Dominika Liszkowska*

Türkiye's Cybersecurity Policy Framework

Abstract

The Internet and cyberspace are a gradually developing structure. Every second, new devices, systems and users connect within the network, which causes constant growth and changes in the sphere of threats arising from cyberspace. Türkiye is one of the countries in the world most exposed to cyber threats. However, one of its goals was to bring the field of cybersecurity to an international level. The aim of this article is to present the framework of Türkiye's cybersecurity policy and answer the following questions: What steps have been taken in Türkiye to protect the state and society against the effects of threats in cyberspace? In which areas has Türkiye achieved significant progress in cyberspace protection, and which are still the biggest challenges?

Key words: Türkiye, cybersecurity, Türkiye's cybersecurity policy, cyberspace, security Policy

* PhD Dominika Liszkowska, Faculty of Humanities, Koszalin University of Technology, ORCID: 0000-0001-6312-341X.

Introduction

The progress and development of new ICT technologies and the emergence of a new, previously unknown zone of operation, or cyberspace (even in the sphere of public administration), forced the state authorities to pay attention to the issue of cybersecurity. In order to achieve the effectiveness of the undertaken activities, it was necessary to develop appropriate plans, which ultimately led to the creation of strategies of individual countries in this area[1]. Thus, a fundamental evolution in shaping government policy was visible, as a result of which cybersecurity became one of the priorities in the field of state security[2].

Currently, every system transferred to cyberspace carries new and serious threats. Cyberattacks have become more frequent, more complex and destructively targeted. Their implementers, despite using basic methods, are able to attack even the best (as it might seem) secured government resources[3]. In addition, IT systems, which are part of the state's critical infrastructure, also require special protection. Nowadays they manage such important elements as energy, fuel, food and water supply systems, but also financial, transport and health care systems[4]. Any damage to their functioning may lead to paralysis of the state and, as a consequence, to huge financial losses.

Türkiye is one of the most technologically, economically and institutionally developed countries in the Middle East. It is also one of the states most exposed to cyber threats in the world[5]. At the same time, according to the Global Cybersecurity Index's (GCI) report published in 2019, Türkiye has become one of the 20 safest countries in the world in terms of cybersecurity and 11th in Europe[6]. In February 2021, the Minister of Transport and Infrastructure of Türkiye – Adil Karaismailoğlu announced that the number of cyberattacks on

1 K. Chochowski, *Strategia cyberbezpieczeństwa jako przejaw polityki administracyjnej*, „Zeszyty Naukowe Uniwersytetu Rzeszowskiego. Prawo" 2019, no. 107, p. 209.
2 *Cybersecurity Policy Making at a Turning Point Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy*, https://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf [access: 5.10.2023].
3 *Cyber Security*, https://cbddo.gov.tr/en/cyber-security [access: 5.10.2023].
4 J. Wrona, *Prace naczelnych organów administracji państwowej a cyberbezpieczeństwo Polski*, „Białostockie Studia Prawnicze" 2016, no. 20B, p. 467.
5 O. Eitan, *Turkey—Challenges to the Struggle against Cyber Threats*, „Cyber, Intelligence, and Security" 2018, vol. 2, no. 1, p. 39–41.
6 *Turkey reveals its three-year cybersecurity plan*, https://www.trtworld.com/magazine/turkey-reveals-its-three-year-cybersecurity-plan-42820 [access: 5.10.2023].

Türkiye decreased from 118,470 in 2020 to 84,113 in 2021[7]. This includes the result of steps taken in recent years to contribute to reducing existing gaps in the defense system against cyber threats. However, according to the criteria assessed by the National Cyber Security Index, actions taken in some areas related to ensuring security in cyberspace are still insufficient.

The aim of this article is to present the framework of Türkiye's cybersecurity policy and answer the following questions: What steps have been taken in Türkiye to protect the state and society against the effects of threats in cyberspace? In which areas has Türkiye achieved significant progress in cyberspace protection, and which are still the biggest challenges? The research methods used to answer these questions are desk research and institutional and legal analysis. They were used in the study of normative acts relating to cyberspace and cybersecurity, the source of which were the Turkish authorities.

An Outline of the Institutional and Legal Framework of Cybersecurity Policy in Türkiye

Regulations regarding cyber law began to be developed in Türkiye in the early 1990s[8]. In turn, the most comprehensive regulation regarding national cybersecurity initiatives was Decision no. 2012/3842 of the Council of Ministers issued in June 2012. Cybersecurity activities were then prepared in connection with the issued document of the Council of Ministers entitled: „Execution, management and coordination of national activities in in the field of cybersecurity". The purpose of this document was to regulate the principles and procedures that constitute the framework for the operation of public organizations and institutions. These regulations concern taking the necessary measures to ensure the security and confidentiality of services, processes, data and systems used in the provision of these services, as well as the management and operation of critical infrastructure in the field of ICT systems[9].

7 *Cyberattacks targeting Turkey dropped in 2021*, https://www.dailysabah.com/turkey/cyberattacks-targeting-turkey-dropped-in-2021/news [access: 5.10.2023].

8 N. Akyeşilmen, *Türkiye in the Global Cybersecurity Arena: Strategies in Theory and Practice*, „Insight Turkey" 2022, vol. 24, no. 3, p. 124.

9 T. Sevim, *Turkey: Cybersecurity*, https://www.dataguidance.com/opinion/turkey-cybersecurity [access: 5.10.2023].

Decision of the Council of Ministers no. 2012/3842, a Law on Electronic Communications (to which the relevant articles were added in 2014), defines the obligations and powers of the Ministry of Transportation, Maritime Affairs and Communication (currently the Ministry of Transport and Infrastructure) in the field of cybersecurity. This ministry is responsible for the implementation and administration of the government services node (e-government). In addition, its tasks include regular supervision of the functioning of Turkish e-government services, delegation of cybersecurity-related responsibilities to other government organizations, and coordination of cooperation with other government ministries and agencies[10]. Moreover, in accordance with the Law on Electronic Communications, the Ministry of Transport and Infrastructure is responsible for: 1) preparing strategies and action plans to maintain state cybersecurity; 2) constructing procedures and policies to ensure the security and privacy of information belonging to public and private institutions; 3) ensuring cybersecurity of the national IT and communication infrastructure, systems and databases; 4) identifying critical infrastructures and strengthening their systems to prevent cyber threats and attacks, through monitoring and continuous supervision of intervention and prevention systems; 5) increasing citizens' awareness of cybersecurity; 6) promoting the development of national cybersecurity tools; 7) planning human resources in the field of cybersecurity, as well as coordinating staff training and monitoring their development; 8) issuing security certificates to natural and legal persons operating in the field of cybersecurity; 9) cooperation with other countries and international organizations in the field of cybersecurity[11].

Until 2018, the most important government organization dealing with national cybersecurity management was the National Cybersecurity Council (Siber Güvenlik Kurulu), established by the decision of the Council of Ministers of June 11, 2012[12]. This institution was established to determine the actions that should be taken by public institutions and organizations as well as natural and legal persons in the field of cybersecurity. In addition, it was entrusted with the responsibility for approving prepared plans, programs, reports, procedures, rules and standards, as well as ensuring their implementation and

10 E. Halisdemir, *National Cybersecurity Organisation: Turkey*, Tallinn 2021, p. 6.
11 Ibidem, p. 10.
12 *Siber Güvenlik Kurulu*, https://www.btk.gov.tr/siber-guvenlik-kurulu [access: 5.10.2023].

coordination[13]. Pursuant to Art. 67, par. 1, of the Electronic Communications Law (Law no. 5809), the council's responsibilities include: a) approving cybersecurity policies, strategies and action plans and making the necessary decisions for their effective implementation throughout the country; b) deciding on proposals for the identification of critical infrastructures; c) identification of institutions and organizations that will be exempt from all or part of the cybersecurity regulations[14]; as well as fulfilling other obligations arising from the law. The first meeting of the Cybersecurity Council took place on December 21, 2012. During the meeting, the „obligations, work procedures and principles of the Cybersecurity Council Directive" were adopted, as well as the „National Cybersecurity Strategy and 2013–2014 Action Plan[15]". Since the entry into force of the provisions of Circular no. 2018/3, the responsibilities and powers of the Cyber Security Council have been taken over by the Presidency of the Republic of Türkiye.

In the strategy for 2013–2014 adopted by decree, the main goals of the state in the field of cyberspace were: 1) ensuring the security of all types of services, transactions and data that public institutions and organizations transmit via information technologies and systems used to present them; 2) ensuring the security of IT systems included in critical infrastructure operated by the public or private sector; 3) defining strategic activities in the field of cybersecurity. This was to be done so as to keep the effects of cybersecurity incidents at a minimum. The systems were also to be ensured that they would return to normal operation as quickly as possible after each incident. Moreover, activities were also to be ensured more effective investigation into the crimes[16].

Some cybersecurity tasks have also been transferred to the Information and Communications Technology Authority (ICTA) (included in the amendments to the Electronic Communications Act of 2016). ICTA is the body responsible for taking the necessary actions to protect public institutions, the private sector and individuals against cyberattacks[17]. Cybersecurity responsibilities and functions assigned under revised the Electronic Communications Act (no. 5809)

13 *Elektronik Haberleşme Kanunu, Kanun Numarası: 5809, Kabul Tarihi: 5/11/2008*, https://www.uab.gov.tr/uploads/pages/siber-guvenlik/5809-ehb.pdf [access: 5.10.2023].
14 Ibidem.
15 *Siber Güvenlik Kurulu...*
16 *Siber Güvenlik Stratejisi ve Eylem Planı*, https://www.btk.gov.tr/siber-guvenlik-stratejisi-ve-eylem-plani [access: 5.10.2023].
17 *Türkiye*, https://cyberpolicyportal.org/states/turkey [access: 5.10.2023].

include: 1) ensuring the confidentiality of information and communications security; 2) ensuring network protection against unauthorized access; 3) taking measures provided for in Turkish law to ensure national security, public order, security of public services, in accordance with the requirements of the electronic communications sector; 4) carrying out duties assigned by the Council of Ministers, the Ministry and/or the Cybersecurity Council in the field of cybersecurity and internet domain names (through the ICTA Presidency or other entities); 5) taking all measures to protect public institutions and organizations, natural and legal persons against cyber-attacks and to ensure deterrence against such attacks[18].

As part of ICTA (in accordance with the National Cybersecurity Strategy and 2013–2014 Action Plan), by decision of May 27, 2013, the National Cyber Incident Response Center (USOM, TR-CERT – Ulusal Siber Olaylara Müdahale Merkezi, Turkish National CERT) was established. Moreover, Cyber Incident Response Teams (Institutional SOME, Sectoral SOME) have been established in public institutions and organizations. Both USOM and SOME are crucial to eliminating cyber incidents, as well as prioritizing and mitigating possible damage. Moreover, both structures at the national level coordinate activities and cooperate in the management of cyber incidents in order to ensure cyber security in the country[19]. The units operate 24 hours a day, 7 days a week, generating alarms, warnings and notifications. In addition, TR-CERT also conducts activities to raise awareness and prepare institutions and organizations for possible cyber attacks[20].

In 2016, a new document „National Cybersecurity Strategy and Action Plan 2016–2019" was published in Türkiye. The strategy was intended to contribute to maintaining cyber security at a manageable and acceptable level. New goals were set as: 1) strengthening the cyber defence and protection of critical infrastructures, 2) combating cyber crimes, 3) improvement of awareness and human resources, 4) developing a cyber security ecosystem, 5) integration of cyber security to the national security[21]. The first comprehensive strategy and action plan for e-government („The 2016–2019 National eGovernment Strategy and Action Plan") was also developed for

18 Ibidem.
19 *USOM Hakkında*, https://www.usom.gov.tr/hakkimizda [access: 5.10.2023].
20 *Türkiye…*
21 *2016–2019 National Cyber Security Strategy*, https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/ulusalsibereng.pdf [access: 5.10.2023].

the same period. Its goal was to provide the accelerated actions needed to drive Türkiye's digital transformation in order to achieve social, economic and environmental development. Developing Türkiye's potential in this area has become an integral element aimed at improving the state's prosperity in line with Türkiye's Vision 2023[22].

As a result of examining the effects of technological development, trends in cyber threats, national needs and international practices, another National Strategy and Action Plan in the field of Cybersecurity for 2020–2023, developed by the Ministry of Transport and Infrastructure, was published in 2020[23].

Steps and Challenges Undertaken in Türkiye to Ensure Cybersecurity

In August 2023, Türkiye was ranked 55th in the National Cyber Security Index (scoring 61.04 points[24]). This index lists countries that have the best solutions in the world that guarantee IT systems security[25]. The issues that continue to pose the greatest challenge to Türkiye are the analysis and information on cyber threats, assessed on the basis of, among others, a report containing an analysis of the cyber threat situation in the country, published at least once a year. Moreover, Türkiye has not established a sufficient protection system for digital and essential services. In this respect, there is a lack of, among others: a competent cyber/information security authority with powers to supervise public and private digital service providers responsible for implementing cyber/information security requirements and also a competent cyber/information security authority with the power to supervise operators of essential services regarding cyber/information security requirements. The issue of military cyber operations also raises great reservations. According to the GCI report, the Turkish Armed Forces do not have a unit (cyber command, etc.) that specializes in planning and conducting cyber operations. Moreover,

22 *Digital Public Administration factsheet 2021. Turkey*, p. 13, https://joinup.ec.europa.eu/sites/default/files/inline-files/DPA_Factsheets_2021_Turkey_vFinal.pdf [access: 5.10.2023].
23 Ibidem, p. 11.
24 *55th National Cyber Security Index*, *Türkiye*, https://ncsi.ega.ee/country/tr/ [access: 5.10.2023].
25 J. Chustecki, *Polska na wysokim miejscu w rankingu NCSI*, https://www.computerworld.pl/news/Polska-na-wysokim-miejscu-w-rankingu-NCSI,444184.html [access: 5.10.2023].

over the last three years, the armed forces have not conducted exercises in the field of cyber operations or exercises with an element of cyber operations in the country. However, over the past three years, a team of Turkish military officials has participated in international exercises related to cyber operations[26].

Despite issues that still require refinement, Türkiye has made many significant steps in developing its cybersecurity policy in recent years. The first is the appointment of a government entity supervising cybersecurity activities at the strategic level, which is the Ministry of Transport and Infrastructure (formerly the Ministry of Transport, Maritime Affairs and Communications), acting jointly with the Presidency of the Republic of Türkiye and the USOM[27]. A national cybersecurity strategy has also been established, called the „National Cybersecurity Strategy and Action Plan (2020–2023)". This document (as previously mentioned) was prepared by the Turkish Ministry of Transport and Infrastructure in cooperation with universities, non-governmental organizations, as well as the private and public sectors[28]. It sets out eight strategic goals: 1) Protecting critical infrastructure and increasing its resilience; 2) Developing national capabilities; 3) Organic cybersecurity network; 4) Security of next-generation technologies; 5) Fighting cybercrime; 6) Development of domestic and national technologies and their support; 7) Integration of cybersecurity with national security; 8) Development of international cooperation[29]. In turn, Chapter 10 of the National Cybersecurity Strategy contains a plan for its implementation[30].

Significant steps have also been taken in the protection of personal data. This issue was regulated on March 24, 2016, and then published in the Official Journal on April 7, 2016 (no. 29677) as Turkish Personal Data Protection Law no. 6698[31]. Pursuant to Art. 1, this document was adopted to establish the protection of fundamental human rights and freedoms, in particular the privacy of personal life (within the processing of personal data). In addition, it

26 *National Cyber Security Index*...

27 *Turkey. Status regarding Budapest Convention*, https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/turkey/pop_up [access: 5.10.2023].

28 *Turkey reveals its three-year*...

29 *Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020–2023)*, https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-2020-2023.pdf [access: 5.10.2023].

30 Ibidem.

31 *Turkish Personal Data Protection Law, no. 6698, Enacted on 24/3/2016*, https://www.kisiselverilerinkorunmasi.org/kanunu-ingilizce-ceviri/ [access: 5.10.2023].

specifies the obligations of natural and legal persons processing personal data, as well as the procedures and principles to be followed[32]. The Personal Data Protection Authority (Kişisel Verileri Korunma Kurumu) is responsible for the protection of personal data in Türkiye. It has administrative and financial independence and public legal personality. This office is based in Ankara, and its decision-making body is the Council, which is an autonomous body. It consists of nine members, five of whom are elected by the Grand National Assembly of Türkiye and four by the President[33].

Issues related to cybercrimes have been defined in Turkish law. Provisions on cybercrime are included in the Turkish Penal Code (no. 5237), the Code of Criminal Procedure (no. 5271), as well as the laws no. 6706 on international legal cooperation in criminal matters and no. 5651 on the regulation of broadcasting on the Internet and combating committed crimes via internet broadcast. The mentioned Turkish legislation covers substantive crimes, procedural rules, as well as rules on international cooperation[34]. Pursuant to Art. 243 of the Turkish Penal Code (no. 5237) of September 26, 2004, anyone who unlawfully accesses or remains in all or part of an information system is liable to imprisonment for up to one year or a fine. In turn, in the case of the crime of fraud (Art. 158, para. 1, point f), a person using IT systems, banks or credit institutions as a tool may be subject to imprisonment from four to ten years and a court fine[35].

In the following years, in addition to the extensive legal framework regarding technical aspects, other important legal acts were introduced relating to the issue of operation in cyberspace. The Electronic Communications Law (Law no. 5809) of November 5, 2008 was introduced to create effective competition in the electronic communications sector. In this respect, it has become necessary (Art. 1) to regulate and supervise, protect consumer rights, expand services throughout the country, effectively use resources, support technological development and new investments in the area of infrastructure, as well as create communication networks and services and establish

32 *Kişisel Verilerin Korunması Kanunu*, *Kanun Numarası: 6698*, *Kabul Tarihi: 24/3/2016*, https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5 [access: 5.10.2023].

33 Ibidem.

34 *Turkey. Status regarding Budapest...*

35 *Türk Ceza Kanunu*, *Kanun Numarası: 5237*, *Kabul Tarihi: 26/9/2004*, https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5237.pdf [access: 5.10.2023].

procedures and rules related to them[36]. On October 24, 2014, the Law (no. 6563) on the Regulation of Electronic Commerce in Türkiye was also adopted. It regulated the rules and procedures for electronic commerce. This document defined the issue of commercial communication, obligations of service providers and intermediary service providers, as well as communication taking place via electronic communication tools. In addition, the obligation to provide information regarding contracts and e-commerce and sanctions applied in this area is regulated[37].

In order to combat cybercrime, there is a Department for Combating Cybercrime, established within the structure of the Directorate General. It was established in 1997 under the name Computer Crime Unit. Then it became a unit for counteracting computer crimes[38]. Pursuant to the Regulation of the Council of Ministers of 2011 (no. 2011/2025), in order to prevent duplication of activities and contribute to the effective and efficient fight against cybercrime, heads of departments dealing with investigations into crimes committed using information technology and the examination of digital evidence were combined. They were previously concentrated in a dispersed structure of voivodeship units[39]. Based on the Minister's decision of February 28, 2013, the department gained a new name, or Department for Combating Cybercrime[40]. As of June 2018, this department operated in 76 of Türkiye's 81 provinces and employed approximately 27,000 employees, 562 of whom were IT and material control experts[41].

In November 2021, the decision of the Council of Judges and Prosecutors (Hâkimler ve Savcılar Kurulu – HSK) was published. It announced the establishment of cybercrime courts in Türkiye. These courts were considered to be criminal courts specializing in cybercrimes defined, among others, as qualified theft committed using IT systems, qualified fraud by presenting a person as a public official or institution and organization, or improper use

36 *Elektronik Haberleşme Kanunu*, *Kanun Numarası: 5809*, *Kabul Tarihi: 5/11/2008*...

37 *Elektronik Ticaretin Düzenlenmesi Hakkında Kanun*, *Kanun No. 6563*, *Kabul Tarihi: 23/10/2014*, https://www.resmigazete.gov.tr/eskiler/2014/11/20141105-1.htm [access: 5.10.2023].

38 F. Kızılkoyun, *'Anti-cybercrime department' monitors 45 million social media users in Turkey*, https://www.hurriyetdailynews.com/anti-cybercrime-department-monitors-45-million-social-media-users-in-turkey-133362 [access: 05.10.2023].

39 *Siber Suçlarla Mücadele Daire Başkanlığı*: *Hakkımızda*, https://www.egm.gov.tr/siber/hakkimizda2 [access: 5.10.2023].

40 Ibidem

41 F. Kızılkoyun, op. cit.

of bank or credit cards[42]. The establishment of cybercrime courts was considered necessary due to the increase in disputes in the area of cyberspace. Moreover, their functioning is intended to enable the unification of practice in the light of developing technology.

Conclusions

Currently, Türkiye ranks 11th in the Global Cybersecurity Index and 55th in the National Cyber Security Index. One of the goals of this state in 2023, or on the 100th anniversary of the founding of the Republic, is to bring the field of cybersecurity to an international level. Since 2018, the Presidency of the Republic of Türkiye, which carries out the duties and powers of the Cybersecurity Council, is engaged in developing the next cybersecurity strategy for public institutions and critical infrastructure in relation to the policy determined by the President. The strategy prepared for the coming years is to define Türkiye's new action plan in the process of transition from „e-government" to „digital government". Preparations, taking into account the most urgent needs of the state and international trends, are carried out within the following strategic priority areas: 1) strategic alignment and governance, 2) data governance in the public sector, 3) digital skills, 4) digital inclusion and participation, 5) technological infrastructures, 6) service design and delivery[43].

Bibliography

Akyeşilmen N., *Türkiye in the Global Cybersecurity Arena: Strategies in Theory and Practice*, „Insight Turkey" 2022, vol. 24, no. 3.

Chochowski K., *Strategia cyberbezpieczeństwa jako przejaw polityki administracyjnej*, „Zeszyty Naukowe Uniwersytetu Rzeszowskiego. Seria Prawo" 2019, no. 107.

Chustecki J., *Polska na wysokim miejscu w rankingu NCSI*, https://www.computerworld.pl/news/Polska-na-wysokim-miejscu-w-rankingu-NCSI,444184.html [access: 5.10.2023].

Cyber Security, https://cbddo.gov.tr/en/cyber-security [access: 5.10.2023].

Cyberattacks targeting Turkey dropped in 2021, https://www.dailysabah.com/turkey/cyberattacks-targeting-turkey-dropped-in-2021/news [access: 5.10.2023].

42 M. Koruturk, İ.N. Dolu, *Turkey establishes Specialized Courts for Cyber Crimes!*, https://legal.deris.com/en/news/it-law/317-turkey-establishes-specialized-courts-for-cyber-crimes [access: 5.10.2023].

43 *Digital Government Strategy*, https://cbddo.gov.tr/en/digital-government-strategy/ [access: 5.10.2023].

Cybersecurity Policy Making at a Turning Point Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy, https://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf [access: 5.10.2023].

Digital Government Strategy, https://cbddo.gov.tr/en/digital-government-strategy/ [access: 5.10.2023].

Digital Public Administration factsheet 2021. Turkey, https://joinup.ec.europa.eu/sites/default/files/inline-files/DPA_Factsheets_2021_Turkey_vFinal.pdf [access: 5.10.2023].

Eitan O., *Turkey–Challenges to the Struggle against Cyber Threats*, „Cyber, Intelligence, and Security" 2018, vol. 2, no. 1.

Elektronik Haberleşme Kanunu, *Kanun Numarası: 5809*, *Kabul Tarihi: 5/11/2008*, https://www.uab.gov.tr/uploads/pages/siber-guvenlik/5809-ehb.pdf [access: 5.10.2023].

Elektronik Ticaretin Düzenlenmesi Hakkında Kanun, *Kanun No. 6563*, *Kabul Tarihi: 23/10/2014*, https://www.resmigazete.gov.tr/eskiler/2014/11/20141105-1.htm [access: 5.10.2023].

Halisdemir E., *National Cybersecurity Organisation: Turkey*, Tallinn 2021.

Kişisel Verilerin Korunması Kanunu, *Kanun Numarası: 6698*, *Kabul Tarihi: 24/3/2016*, https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5 [access: 5.10.2023].

Kızılkoyun F., *Anti-cybercrime department' monitors 45 million social media users in Turkey*, https://www.hurriyetdailynews.com/anti-cybercrime-department-monitors-45-million-social-media-users-in-turkey-133362 [access: 5.10.2023].

Koruturk M., Dolu İ.N., *Turkey establishes Specialized Courts for Cyber Crimes!*, https://legal.deris.com/en/news/it-law/317-turkey-establishes-specialized-courts-for-cyber-crimes [access: 5.10.2023].

National Cyber Security Index, *Türkiye*, https://ncsi.ega.ee/country/tr/ [access: 5.10.2023].

Sevim T., *Turkey: Cybersecurity*, https://www.dataguidance.com/opinion/turkey-cybersecurity [access: 5.10.2023].

Siber Güvenlik Kurulu, https://www.btk.gov.tr/siber-guvenlik-kurulu [access: 5.10.2023].

Siber Güvenlik Stratejisi ve Eylem Planı, https://www.btk.gov.tr/siber-guvenlik-stratejisi-ve-eylem-plani [access: 5.10.2023].

Siber Suçlarla Mücadele Daire Başkanlığı, https://www.egm.gov.tr/siber/hakkimizda2 [access: 5.10.2023].

Türk Ceza Kanunu, *Kanun Numarası: 5237*, *Kabul Tarihi: 26/9/2004*, https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5237.pdf [access: 5.10.2023].

Turkey reveals its three-year cybersecurity plan, https://www.trtworld.com/magazine/turkey-reveals-its-three-year-cybersecurity-plan-42820 [access: 5.10.2023].

Turkey. Status regarding Budapest Convention, https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/turkey/pop_up [access: 5.10.2023].

Turkish Personal Data Protection Law, *no. 6698*, *Enacted on 24/3/2016*, https://www.kisiselverilerinkorunmasi.org/kanunu-ingilizce-ceviri/ [access: 5.10.2023].

Türkiye, https://cyberpolicyportal.org/states/turkey [access: 5.10.2023].

2016–2019 National Cyber Security Strategy, https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/ulusalsibereng.pdf [access: 5.10.2023].

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020–2023), https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-2020-2023.pdf [access: 5.10.2023].

USOM Hakkında, https://www.usom.gov.tr/hakkimizda [access: 5.10.2023].

Wrona, J., *Prace naczelnych organów administracji państwowej a cyberbezpieczeństwo Polski*, „Białostockie Studia Prawnicze" 2016, no. 20B.

Polityki cyberbezpieczeństwa Turcji

Streszczenie

Internet i cyberprzestrzeń stanowią stopniowo rozwijającą się strukturę. W każdej sekundzie nowe urządzenia, systemy oraz użytkownicy łączą się w sieci, co powoduje ciągły wzrost i zmiany w sferze zagrożeń płynących z cyberprzestrzeni. Turcja to jedno z państw świata najbardziej narażonych na zagrożenia cybernetyczne. Jednak jednym z jego celów stało się doprowadzenie dziedziny cyberbezpieczeństwa do międzynarodowego poziomu. Celem niniejszego artykułu jest pokazanie polityki cyberbezpieczeństwa Turcji i odpowiedź na następujące pytania: Jakie kroki zostały podjęte w Turcji w celu zabezpieczenia państwa i społeczeństwa przed skutkami zagrożeń w cyberprzestrzeni? W jakich sferach Turcja osiągnęła znaczące postępy w ochronnie cyberprzestrzeni, a co w dalszym ciągu jest największym wyzwaniem?

Słowa kluczowe: Turcja, cyberbezpieczeństwo, polityka cyberbezpieczeństwa Turcji, cyberprzestrzeń, polityka bezpieczeństwa