CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

National Cyber Security Organisation: TURKEY

Ensar Şeker, İhsan Burak Tolga

National Cyber Security Governance Series

Tallinn 2018

About this study

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

Primarily focusing on NATO Nations that are Sponsoring Nations to the NATO CCDCOE, each country report outlines the division of cyber security roles and responsibilities between agencies, describes their mandate, tasks, and competences as well as coordination between them. In particular, it covers the mandates of political and strategic management; operational cyber security 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 cyber security strategy objectives in order to clarify the context for the organisational approach in a particular nation.

CCDCOE

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) is a NATO-accredited cyber defence hub focusing on research, training and exercises. It represents a community of 21 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 2.0, 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 in Tallinn the International Conference on Cyber Conflict, CyCon, a unique event bringing together key experts and decision-makers of the global cyber defence community. As of January 2018, CCDCOE is 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 its member nations, currently: Austria, Belgium, the Czech Republic, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Portugal, Slovakia, Spain, Sweden, 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 Cyber Security Organisation in the Czech Republic

National Cyber Security Organisation in Estonia

National Cyber Security Organisation in France

National Cyber Security Organisation in Hungary

National Cyber Security Organisation in Italy

National Cyber Security Organisation in Lithuania

National Cyber Security Organisation in the Netherlands

National Cyber Security Organisation in Poland

National Cyber Security Organisation in Spain

National Cyber Security Organisation in Slovakia

National Cyber Security Organisation in the United Kingdom

National Cyber Security Organisation in the United States

China and Cyber: Attitudes, Strategies, Organisation

National Cyber Security Organisation in Israel

Series editor: Kadri Kaska (NATO CCD COE)

Information in this document has been checked for accuracy as of November 2018.

Table of Contents

1. Digital society

Population	*Country total*	80.8 million[1] (TUİK Türkiye İstatistik Kurumu 2018)
	Internet users	67% (July 2017 est.) 61% of population between ages 16-74[2]
Connectivity	*Fixed and mobile subscriptions per 100 inhabitants*	78% (2016)[3]
	Household internet access	76%[4]
	Broadband connections	78% of internet users, of which 72.4% have mobile and 40% landline connections
GDP	*Total*	$851,46 billion[5] (OECD 2018)
Digitalisation	*Integration of Smart Automation Systems in Production Lines*	33% (2016 est.)[6]

1.1 Digital public services

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 the citizens from commuting and losing time between institutions, while also 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.

In 2017, nearly half of the adult population (42% among 16-74 years-olds) used the internet to interact with governmental agencies and organisations and to use governmental services for personal purposes. The figure has grown quickly from the previous year's 37%.[2] In recent years, the most used services of e-government were provided by the public organisations such as Social Security Institution, Revenue Administration, Ministry of Justice, National Police, and General Directorate of Land Registry and Cadastre.[7] Over a third of those online interactions with governmental organisations involved seeking information about governmental services. Some of the most popular facilities included queries to the national health database for individual uses, tax reports and billing, mobile communications service

,[1] Türkiye İstatistik Kurumu - Turkish Statistical Institute, 2018, Adrese Dayalı Nüfus Kayıt Sistemi Sonuçları 2017, Nr: 27587, http://www.tuik.gov.tr/PreHaberBultenleri.do?id=27587

[2] Türkiye İstatistik Kurumu - Turkish Statistical Institute, 2017, Hanehalkı Bilişim Teknolojileri Kullanım Araştırması 2017. Nr: 23862, http://www.tuik.gov.tr/PreHaberBultenleri.do?id=24862

[3] Türkiye İstatistik Kurumu - Turkish Statistical Institute, 2016, Hanehalkı Bilişim Teknolojileri Kullanım Araştırması 2016, Nr: 21779, http://www.tuik.gov.tr/PreHaberBultenleri.do?id=21779

[4] Ibid.

[5] T.C. Sanayi ve Teknoloji Bakanlığı (Republic of Turkey Ministry of Science, Industry and Technology), OECD Economic Outlook, Developments in Individual OECD and Selected Non-member Economies 2017, Volume 2018, Issue 1

[6] T.C. Sanayi ve Teknoloji Bakanlığı, 2017, Dijital Türkiye Yol Haritası, Issue 1, https://www.sanayi.gov.tr/tsddtyh.pdf

[7] e-Devlet Portali Örnek Uygulamalar – e-Government Portal Sample Applications, 2018, http://www.edevlet.gov.tr/ornek-uygulamalar/#1463557923217-4e5071d4-9db8

inquiries, court and legal record inquiries and statistics, social security transactions, road administration services, and personal information updates.

As of 2018, Turkey's e-government services primarily cover:[8]

- 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 unions services, medical appointments, records and queries related to governmental 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 governmental services hub (e-government).[9] The Ministry oversees the regular operation of entire e-government services from a supervisory position, delegates cyber security related responsibilities to other governmental organisations and sustains coordination between related services of other ministries and governmental agencies.

According to 2015 data, public sector information technology investments reached $1.38 billion annually and hold 6.9% of all public sector investments.[10]

As an important step in the efforts of digitalisation of public services, in a circular dated 3 December 2016 from the National Cyber Security Board, it was announced that the information networks of all governmental organisations and institutions would be incorporated into KamuNet (government-use virtual network) to sustain more secure communication across different governmental bodies.[11]

1.2 Digitalisation in business

Online commerce is steadily gaining popularity in Turkey, and 25% of people between 16-74 years old used online commercial services to purchase products or services for personal purposes in 2016. This was 21% higher than in the previous year.[12] The volume of online commerce has also been on the

[8] e-Devlet Portali Uygulamalar – e-Government Applications, 2018, http://www.edevlet.gov.tr/ornek-uygulamalar/#1463557923217-4e5071d4-9db8

[9] 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

[10] T.C. Kalkınma Bakanlığı, Kamu Bilgi ve İletişim Teknolojileri Yatırımları, 2016 - e-Devlet İçin Genel Görünüm, Issue: 1, 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

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

[12] Türkiye İstatistik Kurumu - Turkish Statistical Institute, 2017, Hanehalkı Bilişim Teknolojileri Kullanım Araştırması 2017, Issue: 24862, http://www.tuik.gov.tr/PreHaberBultenleri.do?id=24862.

steady rise over the last few years, and in 2016 the total online commerce market volume reached $10.6 billion. In retail, the online commerce market volume rose by 34% from 2013 to 2016.[13]

Electronic commerce activities are regulated by the *Law on Regulation of Electronic Commerce*, passed by the Grand National Assembly of Turkey (TBMM) in 2014.[14] All public regulatory activities and secondary legislation on e-commerce were tasked to the **Ministry of Trade**.[15] 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.[16] Studies have been directed by the Ministry of Trade and are currently in progress to determine the required future strategy and to identify other parties to participate in coordinated efforts and to decide on actions to be taken.[17]

By September 2017, 96% of newly established companies in Turkey had internet access, showing a slight increase from 94% in 2016. Among those companies, access to and use of the internet is nearly universal (99.7%) for those who have more than 250 employees. The vast majority of new companies have broadband internet access, 75% have a company website, and over 10% have successfully completed at least one online transaction via their web pages, online stores or smartphone applications (94%, 73% and 11% respectively).[18]

To project the rate of uptake of e-government applications for business operations, as of 2016, 86% of recently founded companies used e-government services at least once for their business-related matters.[19]

---

[13] TÜSİAD, 2017 Dijitalleşen Dünyada Ekonominin İtici Gücü – E-Ticaret (Driving Force of E-commerce in Digitalizing World), TÜSİAD-T/2017, 04-587, https://tusiad.org/tr/tum/item/download/8585_56f011d864462b2d0bf20b29439e6022

[14] 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

[15] 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%20e-ticaret%20tarih%C3%A7esi%20devam%C4%B1.pdf?lve

[16] 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

[17] Ministry of Development, 2015, Bilgi Toplumu Stratejisi - Action no. 53 'Establishment of e-Export Strategy' in the Information Society Strategy and Action Plan 2015-2018, http://www.bilgitoplumustratejisi.org/tr

[18] Türkiye İstatistik Kurumu - Turkish Statistical Institute, 2017, Girişimlerde Bilişim Teknolojileri Kullanım Araştırması 2017 Dönemi, http://www.tuik.gov.tr/PreTablo.do?alt_id=1048#

[19] 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

2. National cybersecurity strategy and legal framework

2.1 National strategy

The current national cybersecurity strategy, *National Cyber Security Strategy and Action Plan 2016-2019*, was released in March 2016 by the **National Cyber Security Board** (see Section 3.1).[20] It covers the time period of 2016-2019, as designated by the Board. The document serves as a guideline for all governmental organisations, agencies, officials and legal entities.

Like its predecessor *National Cyber Security Strategy and Action Plan of 2013 – 2014,*[21] the mission of the current strategy and action plans is summarised in the opening statement: '[…] establishing national cyber security, designating and coordinating efficient and sustainable policies and implementing the practising of these policies'.

The *Strategy and Action Plan* emphasises that cyber security is an inseparable part of national security and call for all administrative and technical precautions to ensure the security of all national entities in cyberspace. The strategy is broken down to three sub-parts:

(1) Ensuring the security, secrecy, and privacy of all the data, services, transactions and the systems in information technologies domain, while covering the entire national cyberspace;
(2) Designating cyber security actions related to keeping the impact of cyber-attacks under a reasonable threshold and systems available and running; and assisting governmental and law enforcement agencies in investigating and forensics with related cybercrimes; and
(3) Taking necessary action to make systems and infrastructure that are mission critical for cyber security, secrecy and privacy, manufactured and developed within the nation.

The *National Cyber Security Strategy and Action Plan* is to be updated with respect to the fast-paced evolution of technology and regulations in the domain, as stated in the document itself.

2.2 Legal framework

In order to designate the structure and responsibilities of Ministry of Transport and Infrastructure, the Telegram and Telephone Law of 2000[22] distributed policymaking, regulation, and operation functions in the communications domain, amending the basic laws of the telecommunications sector – the 1924 Law of Telegram and Telephone[23] and the 1983 Law on Establishing Information and Communication Technologies Authority'.[24]

---

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

[21] 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

[22] 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

[23] 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

[24] 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

The Telecommunications Authority, established in 2000, is the first sectoral regulatory body in Turkey. To improve legislative clarity, create competition in the sector, reduce uncertainties for operators and allocate resources to R&D, the Electronic Communications Law came into force in November 2008.[25]

3. Cybersecurity governance

3.1 Political and strategic level management

By Cabinet[26] decision of October 2012 on implementing, administering and coordinating national cyber security actions, the preparation and coordination of policy, strategy and action plans regarding the governance of national cyber security were given to the **Ministry of Transport and Infrastructure**, which acts as the responsible governmental agency and oversees all other cyber security entities through the state.[27]

The Ministry has been overseeing and conducting cyber security activities at the strategic level with the **National Cyber Security Board** (established in 2013)[28] and USOM (Ulusal Siber Olaylara Müdahale Merkezi, the Turkish National CERT) directed by BTK (Bilgi Teknolojileri ve İletişim Kurumu), the **Information and Communication Technologies Authority**.

Hence, all governmental organisations, agencies, officials and legal entities are mandated to follow policies and standards set by the National Cyber Security Board, in particular, the *National Cyber Security Strategy and Action Plan* released by the National Cyber Security Board.

By decision of the Turkish Cabinet of June 2012, the Ministry of Transport and Infrastructure has responsibility for national cyber security and is able to form councils and working groups on conducting practices for fulfilling its given responsibility regarding national cyber security.[29]

The Ministry of Transport and Infrastructure is also responsible for:

- Preparing strategy and action plans to ensure national cyber security;
- Preparing procedures and principles for ensuring the security and privacy of information and data belonging to the public, institutions, and organisations;
- Ensuring cyber security of national information technologies, communication infrastructures, 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 any kind of national solutions and cyber-attack intervention tools in the provision of national cyber security;
- Planning and coordinating the development and training of the necessary and sufficient number of specialised personnel for critical institutions and positions in terms of national cyber security;
- Cooperating with other countries and international organisations;

---

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

[26] 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.

[27] 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 Cyber Security Actions', http://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18.htm

[28] Ibid.

[29] 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

- Increasing awareness and training about cyber security; and
- Giving security certifications by determining the principles and procedures for real and legal persons working in the field of training, testing, and solution of information security.

3.2 Operational-level prevention and response

While policymaking is the responsibility of the Ministry of Transportation and Infrastructure, the regulatory function is assigned to the **Information and Communication Technologies Authority (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.[30]

National and sectoral CERTs

Following the National Cyber Security Action Plan 2013-2014,[31] it was decided to establish a National CERT and sectoral and institutional sub-CERTs among the top governmental / sectoral agencies and organisations. An official announcement on establishing the national **USOM** (Ulusal Siber Olaylara Müdahale Merkezi – National CERT) and sectoral **SOME** (Sektörel ve Kurumsal Siber Olaylara Müdahale Ekipleri – Sectoral and Institutional CERTs) was published in November 2013, providing guidelines and details for forming the relevant cyber security response teams.[32]

USOM was established under BTK, the Information and Communication Technologies Authority, and constantly monitors and provides warnings and announcements for cyber security 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, the national CERT, is split into two subgroups for governmental CERTs and private sector CERTs. Institutional Cyber Events Response Teams are responsible for the main governmental institutions and bodies (see Figure 1). Sectoral CERTs are established and specialise in sectors that are recognised as critical infrastructure for the nation: transportation, energy, electronic communications, finance, water management, and critical governmental services. Each CERT operating under a particular organisation, company or institution, thus reports to the particular sectoral CERT. There is no direct connection between the Ministry of Transport and Infrastructure and National CERT in daily operations, although the National CERT is located under the Information Technologies and Communications Authority's (BTK) domain of authority, which is in turn located under the Ministry.

As of 2018, with respect to the current *National Cyber Security Strategy and Action Plan 2016-2019*, the organisations which have their own sub-CERTs (SOME) are:[33]

- 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

---

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

[31] 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

[32] 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

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

- 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)

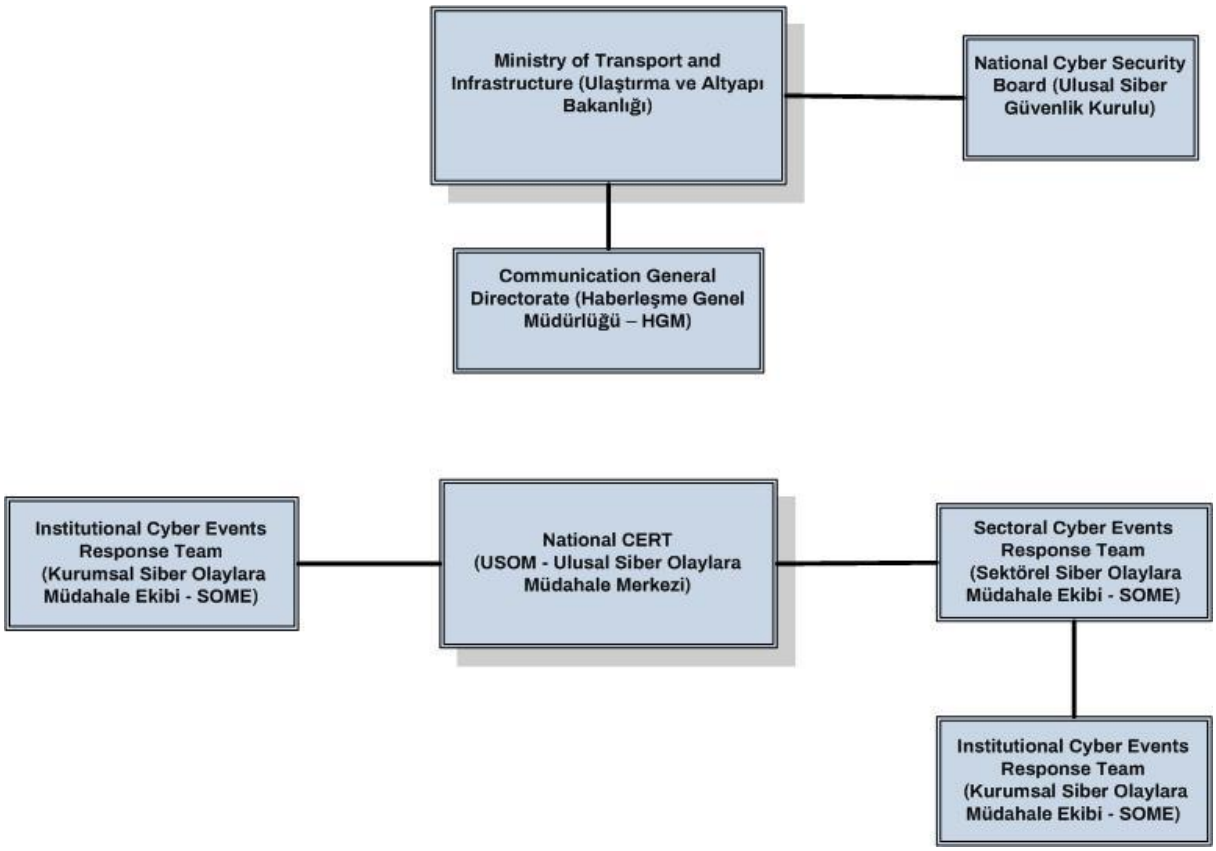

Figure 1. Top level cyber security organisation structure in Turkey[34]

National Cyber Security Board

Supplementary Article 1 added to the *Electronic and Communications Law* established Turkey's **National Cyber Security Board**.[35] The Board is responsible for approving the plans, programmes, reports, procedures, principles, and standards prepared by the governmental bodies that are represented on the board and ensuring their implementation and coordination, to determine the measures to be taken by public institutions and organisations and natural and legal persons in relation to national cyber security. The Cyber Security Board is the top governmental organisation regarding the governance of national cyber security. The level of representation of the ministries and public institutions

[34] Ibid.

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

and organisations involved in the National Cyber Security Board and its members is determined by the Ministerial Cabinet. The Board's other responsibilities are;

- To approve policies, strategies and action plans related to cyber security and to make the necessary decisions for effective implementation of it throughout the country;
- To bid on proposals for the identification of critical infrastructures;
- To determine the institutions and organisations to be exempted from all or some of the provisions related to cyber security; and
- To perform other duties given by law.

The National Cyber Security Board coordinates and prepares the National Cyber Security Strategy and Action Plans. It involves the following agencies and organisations:[36]

- Ministry of Transport and Infrastructure
- Ministry of Foreign Affairs
- Ministry of Interior
- Ministry of National Defence
- The Presidency of National Intelligence Organisation
- Turkish Armed Forces General Staff
- Information and Communications Technologies Authority (BTK)
- Scientific and Technological Research Council of Turkey (TUBITAK)
- Financial Crimes Investigation Board.

3.3 Other public sector bodies

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

The **Presidency of Defence Industries** (SSB – Savunma Sanayii Başkanlığı) was founded in 1985 as the Defence Industry Development and Support Administration Office (SaGeB) under the Ministry of National Defence.[37] The 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, the SaGeB was restructured as the Undersecretariat for Defence Industries (SSM – Savunma Sanayii Müsteşarlığı) in 1989.[38] Since 2017, this organisation has been located under and reporting to the Presidency of Turkish Republic.[39] By legislative decree in 2018,[40] the structure has gone through a reorganisation and has been renamed as 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 the 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.

---

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

[37] 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

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

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

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

SSB, along with other governmental bodies like the BTK, holds annual cyber security 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-scale periodic conferences in Turkey in the cyber security domain.

The **Scientific and Technological Research Council of Turkey's** (TUBITAK) Informatics and Information Security Research Centre (BILGEM) operates on information technology, information security, and advanced electronics. The aim of TUBITAK BILGEM is to support national R&D activities and simultaneously exercise in-house R&D activities; 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 institutions are the National Research Institute of Electronics and Cryptology (UEKAE), the Information Technologies Institute (BTE), the Advanced Technologies Research Institute (İLTAREN), the Cyber Security Institute (SGE) and the Software Technologies Research Institute (YTE).[41]

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 roof to prevent duplicating investment and to fight cybercrime effectively and efficiently. The Department of Cyber Crime Prevention was established within the Turkish National Police General Directorate (EGM) by a Cabinet Decision of 2011.[42]

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

Personal Data Protection Authority (KVKK) provides protection for 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 the competition of the public and private organisations in the world of the 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.[43]

Cyber security awareness-raising events play an important role in Turkey in ensuring awareness of information security and threats to cyber security, general security precautions, organisational information security policies, social media and information on cyber security in mobile devices, and in informing the public about cyber security legislation studies and measures. Many different methods are used to raise cyber security awareness in the public by different actors, and a few examples are given in the following table.

---

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

[42] 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

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

Areas	Events	Responsible Organisations
Training	Cyber Security 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 Cyber Security Summit,[44] International Cyber Warfare and Security Conference[45]	Ministry of Transport and Infrastructure, Presidency of Defence Industries
National Cyber Defence Exercises	National Cyber Defence Exercise,[46] Military Networks Cyber Defence Exercises, Cyber Shield Exercises	Communications General Directorate, Ministry of Transport and Infrastructure, TAF Cyber Defence Command, TUBİTAK, BTK
International Cyber Defence Exercises	NATO Cyber Coalition, Locked Shields, NATO Trident Javelin	TAF Cyber Defence Command, TUBİTAK

3.4 Military cyber defence

Policy framework

The **Turkish Armed Forces** (TSK) runs their cyber security and cyber defence policies and strategy according to existing national, international and NATO standards. Maintaining a continuous synchronisation with the Ministry of Transport and Infrastructure as the top national cyber security authority and with the National CERT (USOM) are held as top priorities, enabling the TSK to stay up to date with current developments in terms of cyber threats, attacks and technology, and to avoid duplication of effort.

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

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

National cyber defence exercises are conducted annually by different parties to measure the competence of the 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.[47]

---

[44] Kamu Siber Güvenlik Zirvesi - Government Cyber Security Summit, 2018, http://www.kamusiberguvenlik.com/

[45] 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

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

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

To contribute to Turkey's cyber capabilities and efforts in military networks and purposes, the Turkish Armed Forces participate in domestic and international cyber exercises, which are given high importance; this remains one of the top priorities of Turkish Armed Forces with respect to the cyber domain. Cyber drills and cyber incident response exercises are run on a regular basis.

Structure and key entities

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 (NCIRC), national CERT and subordinate military CERTs. In the in the command structure, the Turkish Armed Forces Cyber Defence Command is positioned under the Communications, Electronics and Information Systems Directorate (J6 – Turkish: 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 communication channel is maintained between the Ministry of Transport and Infrastructure (TÜBİTAK) and other governmental organisations. The TAF Cyber Defence Command also conducts coordination and joint activities with NATO cyber entities and organisations, and participates in multinational cyber exercises and missions of NATO in this regard.

The current cyber defence strategy of Cyber Defence Command prioritises strengthening the national cyber defence capabilities through recruiting and training new personnel. To support this aim, national defence contractors, universities and technical institutes are included in the new future national defence development plans. In order to improve these plans in a concurrent manner, feedback from these actors is constantly incorporated into these development efforts.

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 2016-2019 National Cyber Security Strategy and Action Plan, 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.

3.5 Cyber intelligence

The **Presidency of National Intelligence Organisation** (MİT – Milli İstihbarat Teşkilatı Başkanlığı) 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.[48] It engages in image and sound analysis, produces image intelligence (IMINT), deciphers encrypted data and conducts activities against cyber threats.[49]

[48] 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

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

3.6 Private sector engagement

The number of private cyber security companies in Turkey has increased rapidly in the last couple of years. Today, more than 100 companies carry on business in the field of cyber security; just 5-6 years ago, this number was between 10 and 20. The private sector has also evolved in capacity. While in the first years of the industry most were distributors for global companies offering information security counselling and penetration testing, they have matured in recent years and are now developing products and technologies, cyber security solutions and operational services.[50] [51]

With the efforts of the private sector operating in the national defence industry, comprehensive research outcomes and reports are continuously published. As an example, *Cyber Threat Situation Report of Turkey* is published several times a year aims to inform the public and governmental officials about the dynamics and recent incidents in national cyber security.[52]

Relevant training is provided by academic institutions, governmental organisations, civil society organisations and private organisations. Some universities in Turkey have cyber security Master's degree programmes to train cyber security experts. A few notable faculties that offer such programmes are Middle East Technical University,[53] Gebze Technical University,[54] Hacettepe University[55] and Marmara University.[56]

In recent years, Turkey has put considerable effort into the process of clustering different actors in a national cyber security domain. In October 2017, the Presidency of Defence Industries (SSB) invited the major cyber security companies in the private sector to discuss this matter further and the possible cooperation among those bodies.[57] Although there is no legal obligation for private industry to take part in such cooperation, the emphasis is kept on the mutual trust and cooperation between public and private institutions. The key motivation behind these effort is 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 participating sides. Because of the common economic interests, companies in the cluster are more productive, more innovative and therefore more competitive than companies operating alone.[58]

---

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

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

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

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

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

[55] Hacettepe Üniversitesi, 2017 Hacettepe Universíty Information Security Masters Program http://www.bilisim.hacettepe.edu.tr/bilgi_guvenligi.php

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

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

[58] Çifci, Hasan., 2017, Her Yönüyle Siber Savaş (2nd ed.), TUBİTAK Yayınları, Ankara.

References

Legislation

Official Gazette of the Republic of Turkey, Bilgi Teknolojileri ve İletişim Kurumunun Kuruluşuna İlişkin Kanun - Information and Communication Technologies Authority Establishment Law, Law Nr: 2813, 1983, http://www.mevzuat.gov.tr/MevzuatMetin/1.5.2813.pdf

Official Gazette of the Republic of Turkey, Savunma Sanayii Müsteşarlığı'nın Kurulması Hakkında Kanun – Law Regarding the Establishment of Undersecretariat of Defence Industry, Law No. 3238 07.11.1985, https://www.ssb.gov.tr/Images/Uploads/MyContents/F_20170913104007039980.pdf

Official Gazette of the Republic of Turkey, Telgraf ve Telefon Kanunu, Ulaştirma Bakanliğinin Teşkilat ve Görevleri Hakkinda Kanun, Telsiz Kanunu ve Posta, Telgraf ve Telefon İdaresinin Biriktirme ve Yardım Sandığı Hakkında Kanun ile Genel Kadro ve Usulü Hakkinda Kanun Hükmünde Kararnamenin Eki Cetvellerde Değişiklik Yapılmasına Dair Kanun - Law Amending Certain Articles of the Telegram and Telephone Law, Law on Organisation and Responsibilities of the Ministry of Transport and Wireless Law, Law on Savings and Aid Fund of the Posts Telegraphs and Telephone Administration and Organisational Charts attached to the Decree with the Decree-Law on the General Cadres and Procedures, Law No 4502 dated as 27.01.2000, https://www.tbmm.gov.tr/kanunlar/k4502.html, Retrieved on 07.11.2018

Official Gazette of the Republic of Turkey, Bakanlar Kurulu Kararı, Cabinet Decision No. 2006/10316, 2012, http://www.resmigazete.gov.tr/eskiler/2006/04/20060420-3.htm

Official Gazette of the Republic of Turkey, Cabinet Decision (No: 2011/2025) Cabinet Decision regarding the Establishment of Department of Defence against Crimes of Information Technologies, http://www.resmigazete.gov.tr/eskiler/2011/07/20110715-1.htm

Official Gazette of the Republic of Turkey, Cabinet Decision number 2012/3842, Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar - Cabinet Decision regarding Implementing, Administering and Coordination of National Cyber Security Actions, http://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18.htm

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

Official Gazette of the Republic of Turkey, Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ – Notification regarding Establishing, Mission and Functions of National CERTs, Notification No. 28818, 11 November 2013. http://www.resmigazete.gov.tr/eskiler/2013/11/20131111-6.htm

Official Gazette of the Republic of Turkey, Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununda Değişiklik Yapılmasına Dair Kanun – Law regarding the Amendment State Intelligence Services and National Intelligence Organization Law, Law Number: 6532 Date: 17/04/2014, updating Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu – State Intelligence Services and National Intelligence Organization Law, Law Number: 2937 Date: 01/11.1983 http://www.resmigazete.gov.tr/eskiler/2014/04/20140426-1.htm

Official Gazette of the Republic of Turkey, Law regarding Electronic Commerce No. 6563, 23.10.2014. http://www.resmigazete.gov.tr/eskiler/2014/11/20141105-1.htm

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

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

Official Gazette of the Republic of Turkey, Decree-Law No. 703 Decree Law Regarding the Changes in Various Decree Laws in order to Aligning with the Changes in Constitution, http://www.resmigazete.gov.tr/eskiler/2018/07/20180709M3.pdf

Policy documents

Ministry of Transport and Infrastructure, 2016-2019 Ulusal Siber Güvenlik Stratejisi, 2016-2019 National Cyber Security Strategy, 2016, http://www.udhb.gov.tr/doc/siberg/UlusalSibereng.pdf

Ministry of Strategy and Budget, Information Society Strategy and Action Plan 2015-2018, Bilgi Toplumu Stratejisi, http://www.bilgitoplumustratejisi.org/tr

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

Reports

Türkiye İstatistik Kurumu - Turkish Statistical Institute, 2016, Hanehalkı Bilişim Teknolojileri Kullanım Araştırması 2016, Nr: 21779, http://www.tuik.gov.tr/PreHaberBultenleri.do?id=21779

Türkiye İstatistik Kurumu - Turkish Statistical Institute, 2017, Hanehalkı Bilişim Teknolojileri Kullanım Araştırması 2017, Issue: 24862, http://www.tuik.gov.tr/PreHaberBultenleri.do?id=24862

Ministry of Economy, Türkiye'de e-Ticaretin Tarihçesi – The History of E-Commerce in Turkey, 2017, https://www.ekonomi.gov.tr/portal/content/conn/UCM/path/Contribution%20Folders/web/Hizmet%20Ticareti/Elektronik%20Ticaret/T%C3%BCrkiyede%20e-ticaret%20tarih%C3%A7esi%20devam%C4%B1.pdf?lve

Türkiye İstatistik Kurumu - Turkish Statistical Institute, Adrese Dayalı Nüfus Kayıt Sistemi Sonuçları 2017 Nr: 27587, http://www.tuik.gov.tr/HbPrint.do?id=27587

OECD iLibrary, OECD Economic Outlook, Developments in Individual OECD and Selected Non-member Economies, Volume 2018, Issue 1, OECD Publishing, Paris

STM, Siber Tehdit Durum Raporu – Cyber Threats Situation Report, 2017, https://www.stm.com.tr/documents/file/Pdf/Siber%20Tehdit%20Durum%20Raporu%20Ocak-Mart%202017.pdf

T.C. Kalkınma Bakanlığı – Ministry of Development, Kamu Bilgi ve İletişim Teknolojileri Yatırımları – Investments on Government Information and Communication Technologies, 2016, http://www.bilgitoplumu.gov.tr/wp-content/uploads/2016/09/Kamu_BIT_Yatirimlari_2016.pdf

Türkiye İstatistik Kurumu - Turkish Statistical Institute, 2017, Girişimlerde Bilişim Teknolojileri Kullanım Araştırması 2017 Dönemi, http://www.tuik.gov.tr/PreTablo.do?alt_id=1048#

Other

T.C. Cumhurbaşkanlığı Savunma Sanayii Başkanlığı, 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

Personal Data Protection Authority - KVKK Kişisel Verileri Koruma Kurumu Başkanlığı, Hakkımızda - About Us, http://www.kvkk.gov.tr/en/misyon-vizyon.html

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

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

Çifci, Hasan., 2017, Her Yönüyle Siber Savaş (2nd ed.) – Complete Cyber Warfare, TUBİTAK Yayınları, Ankara

The Presidency of National Intelligence Organization, Teşkilat – Organization, http://mit.gov.tr/eng/teskilat.html

Ministry of Industry and Technology, Dijital Türkiye Yol Haritası – Turkey Digital Transformation Roadmap, 2017 https://www.sanayi.gov.tr/tsddtyh.pdf

e-Devlet Türkiye, e-Devlet İçin Genel Görünüm – General Look for e-Government, 2018, http://www.edevlet.gov.tr/e-devlet-icin-genel-gorunum/

e-Devlet Portali Uygulamalar – e-Government Applications, 2018, http://www.edevlet.gov.tr/ornek-uygulamalar/#1463557923217-4e5071d4-9db8

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

Gebze Technical University, Gebze Technical University Cyber Security Program, 2018 http://anibal.gyte.edu.tr/ects/?dil=en&bolum=1041&tip=yukseklisans&duzey=ucuncu

Hacettepe Universíty, Hacettepe Universíty Information Security Masters Program, 2018, http://www.bilisim.hacettepe.edu.tr/bilgi_guvenligi.php

Ministry of Interior General Directorate of Security – EGM, Siber Suçlarla Mücadele Daire Başkanlığı – Department of Defence Against Cyber Crimes, 2018, http://www.siber.pol.tr/Sayfalar/hakkimizda.aspx

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

Information and Communication Technologies Authority, Kuruluş – Establishment, https://www.btk.gov.tr/en-US/Pages/Establishment

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

Marmara University, Cyber Security Master's Programme, 2018, http://llp.marmara.edu.tr/organizasyon.aspx?kultur=tr-tr&Mod=2&ustbirim=5200&birim=5236&altbirim=5238&program=1142&organizasyonId=847&mufredatTurId=932001

Middle East Technical University, Middle East Technical University Cyber Security Programme, 2018, https://ii.metu.edu.tr/cybersecurity-ms

T.C. Cumhurbaşkanlığı Savunma Sanayii Başkanlığı – The Presidency of Defence Industries, Siber Güvenlik Kümelenmesi Basın Bülteni 28.06.2018 - Cyber Security Clustering Press Release 28.06.2018, https://www.ssb.gov.tr/website/contentList.aspx?PageID=1209&LangID=1

STM, Şirket Profili - Company Profile, 2017, https://www.stm.com.tr/en/about-us/company-profile

TÜSİAD, 2017 Dijitalleşen Dünyada Ekonominin İtici Gücü – E-Ticaret - Driving Force of E-commerce in Digitalizing World, TÜSİAD-T/2017, 04-587, https://tusiad.org/tr/tum/item/download/8585_56f011d864462b2d0bf20b29439e6022

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

Figures

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	Cyber Security 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