://www.hgm.gov.tr/tr/haber/86

[42] Official Gazette of the Republic of Turkey, 2013, Law No 28818, 'Establishing National CERT and sub-CERTs', published 11 November 2013, http://www.resmigazete.gov.tr/eskiler/2013/11/20131111-6.htm

1). Sectoral CERTs specialise in sectors that are recognised as critical infrastructure for the nation: transportation, energy, electronic communications, finance, water management and critical government services. Each CERT operating under a particular organisation, company or institution reports to the particular sectoral CERT. There is no direct connection between the Transport and Infrastructure Ministry and National CERT in daily operations, although the National CERT is under BTK's authority, which is in turn under the Ministry.

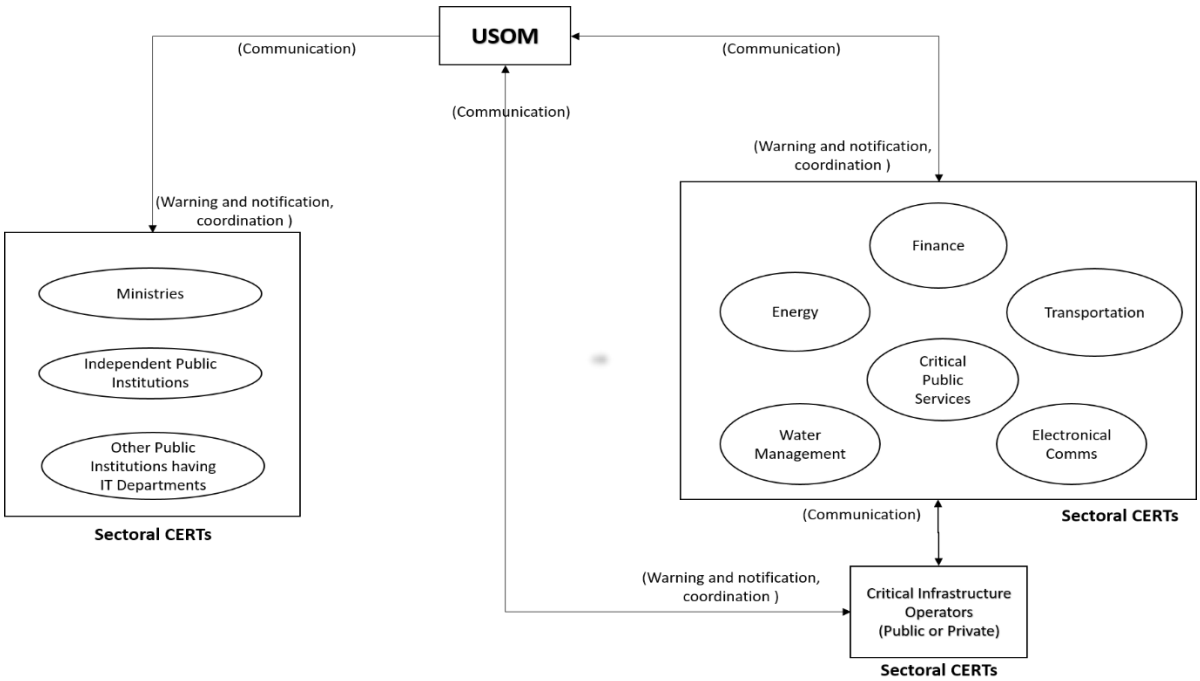

Figure 1. Cybersecurity organisation structure in Turkey[43]

As of 2018, with respect to the current *National Cybersecurity Strategy and Action Plan 2016-2019*, the organisations which have their own sub-CERTs (SOME) were:[44]

- Ministry of Interior
- Ministry of Justice
- Ministry of Treasury and Finance
- Ministry of Commerce
- Ministry of Environment and Urban Planning
- Ministry of Labour, Social Services and Family
- Ministry of Agriculture and Forests
- Ministry of Health
- Ministry of Transport and Infrastructure
    - General Directorate of Highways
    - Directorate General Directorate of State Railroads
    - General Directorate of Maritime and Inland Waters Regulation
    - Directorate General of Civil Aviation
- Information and Communications Technologies Authority (BTK)
- Banking Regulations and Supervision Agency (BDDK)
- Energy Market Regulatory Authority (EPDK)
- Capital Markets Board (SPK)

[43] USOM Sectoral CERTs Establishment and Management Structure, 2014, https://www.usom.gov.tr/dosya/1470335484-Sektorel%20SOME%20Rehberi.pdf

[44] Ministry of Transport and Infrastructure, 2016, 2016-2019 National Cybersecurity Strategy, http://www.udhb.gov.tr/doc/siberg/UlusalSibereng.pdf

3.3 Military cyber defence

Policy framework

The **Turkish Armed Forces** (Türk Silahlı Kuvvetleri - TSK) run their cybersecurity and cyber defence policies and strategies according to existing national, international and NATO standards. Maintaining a continuous synchronisation with the Transport and Infrastructure Ministry and National CERT (USOM) enables the TSK to stay up-to-date with current developments in terms of cyber threats, attacks and technology and avoid duplication of effort.

Turkish military cybersecurity policies and measures are outlined by regulations issued by the Turkish General Staff, which follows the Cabinet's national cybersecurity decisions and related laws.

In keeping up with the continuous evolution of cybersecurity and cyber defence, especially in the last 20 years, the TSK perceives cyber defence as a distinct military domain, correlating to NATO's recognition of cyberspace as a domain of operations in the 2016 Warsaw Summit. To cope with the increasing threats and hostility in cyberspace, whether from state or non-state actors, establishing and maintaining a strong and resilient cyber defence posture and capabilities are among the top priorities of Turkey's defence strategy.

The current cyber defence strategy of the Cyber Defence Command prioritises strengthening the national cyber defence capabilities through recruiting and training new personnel. To support this goal, national defence contractors, universities and technical institutes have been included in the future national defence development plans. To improve these plans coherently, feedback from these actors is constantly incorporated into development efforts.

Structure, key entities and activities

The **Ministry of National Defence** maintains overall responsibility for military cyber defence and holds the highest position with respect to the military cyber domain.

The **Turkish Armed Forces Cyber Defence Command** (Türk Silahlı Kuvvetleri Siber Savunma Komutanlığı) is the top authority for the defence of military networks in Turkey and the top military-CERT (TAF-CERT). TAF-CERT functions as the outer layer of TAF military networks and interface between NATO (NATO Computer Incident Response Capability – NCIRC), National CERT and subordinate military CERTs. In the command structure, the Command is positioned under the Communications, Electronics and Information Systems Directorate (J6 – Turkish: Muhabere Elektronik Bilgi Sistemleri – MEBS) of the Turkish General Staff.

The Cyber Defence Command is a joint command that has personnel from all services. To sustain a high level of synchronisation and coordination, an active communications channel is maintained between the Transport and Infrastructure Ministry and other government organisations. Cyber Defence Command also conducts coordination and joint activities with NATO cyber entities and organisations and participates in multinational cyber exercises and NATO missions.

National cyber defence exercises are conducted annually by different parties to measure the resilience of public institutions against cyber threats, for both military and non-military cyber defence objectives. The main purpose of the exercises is to train to be able to act proactively against threats to national interests or citizens, to prevent attacks, to eliminate them and to develop countermeasures.[45]

To contribute to Turkey's cyber capabilities and efforts in military networks and purposes, the TSK participates in domestic and international cyber exercises, which are given high importance; this remains one of the top priorities of the TSK for the cyber domain. Cyber drills and cyber incident response exercises are run regularly.

[45] Haberleşme Genel Müdürlüğü, 2017, Etkinlik - Ulusal Siber Savunma 2017 Tatbikatı – National Cyber Defence Exercise, http://www.hgm.gov.tr/tr/etkinlik/24.

R&D and financing

Under the modernisation programme of the Cyber Defence Command, a new Military-CERT command centre, a dedicated cyber defence training laboratory, a military networks monitoring facility and related support structures have been developed. The funding for these processes and transformations has come from the national defence budget. Research and development projects under the *National Cybersecurity Strategy and Action Plan 2016-2019* have been awarded to top defence industry contractors and universities and the research agenda and plans are pursued in cooperation with TUBİTAK and the UEKAE institute.

3.4 Engagement with the private sector

The number of private cybersecurity companies in Turkey has increased rapidly in the last couple of years. Today, more than 100 companies conduct business in the field of cybersecurity. The private sector has also evolved in terms of capacity. While during the first years of the industry, most national companies were just distributors of global companies offering information security counselling and penetration testing, they have matured in recent years and are now developing products and technologies, cybersecurity solutions and operational services for the sector.[46]

With the efforts of the private sector operating in the national defence industry, comprehensive research outcomes and reports are continuously published. As an example, the *Cyber Threat Situation Report of Turkey* is published by STM (Savunma Teknolojileri Mühendislik ve Ticaret A.Ş.) several times a year aims to inform the public and government officials about the dynamics and recent incidents in national cybersecurity.[47]

Training is provided by academic institutions, government organisations, civil society organisations and private organisations. Some universities in Turkey have cybersecurity Master's degree programmes to train cybersecurity experts. A few notable faculties that offer such programmes are Middle East Technical University,[48] Gebze Technical University,[49] Hacettepe University[50] and Marmara University.[51]

In recent years, Turkey has put considerable effort into the process of clustering different actors in a national cybersecurity domain. In October 2017, the Presidency of Defence Industries (SSB) invited the major cybersecurity companies in the private sector to discuss this and possible cooperation among those bodies further.[52] There is no legal obligation for private industry to take part in such cooperation – the emphasis is on mutual trust and cooperation between public and private institutions. The key motivation was strengthening buyer-supplier relationships, common distribution channels, common pools of work and R&D activities conducted by universities with companies that can create better opportunities and benefits for both sides. Because of the common economic interests, companies in the cluster are more productive, more innovative and therefore more competitive than the companies operating alone.

---

[46] STM A.Ş., 2018, Company Profile, https://www.stm.com.tr/en/about-us/company-profile; HAVELSAN, 2018, Our Capabilities, http://www.havelsan.com.tr/ENG/Main/icerik/937/our-capabilities.

[47] STM A.Ş., 2017, Siber Tehdit Durum Raporu, https://www.stm.com.tr/documents/file/Pdf/Siber%20Tehdit%20Durum%20Raporu%20Ocak-Mart%202017.pdf

[48] Orta Doğu Teknik Üniversitesi, 2017, Middle East Technical University Cybersecurity Program https://ii.metu.edu.tr/cybersecurity-ms.

[49] Gebze Teknoloji Üniversitesi, 2017 Gebze Technical University Cybersecurity Program. http://anibal.gyte.edu.tr/ects/?dil=en&bolum=1041&tip=yukseklisans&duzey=ucuncu.

[50] Hacettepe Üniversitesi, 2017 Hacettepe Universíty Information Security Maste'rs Program http://www.bilisim.hacettepe.edu.tr/bilgi_guvenligi.php.

[51] Marmara Üniversitesi, 2017, Marmara University Cybersecurity Master's Program, http://llp.marmara.edu.tr/organisasyon.aspx?kultur=tr-tr&Mod=2&ustbirim=5200&birim=5236&altbirim=5238&program=1142&organisasyonId=847&mufredatTurId=932001

[52] Savunma Sanayii Başkanlığı, 2018, Siber Güvenlik Kümelenmesi Basın Bülteni 28.06.2018 (Cybersecurity Clustering Press Release 28.06.2018). https://www.ssb.gov.tr/website/contentList.aspx?PageID=1209&LangID=1

References

Policy

Information and Communication Technologies Authority, 2015, Information and Communication Technologies Authority (BTK) Establishment, https://www.btk.gov.tr/en-US/Pages/Establishment

Official Gazette of the Republic of Turkey, 2012, Cabinet Decision number 2012/3842 on 20 October 2012 of 'Cabinet Decision on Implementing, Administering and Coordination of National Cybersecurity Actions', http://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18.htm

Official Gazette of the Republic of Turkey, 2012, Turkish Cabinet's Decision number 2012/3842 on 11 June 2012, http://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf

Official Gazette of the Republic of Turkey, 2018, 10/7/2018 - 30474, https://www.mevzuat.gov.tr/mwg-internal/de5fs23hu73ds/progress?id=DHJFxRZke6x92mVzCu2GjMOkXfzkurGtxHNySbcyINw

Information and Communication Technologies Authority, 2015, Information and Communication Technologies Authority (BTK) Establishment, https://www.btk.gov.tr/en-US/Pages/Establishment

Ministry of Transport and Infrastructure, 2016, 2016-2019 National Cybersecurity Strategy, http://www.udhb.gov.tr/doc/siberg/UlusalSibereng.pdf

Official Gazette of the Republic of Turkey, 2014, "Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununda Değişiklik Yapılmasına Dair Kanun" Law Number: 6532 of 17/04/2014, updating the law "Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu", Law Number: 2937 of 01/11.1983, http://www.resmigazete.gov.tr/eskiler/2014/04/20140426-1.htm

The Presidency of National Intelligence Organisation, 2017, Structure and Departments, http://mit.gov.tr/eng/teskilat.html

Official Gazette of the Republic of Turkey, 1985, Law No. 3238, Law Regarding Various Regulations of Defence Industry - 07/11/1985 http://www.mevzuat.gov.tr/MevzuatMetin/1.5.3238.pdf

The Presidency of Defence Industries – Savunma Sanayii Başkanlığı, About Us, http://www.ssm.gov.tr/WebSite/contentlist.aspx?PageID=39&LangID=2

TUBİTAK, BILGEM Informatics and Information Security Research Centre, 2017, Information, http://bilgem.tubitak.gov.tr/en/kurumsal/bilgem-informatics-and-information-security-research-center

Personal Data Protection Authority - KVKK - Kişisel Verileri Koruma Kurumu Başkanlığı, 2017, About Us. http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf

Kamu Siber Güvenlik Zirvesi - Government Cybersecurity Summit, 2018, http://www.kamusiberguvenlik.com/

Ministry of Transport and Infrastructure, Ulusal Siber Güvenlik Stratejisi ve 2013 - 2014 Eylem Planı, 2013, http://www.udhb.gov.tr/doc/siberg/SOME_2013-2014_EylemPlani.pdf

Official Gazette of the Republic of Turkey, 2013, Law No 28818, 'Establishing National CERT and sub-CERTs', published 11 November 2013, http://www.resmigazete.gov.tr/eskiler/2013/11/20131111-6.htm

Ministry of Transport and Infrastructure, 2016, 2016-2019 National Cybersecurity Strategy, http://www.udhb.gov.tr/doc/siberg/UlusalSibereng.pdf

Law

Official Gazette of the Republic of Turkey, 2000, Law No 4502 dated 27 January 2000, http://www.mevzuat.gov.tr/MevzuatMetin/1.5.4502.pdf

Official Gazette of the Republic of Turkey, 2008, Telgraf ve Telefon Kanunu 1924 Law No: 406, http://www.mevzuat.gov.tr/MevzuatMetin/1.3.406.pdf

Official Gazette of the Republic of Turkey, 2016, Personal Data Protection Law No: 6698, https://www.kisiselverilerinkorunmasi.org/kanunu-6698-sayili/

Official Gazette of the Republic of Turkey, 2011, Information and Communication Technologies Authority Establishment Law (Bilgi Teknolojileri ve İletişim Kurumunun Kuruluşuna İlişkin Kanun 1983), Law No: 2813 / 1983, http://www.mevzuat.gov.tr/MevzuatMetin/1.5.2813.pdf

According to the Constitution of Turkey; the Cabinet of Turkey, or Council of Ministers, is the body that regularly assembles under the leadership of President and possesses the supreme executive authority in Turkey.

Official Gazette of the Republic of Turkey, 2008, Cabinet Decision Law No. 5809, http://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18.htm

Official Gazette of the Republic of Turkey, 2017, Decree-Law No: 696 http://www.resmigazete.gov.tr/eskiler/2017/12/20171224-22.htm

Official Gazette of the Republic of Turkey, 2018, Decree-Law No: 703, http://www.resmigazete.gov.tr/eskiler/2018/07/20180709M3.pdf

Official Gazette of the Republic of Turkey, 2013, Cabinet Decision No: 2011/2025, HAKKIMIZDA - EGM Siber Suçlarla Mücadele Daire Başkanlığı (Name changed to current version by the Ministry of Interior's approval of 28.02.2013), http://www.siber.pol.tr/Sayfalar/hakkimizda.aspx

Other

T.C. Cumhurbaşkanlığı, Savunma Sanayii Başkanlığı – The Presidency of Defence Industries, 2018, 3. Uluslarası Siber Savaş ve Güvenlik Konferansı - 3rd International Cyber Warfare and Sacurity Conference, https://www.ssb.gov.tr/Website/contentList.aspx?PageID=1068&LangID=1

Haberleşme Genel Müdürlüğü, 2017, Ulusal Siber Güvenlik Tatbikatı - National Cyber Defence Exercise http://www.hgm.gov.tr/tr/haber/86

Haberleşme Genel Müdürlüğü, 2017, Etkinlik - Ulusal Siber Savunma 2017 Tatbikatı – National Cyber Defence Exercise, http://www.hgm.gov.tr/tr/etkinlik/24

STM A.Ş., 2018, Company Profile, https://www.stm.com.tr/en/about-us/company-profile

HAVELSAN, 2018, Our Capabilities, http://www.havelsan.com.tr/ENG/Main/icerik/937/our-capabilities

STM A.Ş., 2017, Siber Tehdit Durum Raporu, https://www.stm.com.tr/documents/file/Pdf/Siber%20Tehdit%20Durum%20Raporu%20Ocak-Mart%202017.pdf

Orta Doğu Teknik Üniversitesi, 2017, Middle East Technical University Cybersecurity Program https://ii.metu.edu.tr/cybersecurity-ms

Gebze Teknoloji Üniversitesi, 2017 Gebze Technical University Cybersecurity Program. http://anibal.gyte.edu.tr/ects/?dil=en&bolum=1041&tip=yukseklisans&duzey=ucuncu

Hacettepe Üniversitesi, 2017 Hacettepe Universíty Information Security Master's Program http://www.bilisim.hacettepe.edu.tr/bilgi_guvenligi.php

Marmara Üniversitesi, 2017, Marmara University Cybersecurity Master's Program, http://llp.marmara.edu.tr/organisasyon.aspx?kultur=tr-tr&Mod=2&ustbirim=5200&birim=5236&altbirim=5238&program=1142&organisasyonId=847&mufredatTurId=932001

Savunma Sanayii Başkanlığı, 2018, Siber Güvenlik Kümelenmesi Basın Bülteni 28.06.2018 (Cybersecurity Clustering Press Release 28.06.2018). https://www.ssb.gov.tr/website/contentList.aspx?PageID=1209&LangID=1

Figures and Tables

Acronyms

BDDK	Bankacılık Düzenleme ve Denetleme Kurumu – Banking Regulations and Supervision Agency
BİLGEM	Informatics and Information Security Research Centre
BTE	Information Technologies Institute
BTK	Bilgi Teknolojileri ve İletişim Kurumu – Information and Communication Technologies Authority
EGM	Emniyet Genel Müdürlüğü - Turkish National Police General Directorate
EPDK	Enerji Piyasası Düzenleme Kurumu – Energy Market Regulatory Authority
İLTAREN	Advanced Technologies Research Institute
KVKK	Kişisel Verileri Koruma Kurumu – Personal Data Protection Authority
MEBS	Communications, Electronics and Information Systems Directorate (J6)
MİT	Milli İshtihbarat Teşkilatı Başkanlığı – The Presidency of National Intelligence Organisation
SaGeB	Defence Industry Development and Support Administration Office
SGE	Cybersecurity Institute
SPK	Sermaye Piyasası Kurumu – Capital Markets Board
SSB	Savunma Sanayii Başkanlığı – The Presidency of Defence Industries
TBMM	Türkiye Büyük Millet Meclisi – The Grand National Assembly of Turkey
TSK	Türk Silahlı Kuvvetleri – Turkish Armed Forces (TAF)

TUBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu – The Scientific and Technological Research Council of Turkey
TÜİK	Türkiye İstatistik Kurumu – Turkish Statistical Institute
UAB	Ministry of Transport and Infrastructure
UEKAE	National Research Institute of Electronics and Cryptology
USOM	Ulusal Siber Olaylara Müdahale Merkezi – Turkish National CERT
YTE	Software Technologies Research Institute