The Turkish Cyber Security Strategy: Structure, Legislation, and Challenges

Emin Daskin (Ghent University)

Abstract

Given that Turkey enjoys an important geostrategic position, plays multiple critical roles in its region, and is a key NATO member, the country's cyber security has far-reaching implications. As such, an examination of Turkey's cyber security strategy, its defensive and offensive cyber capabilities and the main threats facing the country on this front is warranted.

This article gives a brief history of the drafting of Turkey's first cybersecurity strategy, followed by an analysis of the setting-up of the Turkish cybersecurity community and a discussion of its aims and goals. The conclusion highlights the phenomenon of hacktivism as a central challenge to Turkey's cyber security. The article suggests that the country's early enthusiasm for dealing with cyber threats has shrunk and questions whether the adopted strategy has been successfully implemented, in light of recent cyber incidents. The paper also touches upon the effects on Turkish cyber security of political turmoil, infiltration of the state apparatus and agencies by the Gülen sect, and the population's social vulnerability and lack of digital safety awareness.

Introduction

Over the past two decades, Turkey has increased its international ambitions and directed its policies toward being present on all platforms and industries. Bolstered by these efforts, Turkey enjoys an important geostrategic position, plays multiple critical roles in its region, and is a key NATO member. As such, the security of the country's cyberspace has far reaching implications, making it imperative to examine its cyber security strategy, capacity, and the threats faced.

Just as it has with other important initiatives, such as improvements to transportation and health, Turkey attempted to achieve significant progress in the areas of digitalization, cyberspace, and cyber security in a very short time. An ambitious strategy was developed that created new structures and included all possible stakeholders. This was followed initially by an enthusiastic implementation process. Within a few years, however, this ambition and enthusiasm were scaled back to more realistic levels. Large amounts of funding continued to be channelled to R&D projects and the development of academic expertise and training programs, with the main concerns being related to economic and security-related questions.

This article starts by briefly summarizing the efforts that shaped the road to the current strategy. It then examines the legislation and strategy related to cyber incidents and crimes, and the creation of agencies for protective measures and intelligence collection. Next, the structure of Turkey's cyber security landscape is described. The last section of the article illustrates the cyber threats Turkey deals with via a discussion of recent cases of cyberattacks and incidents related to the phenomenon of hacktivism.

Before continuing, it should be noted that the Turkish cyber security strategy, legislation, and the structures involved are very new and thus not fully developed yet. Academic research on this topic is limited, mostly focusing on certain aspects of cybercrime; meanwhile, the few existing publications by government agencies are very repetitive and characterized by a lack of transparency. Finally, the author wishes to make clear that he does not take a stance on any of the discussed cyber security incidents, involved agencies, references, and cited sources; that all data mentioned in this article have been collected exclusively through various open source documents; and that he has no conflict of interest in writing this piece.

The First Efforts to Develop a Strategy

The first time the Turkish government officially considered cyber security on a high level was at a meeting of the National Security Council in 2010, during which the cyber threats toward Turkey and attempts to counter them were discussed (according to the meeting's final report; see T. C. Milli Güvenlik Kurulu Genel Sekreterligi 2010). Subsequent to these discussions, Turkey's first and so far only cyber security strategy was created on June 19, 2012, during a workshop organized by the Ministry of Transportation, Maritime, and Communications, with the cooperation of the Association for Information Security and the Union of Turkish Bar Associations, the sponsorship of Huawei, and the participation of several government agencies, universities, and private companies (veTeknoloji 2012). In an initial draft, the workshop participants set the strategy's goals, a limited roadmap, and the first steps to be taken to create a cyber security structure. The draft informed the fundamentals of Turkey's cyber security policy and was copied almost word for word in the strategy's publicly accessible official version. As such, it needs to be discussed here in some detail.

The June 2012 draft articulates three main goals, namely: 1) increasing security of Turkish cyber space; 2) assuring durability and continuity of critical infrastructure protection against cyberattacks; and 3) assuring the protection of individual and institutional data. In addition, a set of values was defined that was deemed critical to ensuring the utility and benefits of citizens' use of cyberspace: 1) the protection of basic rights and liberties; 2) compliance with the requirements of democratic society and order; 3) compliance with the rule of law; 4) inclusion of all stakeholders in the process of decision making; 5) finding a balance between privacy, security, and usability; 6) compliance with international regulations; 7) developing a holistic approach toward cyber security, including legal, technical, administrative, economic, political, and social dimensions; and 8) contribution to international cooperation.

The 2012 draft also stipulates a few basic definitions of cyberspace, cyberattack, cyber security, cyber defense, and critical infrastructure. While the definitions offered for the first four terms are very simple, the last one provides some insight into Turkey's strategy and priorities. Critical infrastructure is defined here according to ten categories that are divided into four levels. The first, core layer includes only the category Informatics. The second layer includes the categories Energy, Finance, and Health; the third consists of Food, Water, and Transportation. The final layer encompasses Defense (Military), National Security, and CBN capabilities (Chemical, Biological, and Nuclear).

Furthermore, the draft delineates nine strategic objectives that should guide Turkey's efforts to secure the country's cyberspace. Priority is given to, first, defining and mapping critical infrastructure in order to take protective measures depending on the different levels of sensitivity mentioned above; second, creating a culture of cyber security and informing and familiarizing citizens with the latter, with special attention to people in management roles; and third, supporting the development and implementation of Turkish cyber security technologies. Fourth, the draft envisioned the development of legislation related to cyber security and cyber defense that is both deterrent and implementable, in line with international law and regulations. Such legislation would ensure access to information and freedom of expression; protect the privacy of communication, personal information, and personal opinion (except in cases of court order); ensure usability, integrity, privacy, undeniability, and authentication; improve the knowledge of law enforcement on cybersecurity legislation; strengthen security and counter measures against cyber and economic espionage; and create a legal basis for information sharing between state agencies and private companies.

The fifth strategic objective expressed by the 2012 draft focused on investment in human capital and the training of new cyber security experts by creating undergraduate and graduate programs in cyber security; adding compulsory courses on the subject at universities; creating relevant research institutions; giving priority scholarships for cyber security degrees; sending students abroad to study at institutions with a proven record of expertise in this sphere; appointing cyber security or information security managers to all public institution; setting a minimum quota for public servants to be trained in these issues; and continually organizing trainings on new developments in the field.

Sixth, the authors of the draft strategy provide a roadmap for the institutionalization of cyber security measures through the creation of several dedicated institutions. These included a National Cybersecurity Council to ensure the implementation of the *Cyber Security Strategy*; Turkish National Cyber Incident Response Teams which would work in close coordination to deal with cyberattacks; and a National Cyber Threat and Vulnerability Examination Laboratory, which would be an office for the surveillance and registration of national and international cyberattack types, cyber attacker and hacker profiles, cyberattack group structures, attack scenarios, reasons and motivations of attack, attack timing, as well as the development of counter scenarios and strategies. Also, the draft proposes the foundation of a National Cybersecurity Excellence Network under the supervision of the Under Secretariat for Defense Industry, without further clarification of its possible structure or mission statement,

The seventh strategic objective concerns strengthening state-academia-private sector cooperation in the realm of cyber security, through sharing knowledge and best practices, technology, and R&D development; increasing awareness and interest on the topic and providing contracted government job opportunities for experts from the private sector; adding Cyber Security to the 1511 coded list of topics that are set as a priority for scholarships by the Scientific and Technological Research Council of Turkey; adding Cyber Security to the SAN-TEZ program (which is supported by the Ministry of Science, Technology, and Industry and encourages dissertation and thesis-level research on topics related to industry and technology); making research on cyber security compulsory for R&D centers if they want to enjoy state support; and setting a yearly minimum quota for the number of master's and PhD students in the field. Finally, the eighth and ninth strategic objectives relate to encouraging or making mandatory the use of nationally developed security systems and services that are approved by international certification agencies; and fostering international cooperation on cyber security issues on the bilateral and multilateral levels, especially when it comes to the sharing of best practices, intelligence sharing, and cooperation on counter-sabotage.

These listed strategic objectives give insights into the draft authors' understanding of the deficiencies in Turkish cyber security, as well as their priorities in this realm. As suggested before, critical infrastructure is at the forefront of their concerns, depending on the levels of sensitivity outlined above. The other eight listed objectives can be interpreted as a summary of perceived deficiencies and weaknesses and possible objectives to work toward. The objective related to creating awareness on cyber security reveals a recognition of the weakest link in cyber security, that is, systems' users. The emphasis on training people in (government) management roles shows that there is still, in these circles, a lack of knowledge on cyber security and its potential consequences and possibly some resistance on keeping up with the times. Similarly, the highlighting of the need for deterrent legislation is related to for the authors' desire to raise awareness about the importance of cyber security.

Furthermore, the promotion of national technologies can be seen in terms of Turkey's broader economic strategy to develop, use, test, and standardize products in the internal market and promote their export; it also fits within the regime's ambition to lessen dependence on foreign countries in terms of technological products and broaden its own zone of influence by becoming a supplier of these products, particularly those related to the defense industry. This same perceived need to develop technologies domestically also informs the draft's strategic objectives related to human capital and the promotion of innovation and entrepreneurship.

It is worth mentioning that this emphasis on the domestic development of defense-related technologies should be understood in light of the 1974 weapons embargo by the United States on Turkey in the context of Turkey's Cyprus Peace Operation to protect Turkish Cypriots from EOKA's massacres. Indeed, historically, the 1974 crisis acted as a major stimulant for Turkey to develop its national defense industry and create related research facilities. Founded in 1975 as a reaction to the embargo, Aselsan became Turkey's major defense company and training facility for defense and technology experts, working in close cooperation with the military, security forces, and scientific institutions (CNNTurk 2019). One could argue that the authors of the 2012 draft cyber security strategy were also reacting to a perceived crisis (involving increasingly sophisticated cyber attacks against the country), resulting in the similar creation of new domestic capacity to deal with an external challenge.

Finally, the 2012 draft emphasizes that the strategic objectives must be clear, reasonable, and feasible and adapted to Turkey's economic circumstances, technological development, geopolitical positioning, and natural resources in order to be successfully implemented. This may be interpreted as an attempt to create a mindset that accepts that the cyber security strategy should be a step-by-step roadmap driven by demand and limited by existing resources, avoiding the temptation of overambition driven by aspirations that are not matched by realistic capabilities.

Legislation and Adopted Strategy

The cyber security strategy draft discussed in the previous section was soon followed by the adoption of legislation meant to shore up the country's security in this realm. It also resulted in the adoption in 2013 of Turkey's first *Cyber Security Strategy*. Both are discussed in some detail below.

Legislation

The discussed draft resulted in a Council of Ministers Decree (no. 2012/3842), issued on June 11, 2012, and published on October 20, 2012, in State Gazette no. 28447 under the title "Decision Related to the Conduct, Management, and Coordination of National Cyber Security Efforts." This decree regulates the bureaucratic procedures and structure, the responsibilities of the actors involved in cyber security, and the creation and organization of the National Cyber Security Council and working groups on cyber security. On February 19, 2014, a revision was promulgated in State Gazette no. 28918, whereby the authority to determine the members of the National Cyber Security Council was taken from the Ministry of Transportation, Maritime, and Communications and given to the Council of Ministers (under the authority of the Prime Minister); the assignment of duties and working principles of the National Cyber Security Council was relegated to the Prime Minister's authority; and small additional topics such as the promotion of safe use of the Internet were added to the program.

In addition to the Council of Ministers' Decree, the effort to regulate Turkey's cyber security sphere is supported by other existing legislation. This includes first and foremost the no. 5809 Law on Electronic Communication, which regulates the field of electronic communication in sixty-nine articles. Moreover, the Turkish Penal Code also includes several articles related to cyber security that can be found under the section "Crimes against Society Part 10: Crimes Committed in the Field of Information." The specific articles are Article 243 on intrusion into IT systems; Article 244 on the disruption, destruction, and replacement of data on IT systems, as well as the achievement of unlawful benefits through the exploitation of IT systems; and Article 245 on the misuse of debit and credit cards. The Penal Code also includes articles that are not directly classified as relating to cyber incidents but that are applicable whenever there is an important IT related aspect involved in a specific crime. These are mentioned in the section on “Crimes against Individuals,” under Article 124 on the disruption of communication; Article 125 on Insulting; Article 132 on privacy of communication; Article 142 on theft; and Article 158 on fraud.

Turkey is also party to the Budapest Convention on Cybercrime of the Council of Europe, which is the only international convention on cyber crime allocating responsibility to the signing parties. The Budapest Convention serves as a guideline for national legislation and strategies and provides a backbone for the Octopus Conference organized by the Council of Europe, where current and developing issues in cyber security are addressed. As a signatory, Turkey is subject to the Convention’s protocols on copyright infringements, computer-related fraud, violations of network security, and child pornography. The Convention was signed by Turkey in 2010, ratified in 2014, and entered into force in 2015, fourteen years after the Convention was opened for signature by the Council of Europe in 2001 (Council of Europe 2019). This delay can be explained by the absence of an official Turkish national cyber security strategy until 2013. The Convention also has an additional protocol on criminal acts of racism and xenophobia committed in cyber space, which Turkey signed in 2016 (thirteen years after it was first open for signature, in 2003) but which has not yet been ratified. (Council of Europe 2019).

Strategy

Building on the draft and Decree published in 2012, Turkey’s first *National Cyber Security Strategy and Action Plan* was published in January 2013 by the Ministry of Transportation, Maritime, and Communications. It was this specific ministry that was given the role of drafting, managing, updating, and coordinating policies, strategies, and action plans related to cyber security. Although it was made public in January 2013, the *Strategy* entered into force with a lag of almost six months after its publication in State Gazette no. 28683 on June 20, 2013, probably due to bureaucratic delay.

The *Strategy* resembles closely the draft published in 2012, although it is somewhat more detailed and expanded. First, where the draft defines only four basic terms, the *Strategy* defines twelve of the latter and makes several terminological distinctions, such as between cyber space and cyber structures and between public and private information systems. Furthermore, in addition to national security aspects and the need for the development of expertise, the *Strategy* attaches great importance to the link between cyber security and economic competitiveness, referring explicitly to the dangers posed by economic espionage and sabotage. This is also observable in the definitions given; for example, threats to critical infrastructure now include economic loss in addition to loss of life and threats to national security and public order. Another remarkable addition is the realistic admission that cyberattacks can never be fully exterminated or protected against; accordingly, the goal of the *Strategy* is defined as minimizing the number of cyberattacks and their impact and bringing IT systems to normal in the shortest period of time after an incident.

Similarly, the *Strategy* mentions the need to be realistic when assessing the risks and capabilities related to cyber security, but the subsequent list of risks specific to Turkey is very superficial. It includes: poor national awareness on the topic; poor national coordination between different actors involved in cyber security; a lack of reporting of cyber incidents and attacks due to fear of loss of face and other reasons; cooperation problems caused by deficiencies in national and international legislation; poor user awareness and user errors at the individual and institutional levels; the vulnerability of IT systems in case of natural disasters and the lack of capacity to take the needed precautions; the lack of infrastructure for information management; the lack of knowledge, awareness, and ownership on the issue on the management level; poor institutional infrastructure; lack of personnel; poor levels of expertise and lack of experience among existing personnel; insufficient oversight on cyber security; not taking into account cyber security aspects during the public purchase of products and services; and poor levels of national initiatives on hardware and software development.

In order to overcome these deficiencies and implement the cyber security strategy nationwide, the *Strategy* mandated several strategic actions with an initial deadline of 2014. The first of these concerned the creation of legal regulations and a cyber security terminology glossary, along with structures to support the judicial process and forensics in case of cyber incidents and attacks. The strategic actions also included the establishment of the National Computer Emergency Response Center (USOM, TR-CERC) and sectorial Computer Emergency Response Teams (SOME, CERT) coordinated by TR-CERC; the document also envisioned the strengthening of the national cyber security infrastructure, investing in human capital, and the development of national technologies. The final strategic action mentioned by the *Strategy* involves the extension of the jurisdiction and task range of national security organizations in order to cope with cyber security. Because these strategic actions are very broad, 29 specific missions and 95 sub-missions are defined and delegated to specific ministries or agencies, with explicit deadlines for implementation.

Two years after the *Strategy*'s adoption, seven workshops were organized in 2015 to evaluate and revise it. Referred to as the Platform for Common Mind, these meetings involved the participation of 126 experts representing 73 institutions and resulted in the subsequent publication of an updated version of the *Strategy,* which outlined Turkey's priorities in the cyber security realm until 2019. Starting from the introduction, this document stresses again that cyber security is a crucial aspect of Turkey's economy (this time mentioning e-commerce as an area of concern for the first time) and stresses the threats of cyber espionage with a focus on economic espionage, particularly in the defense industry.

Additionally, the language of the updated *Strategy* indicates that there was some work on aligning Turkey's cyber security strategy with the EU, OECD, and NATO.

It should be noted that both the 2012 draft and the 2013 *Strategy* stipulated that the strategy would be updated at least once a year. However, in practice, this has not occurred, which probably explains why specific quotas and time limits related to projects and publication of updates were deleted from the updated document. More than that, the latter now includes language specifying that "proposed actions that could not be finalized and goals that could not be accomplished before the publication of the following strategy document would be transferred to the next document." These two changes give the impression that the initial enthusiasm among relevant policy actors has diminished and given way to the acceptance of delay and postponement. A similar conclusion can be reached when we examine the website of the Information and Communication Technologies Authority (Bilgi Teknolojileri Kurumu - BTK), one of the major actors in Turkey's cyber security. As of this writing the webpages related to cyber security were out of date, with the last update being from December 2017. In the aftermath of the July 15, 2016, coup attempt and the subsequent reform of the presidential system, many things have changed in terms of state structure and thus also the structure related to cyber security. However, none of these changes have been reflected via updates to relevant strategy documents and government websites. For example, the BTK website still makes references to the Under Secretariat of Public Order and Security, which was shut down in 2018, and even to the Telecommunication and Communication Authority, which was shut down in 2016, one year before the BTK's webpage was last updated (Bilgi Teknolojileri Kurumu 2017).

Still, two important developments were included in the updated *Strategy* from 2016. The first was the recognition of Internet and social media addiction as a cyber security risk affecting the Turkish population; in response, a special Parliamentary Research Commission was set up to investigate this issue and come up with solutions (Takvim 2019). Second, the updated *Strategy* mentions that, in addition to protective measures, Turkey also aims to build proactive cyber capabilities for preventive and pre-emptive purposes.

Besides the official declarations mentioned above, certain other elements influencing Turkey's cyber security and intelligence strategy are worth mentioning. These include, but are not limited to, far-reaching digital surveillance, the struggle against terrorist propaganda and social engineering, limitations on Internet access, unlawful wiretapping and "tape scandals" that reflect the abuse of power due to lack of oversight, vulnerability against cyber sabotage, lack of data protection, and breaches of privacy.

More specifically, Turkey's surveillance and wiretapping culture has been the object of much criticism. The 2018 brutal killing of journalist Jamal Khashoggi subjected the country's surveillance capabilities and activities to international media scrutiny. Turkey's foremost evidence against Saudi Arabia in this case was a recording of discussions in the Saudi consulate in Istanbul; this led to suspicions that Turkey was eavesdropping on foreign representations inside its borders. Further outcry was caused by public leaks of unlawful secret voice recordings related to national topics (Global News 2018), particularly leaks related to talks between Turkish intelligence and the Kurdish PKK, a high-level security meeting on the Syrian conflict, and alleged corruption cases. In addition, over the past few years Turkey has witnessed dozens of sex-tape leaks and blackmailing of politicians who were forced to resign, including the most powerful opposition figure Deniz Baykal. Before the leak, Baykal accused the director of MIT's Department of Electronic-Technical Intelligence (which is responsible for electronic surveillance) with being an agent of the Gülen sect. This group, which is considered a terrorist organization by the Turkish state, already had the reputation for unlawful eavesdropping on politicians, journalists, academics, businessmen, police and military personnel, judges, prosecutors and numerous others, including foreign targets (CNN Turk 2018).

Structure

The June 12, 2012, Council of Ministers Decree outlined what would henceforth be Turkey's main cyber security structure. The Cyber Security Council under the presidency of the Minister of Transportation, Maritime, and Communications was designated as the core organ responsible for cyber security, with the participation of the Undersecretaries of the Interior, Foreign Affairs, National Defense, Transportation, Maritime, and Communications, the National Intelligence Agency (MIT), the Army General Staff Head of Communication Electronics and Information Systems (MEBS), the Director of the Information and Communication Technologies Authority (BTK), the Director of the Scientific and Technological Research Council (TÜBITAK), the Director of the Financial Crimes Investigation Board (MASAK), and other officials who may be appointed by the Ministry of Transportation, Maritime, and Communication (this structure was somewhat modified by the subsequent 2014 revision mentioned above). As it is clear from this structure, the Ministry of Transportation, Maritime, and Communications is the main actor in terms of Turkish cyber security and is given the task to draft, manage, update, and coordinate policies, strategies, and action plans to protect the country in this realm. The actual execution of protection and reaction against cyberattacks is carried out by the CERC and CERT teams.

The rest of this section examines more closely the various agencies involved in Turkey's cyber security structure, touching upon their respective roles and internal organization. As we are examining a security-related topic we will also touch upon the role of security and intelligence organizations within the cyber security ecosystem. However, it should be noted that remarkably little has been written about Turkey's four main security establishments, and that this enigmatic character of the Turkish security establishment is no different when it comes to cyber security. Still, as we will see, some of these actors are more transparent than others.

Informational and Communication Technologies Authority (Bilgi Teknolojileri ve Iletisim Kurumu – BTK)

Receiving its tasks from Law no. 2813, Law no 4502 and Law no 5809, The BTK receives its mandate from Laws no. 2813, no. 4502, and Law no. 5809, and is an important actor in terms of regulating, controlling, and auditing the Internet and Internet access, the communication sector, and cyberspace. The institution has considerable power and freedom, defined under Article 4(3) of its management regulations document (Bilgi Teknolojileri ve Iletisim Kurumu 2011). The same document defines the BTK's different duties and jurisdiction under Article 5. Besides the CERC and CERTs, which are discussed below, the departments within BTK dealing with cyber security are the Information Systems Department, Information Technology Department, Internet Department, Department for Access and Tariffs, Sectorial Research and Strategy Development Department, and the Technical Operations Department.

According to publicly available information from the BTK itself, the agency's most important activities related to cyber security are cyber security exercises (Bilgi Teknolojileri ve Iletisim Kurumu 2017). The goals of these exercises are testing, evaluating, and developing counter capabilities; evaluating and improving coordination inside and between the actors involved; and improving awareness on cyber security issues. Since 2015, four exercises have been organized, with the participation of the Ministry of Transportation, Maritime, and Communications, TÜBITAK, and Istanbul Technical University.

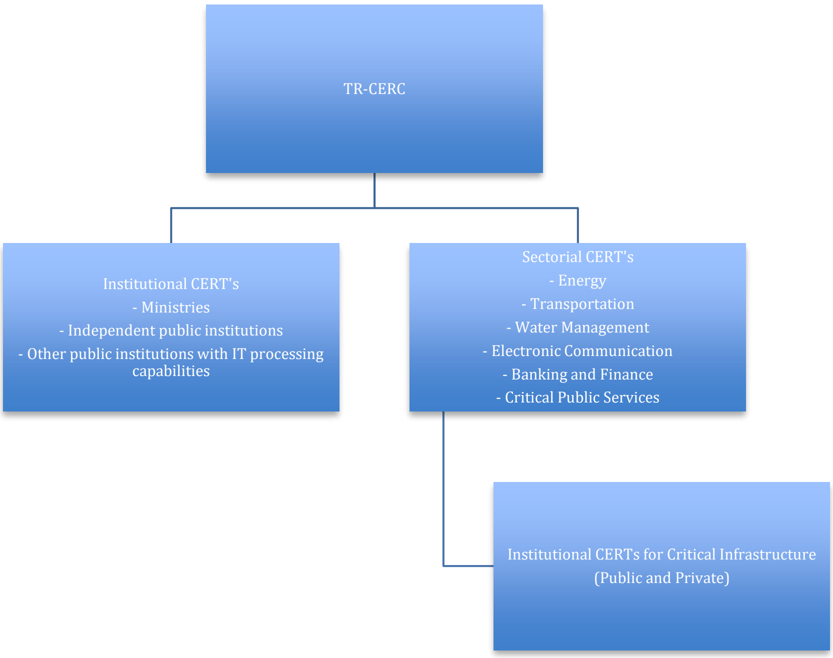
Turkey Computer Emergency Response Center (TR-CERC)

The TR-CERC, which is responsible for the dealing with cyber incidents on the national level, is housed within the BTK. It plays the main coordinating role for information related to cyber incidents with different government and private actors and is responsible for alarms, warnings, and announcements on cyber incidents and the detection of attacks. In terms of security updates, the TR-CERC webpage is updated regularly; however, the content is only a copy-paste of updates from a limited number of major companies such as Cisco, Mozilla, Microsoft, Apple, Oracle, Google, and Adobe. When it comes to announcements from the TR-CERC itself, the alert list only contains five alerts published between January 2015 and August 2017, of which four are actually related to the activities of the Computer Emergency Response Teams (see below); the content of each alert is limited to no more than a few lines. Additionally, TR-CERC provides twelve awareness-raising documents on its website. However, these are also outdated, being from between 2014 and 2016. The outdated nature of the website can give a distorted image of TR-CERC's activities, suggesting that it is far less active than is in reality; the issue here is one of a lack of transparency, characteristic generally of the Turkish bureaucratic system.

Computer Emergency Response Teams (CERT)

The details related to the regulations, tasks, and responsibilities of the CERTs are provided in State Gazette No. 28818 (Resmi Gazete 2013). The structure of the CERTs is divided according to sectors and infrastructure, with the teams technically part of the specific institution within they are housed. The CERTs are responsible for taking measures to ensure information security of a specific sector or a particular institution; protecting a specific sector or institution against cyberattacks; taking measures to lower the damage in case of an attack; reacting against possible attacks; ensuring information flow with different partners; and ensuring 24/7 preparedness and availability. The information given on BTK's own website mentions that the CERT on electronic communication within BTK consists of a total of six personnel, including one coordinator and five experts. In a recent interview on CNN Turk, BTK director Omer Fatih Sayan stated that there are around three thousand legally employed cyber security experts working 24/7 at more than one thousand CERTs across Turkey (Sayan 2019).

The following diagram from the BTK website gives a general overview of the relationship and hierarchy between the TR-CERC and CERTs:


TR-CERC
Institutional CERT's
- Ministries
- Independent public institutions
- Other public institutions with IT processing capabilities
Sectorial CERT's
- Energy
- Transportation
- Water Management
- Electronic Communication
- Banking and Finance
- Critical Public Services
Institutional CERTs for Critical Infrastructure (Public and Private)

Source: https://www.btk.gov.tr/usom-ve-kurumsal-siber-olaylara-mudahale-ekibi

General Directorate of Security (Emniyet Genel Mudurlugu)

The Turkish police force, officially known as the General Directorate of Security and housed within the Ministry of Interior, has undergone significant evolution in both structure and duties over the years. Prior to 2011, cyber incidents and crimes were dealt with by the police forces in a decentralized way. Efforts that dealt with cyber related aspects of investigations were seen as supportive services. As there was no specific cyber department, relevant personnel working at different departments at the headquarters or local police departments were assigned ad hoc. In 2011, these efforts were consolidated within the Department of Combating Information Technology Crimes under Ministerial Decree 2011/2055. Based on another ministerial decision, on February 28, 2013, the department was renamed the Department of Combating Cyber Crimes. The department's mission statement declares its purpose as "reacting against crimes committed through the use of or targeting of information technology systems, preventing misuse of information technology systems, making assessments related to cybercrime threats, training forensic computing and cybercrime experts and inspectors, working on an international level to combat cybercrimes, and creating public awareness" (Emniyet Genel Mudurlugu sd). The department strives to achieve these objectives with a budget of around 86 million Turkish Lira (Emniyet Genel Mudurlugu 2018).

An overview of this unit's actions can be seen in a declaration on its website dating from December 19, 2018. Within the department, the areas of work are divided among twelve desks that do surveillance and online patrols 24/7, specifically focused on social media; citizens are given the opportunity to assist the department by reporting suspicious webpages or profiles through an online system. The internal division of the twelve desks is listed as follows: 1) fraud related to payment methods; 2) IT systems related crimes; 3) the online sale of narcotics and weapons; 4) religiously motivated terrorism; 5) illegally infiltrated structures into the state apparatus under the control of the Gülen sect, linked to the July 15 coup attempt; 6) separatist terrorism; 7) extremist left-wing terrorism; 8) security; 9) child abuse and prostitution; 10) illegal gambling; 11) administrative investigation; and 12) a category combining uncategorized crimes under the label "other."

It should be noted that the separate category "security" is an interesting combination of various topics, including different activities designated as crimes, such as "insulting Atatürk, insulting statesman, insulting the Turkish nation/people, social engineering, illegal gathering callouts, fake profiles, insulting religious values, organ trade, threatening, inducement to suicide, and violence against animals." In the event, in 2018 the twelve desks investigated approximately 110,000 social media accounts, around 45 000 users were “identified” (with no further information shared as to what this meant), and 7,109 people were arrested for criminal or terrorist activities online.

Since the official start of the Turkish *Cyber Security Strategy* in draft form in 2012, the cybercrime department of the police force has organized yearly Cyber Crime Workshops, of which the fifth was organized between December 10 and 12, 2018, in Ankara, with the participation of Turkish and international experts from law enforcement, academia, and major companies from the finance sector and defense industry. The main topics of interest were social media and discourse analysis, social engineering, banking fraud, business related cyber crimes, cybercrime in court orders, cryptology and law enforcement, Dark Net, financial crimes, public-private partnerships, and the maintenance of a safe Internet for children. This conference series is also an important chain in the cooperation between Turkey and the European Union and Council of Europe, under the iPROCEEDS joint project for cooperation on cybercrime under the Instrument of Pre-Accession (Council of Europe sd). The police force has also launched safe Internet usage awareness campaigns for children, in the form of brochures and posters with cartoons meant to promulgate knowledge about the dangers posed by malicious people online.

Moreover, the police cybercrime department offers courses on cyber security, of which the titles and syllabuses give an idea of priority topics and the importance attached to bringing personnel up to a desired knowledge level. In total twenty courses are listed that add up to 607 hours of theoretical and practical training, including classes on the legal aspects of countering cyber crime, police patrol in cyber space, Deepweb and Darknet, social engineering, fighting online child abuse, technical analysis for different operating systems, retrieving data, cyber and network forensics, electronic evidence collection, counter intelligence, secret investigation techniques, and surveillance and observation (EGM Siber

Suclarla Mucadele Daire Baskanligi sd). An additional course of fifty hours under the name "Branch Training" is included on the online list of courses, without further specification.

Besides the Department of Combating Cyber Crimes, the police force has a separate Department of Information Technology. This department, with a budget of around 216 million Turkish Lira, is responsible for the security of the Directorate of Security's internal communication, computer systems, and networks (Emniyet Genel Mudurlugu 2018). The relevant sub-departments are information security; IT network security; systems security; software; database; and IT projects (EGM Bilgi Teknolojileri Daire Baskanligi sd).

National Intelligence Service (Milli Istihbarat Teskilati – MIT)

Similar to the previously mentioned state institutions, the National Intelligence Service MIT (Milli Istihbarat Teskilati) has experienced important transformations in recent years. Besides the changes in the law regulating the intelligence service and the changes in structure, an important step was taken to open the agency to the public and create transparency related to its workings. As part of this transparency campaign, the MIT invited journalists to the MIT Headquarters and briefed them about the structure and working of the service (TRT Haber 2012). In the following year, the MIT's website was renewed, providing basic information on how MIT works (Hurriyet 2013). The website also launched a career webpage, on which (as of this writing) seventeen of nineteen career opportunities were within IT-related departments, varying from jobs for SIGINT analysts to cyber security and Internet technology experts (Milli Istihbarat Teskilati IK sd). Building on this information, it is plausible to assume that these departments are growing or gaining importance for the MIT.

The agency combines all intelligence tasks in one organization, which means that besides the archetypal intelligence duties such as counter intelligence, security and operations departments, the MIT also incorporates the Department of Signal Intelligence and the Department of Electronic-Technical Intelligence (Milli Istihbarat Teskilati sd), which need more specific specialization and for which many countries opt to set up separate independent agencies. This raises questions related to specialization and optimal deployment of staff (in case of rotation), a possible mentality gap between staff (HUMINT <-> SIGINT), and many other human resources and organization related issues.

The Department of Signal Intelligence is responsible for the interception of signals and processing them through the intelligence cycle. Prior to its transfer to the MIT in 2012, this department was under the Army General Staff Electronic Systems Command (Genelkurmay Elektronik Sistemler – GES). In order to compensate for the probable reducing of SIGINT capabilities at air and sea after the department's separation from the Army, MIT procured UAVs and one ship. The agency purchased ANKA-I UAVs produced by TAI (Turkish Aerospace Industries) (Milliyet 2018) but also showed interest in the Global Hawk produced by Aerovironment (USA) and still cooperates with TUBITAK and Turkish defense companies for other projects (Cumhuriyet 2014). Additionally, MIT has four CASA CN235 airplanes transformed in order to meet SIGINT needs and has considerable satellite technology developed by national and international companies. Besides these, MIT has an order standing for a fully equipped SIGINT airplane, about which no recent news is available (Haber7 2015).

MIT's first ship was ordered in 2012 (Boshporus Naval News 2012), produced in cooperation between STM (Savunma Teknolojileri Muhendislik ve Ticaret A.S.) and ASELSAN, and was delivered on February 9, 2019, under the name TCG Ufuk A-591 (Milliyet 2019). The project was developed officially as a "testing and training ship" but Turkish president Erdogan revealed during the ceremony of the delivery of the ship that TCG Ufuk was to be the country's first intelligence ship, meant to be its eyes and ears on the high seas (T.C. Cumhurbaskanligi Savunma Sanayii Baskanligi 2019). This move is a clear message about Turkey's ambitions in the region, its commitment to protect its interests on the high seas, and its intent to preserve Turkish security beyond Turkey's borders.

While the above developments clearly demonstrate the strengthening of the SIGINT department's capacity, the current dominant view is that the former has also in recent times suffered some damage due to infiltration by members of the Gülen sect (Sabah 2018). Moreover, there was much critique when SIGINT capabilities were taken from the Army and transferred to the MIT, as possible communication failures or delays could cause serious problems for military operations. Some experts (including the former director of GES) claimed that a probable miscommunication or delayed communication between the MIT and the Air Force was the reason for the shooting down of a Turkish jet by Syrian missiles in 2012 and the shooting down of a Russian Sukhoi Su-24 by a Turkish F16 in 2015; allegedly, the intercepted intelligence was delivered to the President before reaching the Army General Staff, resulting in a critical delay (Sozcu 2015; T24 2015). Other observers were convinced that the miscommunication was caused by Gülenist sabotage.

The second MIT department working on the cyber dimension is the Department of Electronic-Technical Intelligence. The duties of this unit are defined as "interception and evaluation of communication in order to detect state secret disclosure/leaks and terrorist activities, [and] keeping records of the intercepted data" (Milli Istihbarat Teskilati sd). Additionally, the unit is responsible for "Imagery Intelligence (IMINT), deciphering intercepted encrypted data, analysis of intercepted voice and imagery, [and] counter activities against cyber threats and attacks." As many state institutions, this department appears to have been the target of infiltration at the highest level by the Gülen sect. In a striking example, the previous director of this department Basri Aktepe has been accused by various opposition actors of being a Gülenist infiltrator for more than ten years (Terkoglu 2011), and is now being prosecuted for allegedly participating in the coup attempt and being a member of a terrorist organization (CNN Turk 2019).

The third MIT department active in cyber security is the Counter-Intelligence Department (CID), with a focus on countering foreign espionage threats. As part of this effort, this unit introduced briefings on counterespionage and protection against cyber threats as far back as 2009, a very proactive effort predating the official start of Turkey's cyber security strategy. Since then, more than 18 thousand people from 390 different institutions have been briefed by CID (SputnikNews 2018). Finally, the MIT in general provides "strategic cooperation" briefings and recently introduced "regional security evaluation" briefings directed toward the academic community (Gazete Yolculuk 2019).

Army General Staff Department of Communication Electronics and Information Systems (Muhabere Elektronik ve Bilgi Sistemleri - MEBS)

The Department of Communication Electronics and Information Systems under the Army General Staff is responsible for the management and protection of military communication systems, electronic warfare, information systems, and IMINT (Kara Kuvvetleri Komutanligi sd). The department is organized according to the Network-Centric Warfare doctrine in order to enhance operational effectiveness. Recently, the brigadier general in charge of this unit was appointed to the NATO Communications and Information Agency based in Brussels (Yeni Akit 2019).

A department with a similar name also exists within the Presidency of Defense Industries of the Presidency of the Republic of Turkey, which oversees and manages the development of new projects and products related to this area (T.C. Cumhurbaskanligi Savunma Sanayii Baskanligi sd). This Presidency also houses a separate department on Cyber Security and Information Systems.

Gendarmerie General Command Branch of Communication Electronics and Information (Jandarma Genel Komutanligi Muharebe Elektronik ve Bilgi Sistemi - MEBS)

The Gendarmerie has its own communication electronics and information branch. The similarity of its name with that of the above-discussed department of the Army General Staff is probably because the Gendarmerie was based within the Army General Staff for a long time, being transferred to the Ministry of Interior only after the 2016 coup attempt. The cyber capabilities and duties of the Gendarmerie are not very clear. However, it is possible to determine some of the unit's activities via its advertised job vacancies (T.C. Icisleri Bakanligi Jandarma Genel Komutanligi 2018). For example, the currently listed vacancies do not provide any information on the job content. However, the education requirements listed (graduate degrees in electronics, computer sciences, communication technology, and Internet and network technology) are suggestive. One of MEBS's probable activities is the management and security of the Gendarmerie Integrated Communication and Information System (Jandarma Entegre Muhabere ve Bilgi Sistemi – JEMUS), which is in fact the integrated working of the Gendarmerie General Command Incidents Information System and the Gendarmerie Integrated Intelligence System.

Scientific and Technological Research Council of Turkey (Turkiye Bilimsel ve Teknolojik Arastirma Kurumu – TUBITAK)

TUBITAK is Turkey's state-run agency responsible for the setting-up, funding, management, coordination, testing and evaluation, and commercialization of scientific projects and technological R&D within state defined targets, in close collaboration with academia, government, private companies, and international institutions. As Turkey's foremost R&D agency, TUBITAK plays an important role in cyber security and the development of new national technologies. Within TUBITAK, the Informatics and Information Security Research Center (Bilisim ve Bilgi Guvenligi Ileri Teknolojileri Arastirma Merkezi – BILGEM) is the lead actor when it comes to cyber and information security. More than 1600 scientists work at different research institutes under BILGEM, including 1) the National Research Institute of Electronics and Cryptology, 2) the

Information Technologies Institute, 3) the Advanced Technologies Research Institute, 4) the Cyber Security Institute, and 5) the Software Technologies Research Institute. These institutions provide important solutions, varying from secure communication, electronic intelligence, smart transportation, electronic warfare systems, cloud computing, and disaster management. Critical projects like the new electronic National ID Card, the GÖKTÜRK Reconnaissance and Surveillance Satellite and its Crypto System, the National Military Messaging Handling System, and the MILCEP project for crypto mobile phones are just a few of the many projects carried out under BILGEM's auspices. TUBITAK also plays an important role in the development of new surveillance technologies and cyber security solutions for the National Intelligence Agency in close cooperation with Turkey's leading defense companies, such as ASELSAN and HAVELSAN. For this reason, TUBITAK has also been a target for foreign intelligence services.

Other Agencies

The picture of Turkey's current cyber security structure would be incomplete without at least a brief mention of the Disaster and Emergency Management Authority (AFAD), which includes cyber threat and cyber security in its Disaster Management Glossary. AFAD has a coordination role related to cyber threats and incidents against critical infrastructure, which the agency refers to as "technological disasters." However, AFAD's role is only the coordination of information. Responsibility and execution is delegated to numerous different national and local institutions. For this reason AFAD has been lobbying for a clearly defined structure with clear boundaries related to responsibility, accountability, task division, optimized communication and coordination, and the development of clear critical infrastructure security plans (Afet ve Acil Durum Yonetim Baskanligi 2014).

Finally, the Cyber Security Initiative within the Internet Development Council is a platform where stakeholders gather for sharing information and discussing possible improvements on cyber security, with the results of these discussions being presented to the Ministry of Transportation, Maritime, and Communication (Bilgi Teknolojileri ve Iletisim Kurumu 2017). In addition, this platform also aims to inform and create awareness among citizens and SMEs, conduct sectorial risk analysis, determine cyber security standards, and publish reports and manuals on the topic, among other activities.

History of Cyber Attacks and Incidents in Turkey: The Case of Hacktivism

Having presented Turkey's *Cyber Security Strategy* and the institutions tasked with achieving its goals, we conclude this article with a discussion of one of the major cyber security threats faced by the country in the twenty-first century, namely, hacktivism. Doing so highlights the importance of Turkey's efforts in this realm and raises questions about the success of the present *Strategy* and its implementation.

In the twenty-first century, Turkey has witnessed cyber incidents and attacks on an unprecedented scale, with devastating results, a phenomenon that makes it difficult to understand the delay in state action to develop a cyber security strategy. The incidents that are available through open sources have mainly involved cyberattacks for economic purposes, sabotage, hacktivism, and crimes between citizens for various reasons. Besides these, there have undoubtedly also been incidents related to espionage that have not been made public.

Acknowledging that cyber incidents with a fraudulent economic aim are a serious problem for Turkey, such as in the example of the hacking of HSBC Turkey where the account and credit card information of 2.7 million customers was stolen, this article will only consider cyber incidents with a political dimension, known more specifically as hacktivism, which has been a serious challenge for Turkey. Numerous incidents have taken place in recent years, with the main actors being Turkish groups sometimes operating with the support of foreign or international hacker communities. Hacktivist communities in Turkey can be divided in two clearly separate groups: the nationalist hacktivist groups who perform cyber attacks in line with what they see as the interest of the Turkish state and nation, and secondly the left-wing hacktivist groups who perform cyber attacks in line with their political beliefs and self-proclaimed responsibilities as cyberguerillas. Finally, it should be noted that while hacktivism incidents have in general demonstrated the vulnerability of the Turkish state institutions to cyberattacks, some hacker groups have stated explicitly that their actions are meant to create awareness of this problem and to force state institutions to take up the responsibility to protect their systems (Yeni Mesaj 2006).

Over the past several years, the webpages and information systems (such as PolNet) of Turkish security forces have been hacked repeatedly, with the retrieved information being leaked to the public. In the leaks after the hack of the Ankara Security Directorate (police force), the hackers also publicized that the access code for the Directorate's database was simply "123456" (Posta 2012). It should be noted that some experts claim that the consequences of the hacks of the Security Directorate were more severe than was made public.

In the meantime, the Army has also been a regular target of cyberattacks. For example, the Land Forces Command was hacked several times in 2012, and some details of personnel were made public. The hackers left the following message: "If we can get access to this information, imagine what foreign intelligence services could do," attracting attention to the deficiencies in Turkey's cyber security (Sabah 2012). Cyberattacks against the Army have taken very creative forms. On March 1, 2019, the Army General Staff sent out an alert to its personnel related to online games that were used for cyberattacks, wherein military personnel were targets of social engineering to retrieve intelligence (Internethaber 2019). Similarly, the MIT has suffered attacks by hacktivists on several occasions in the form of DDoS attacks and hacks to the MIT website.

Other governmental institutions, mostly related to security or strategic projects, have been regular targets. The ministries of urban planning and energy have been repeatedly targeted by self-proclaimed environmentalist hackers opposing hydroelectric power plants and projects for nuclear power plants with slogans such as “Nuclear power plant is fascism.” Major power outages on national scale have also been attributed to cyberattacks. For example, the unprecedented power outage that occurred on March 31, 2015, and stopped life in Turkey for twelve hours (affecting hospitals, airports, traffic, and infrastructure such as water, but also simple things like elevators and refrigerators) was ascribed by some sources based on leaked documents to hacking by Iranian hackers (T24 2017). The Turkish Ministry of Energy also attributed power outages that happened between December 2016 and January 2017 to cyberattacks and sabotage attempts from US-based platforms and claimed that subsequent infiltration attempts were countered (Sputnik 2017). In these cases, the question of whether the attacks were carried out by hacktivists (with or without government support) or were in fact the products of foreign government action is still unanswered; they are included here as examples of the scale of the problem Turkey faces.

The Turkish Telecommunication Authority (Telekomunikason Iletisim Baskanligi – TIB), which was transferred to the BTK after the 2016 coup attempt, was hacked by a Marxist-socialist hacker group and the retrieved institutional information was made public. The hacktivists proclaimed their purpose as “protesting the heavy Internet censorship imposed by the TIB,” and left an explicit message to the TIB: “You thought you calculated everything, but you forgot the main coordinator of everything. The prohibitor gets prohibited” (CNN Turk 2014). Other hacktivists have performed cyberattacks to protest high Internet prices and low connection speeds or even a high heating bill. Discontent is also visible in the form of targeting political parties and politicians. The website of the ruling Justice and Development Party is attacked regularly, in the form of deceptive messages, mostly with communist imagery. On what could be considered a positive side, Turkish hacktivists also perform attacks against child abuse networks by taking down their networks.

Both left-wing and right-wing hacktivists also perform attacks against foreign state targets, which are ironically most of the time Turkey's close allies. Numerous targets (including police forces, the ministries of defense and newspapers) abroad have been subjected to attacks for reasons ranging from protests against racist policies against minorities, active or passive state support for anti-Turkish terrorist organizations, and anti-Turkish sentiment in politics and media (Nieuwsbald 2007; Yeni Akit 2017; Knack 2019). For example, after a spate of cyberattacks in March 2013 against Israeli targets to protest Israel's policies towards Palestinians, Turkish hackers announced the following: "The real large attack will be on the 7th of April on a global scale, we will erase Israel from the Internet" (Oda TV 2013). Interestingly, protective measures against the subsequent cyberattacks in April failed despite the fact that these attacks were announced weeks before (Oda TV 2013). Similarly, American state institutions have also been exposed to Turkey-based attacks (Hurriyet 2007; Mynet 2010; Yeni Akit 2018; Sabah 2016), as have European countries.

Finally, multinational organizations have been targeted, often around issues of deep concern to Turkish society broadly speaking. For example, the website of the United Nations was hacked in 2007 and 2014 in order to protest the policies of Israel and the United States toward Palestine (Hurriyet 2007) (Milliyet 2014). Another attack against the UN was carried out to protest the ethnic persecution by China of Uyghur Turks (HaberTurk 2009).

Conclusion

As mentioned in the introduction to this article, Turkey began its cyber security campaign with high ambitions and enthusiasm. This was largely fuelled by the country's need for security, made obvious by a series of related incidents, but also by its desire to become a global player in all possible fields. When we examine the *Cyber Security Strategy* adopted in 2013 (Turkey's first official document of this nature), both the failure to carry out the mandated updates and lacklustre implementation suggest that this early enthusiasm did not last long. At the same time, this impression is strengthened by the lack of governmental transparency in this sphere, or at least in the reluctance of the state agencies to share information.

Moreover, based on the fact that cyberattacks, crimes and other incidents (including but not limited to the hacktivism discussed in the above section) have continued at a high pace since the *Strategy*'s adoption, it is unlikely that the policy's main declared goals are being reached, particularly when it comes to the protection of critical infrastructure and individual and institutional data. Further research is needed to answer the question whether this is due to the failure or shortcomings of the Turkish strategy and agencies, or whether it is due to an increase in the number and sophistication of attacks and attackers.

More importantly, when looking at the practice, it is unclear whether any of the explicitly listed values meant to inform the cyber security strategy are truly being taken into account. Notably, critics have pointed to censorship and lack of oversight resulting in a culture of unlawful misuse of cyber capabilities, particularly visible in the form of the "tape scandals" that have emerged over the past several years. This situation suggests the need to open a discussion on what is meant by (cyber)"security," its depth and scope, and the importance of democratic oversight of cyber security capabilities.

At the same time, on the positive side, the 2013 *Strategy*, related efforts, and legislation demonstrate that Turkey attaches great importance to complying with international (technological) standards (mainly due to economic reasons), as well as to cooperation with NATO, EU, OECD and its allies. It is important that these commitments continue despite attempts to subvert Turkish public opinion and sabotage attempts by domestic and foreign actors.

Moreover, an evaluation of the cyber security structures created in the aftermath of the *Strategy*'s adoption shows that the proposed agencies and institutions were created and activated inside the mandated time limits. The existence and apparent potential of the created agencies also suggests that Turkey has the intention to achieve serious preventive and pre-emptive capabilities. However, the requisite human capital and expertise have seemingly not yet been arrived at. This conclusion is partially due to the fact that the results of investments in human capital are only visible after a period of time (meaning that it may be too early to draw either negative or positive conclusions in this regard), as well as to the loss of capacity and expertise stemming from the political turmoil of recent years. Political turmoil and battle for power and jurisdiction inside Turkey's security establishment resulted in the restructuring of the still young cyber security structures, which in turn caused critique related to incidents caused by communication failures.

In addition to political turmoil, the Turkish ruling elite is aware of the vulnerability of the Turkish population to cyber and social media addiction, which in combination with a lack of awareness on safe use of the Internet constitutes a significant challenge. Together, political turmoil and social vulnerability form a serious problem, as the existing tensions are exploited for social engineering purposes by both domestic and foreign actors. Another major issue relates to the leaks of information retrieved through hacking, more specifically hacktivism. In order to overcome these issues, Turkey has visibly tightened the grip on Internet access and increased its digital surveillance; however, critics have suggested that there may be political motives behind these censorship efforts that trump purely cyber security concerns.

When looking at the final picture, Turkey started dealing with its existing cyber security problems with a significant delay but managed to set up a reactive system in a considerably short period. In order to reach the defined goals within the boundaries of the explicitly stated values while finding a healthy equilibrium in the security-freedom nexus for this new state structure, the notions of transparency, critique, and discussion should be accepted as fundamental. For the rest, the system must be given time to develop to the intended level and prove itself. Finally, but crucially, democratic oversight of this system must be guaranteed in order to audit its effectiveness and safeguard the fundamental values of liberty and justice.

Bibliography

Afet ve Acil Durum Yonetim Baskanligi. *Kritik Altyapilarin Korunmasi Yol Haritasi Belgesi 2014-2023.* Ankara: AFAD, 2014.

Bilgi Teknolojileri ve Iletisim Kurumu. *Siber Güvenlik İnisiyatifi* . December 15, 2017. https://www.btk.gov.tr/siber-guvenlik-inisiyatifi (accessed February 28, 2019).

Bilgi Teknolojileri ve Iletisim Kurumu. *Siber Guvenlik Kurulu.* December 15, 2017. https://www.btk.gov.tr/siber-guvenlik-kurulu (accessed February 24, 2019).

Bilgi Teknolojileri ve Iletisim Kurumu. *Siber Guvenlik Tatbikatlari.* December 15, 2017. https://www.btk.gov.tr/siber-guvenlik-tatbikatlari (accessed February 21, 2019).

Bilgi Teknolojileri ve Iletisim Kurumu. *Bilgi Teknolojileri ve Iletisim Kurumu Teskilat Yonetmeligi*. 2011.

Boshporus Naval News. *Turkish National Intelligence Organisation Asks for A SIGINT Ship.* October 21, 2012. https://turkishnavy.net/2012/10/21/turkish-national-intelligence-organisation-asks-for-a-sigint-ship/ (accessed February 25, 2019).

Boshporus Naval News. *What Does the Exercise Mavi Vatan Mean?* February 27, 2019. https://turkishnavy.net/2019/02/27/what-does-the-exercise-mavi-vatan-mean/ (accessed February 27, 2019).

CNN Turk. *İstihbaratçı polisten Deniz Baykal itirafı* . December 11, 2018.

https://www.cnnturk.com/turkiye/istihbaratci-polisten-deniz-baykal-itirafi (accessed March 06, 2019).

CNN Turk. *Eski istihbaratçı Aktepe için FETÖ'den 15 yıl istendi* . February 7, 2019. https://www.cnnturk.com/turkiye/eski-istihbaratci-aktepe-icin-fetoden-15-yil-istendi (accessed February 27, 2019).

CNN Turk. *Redhack TIB'i "hack"ledi.* March 28 2014. https://www.cnnturk.com/haber/bilim-teknoloji/internet/redhack-tibi-hackledigini-duyurdu (accessed February 28, 2019).

CNN Turk. *ASELSAN'dan 2 milyar liralik ciro.* May 9, 2019. https://www.cnnturk.com/ekonomi/aselsandan-2-milyar-liralik-ciro (accessed May 17, 2019).

Council of Europe. *Chart of Signatures and Ratifications of Treaty 185.* May 18, 2019. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=srkvCSDR (accessed May 18, 2019).

Council of Europe. *Chart of Signatures and Ratifications of Treaty 189 Additional Protocol.* 18 May 2019. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures?p_auth=srkvCSDR (accessed May 18, 2019).

Council of Europe. *iPROCEEDS – Targeting Crime Proceeds on the Internet in South Eastern Europe and Turkey.* https://www.coe.int/en/web/cybercrime/iproceeds (accessed March 04, 2019).

Cumhuriyet. *MIT kitalararasi istihbarat toplayacak.* September 1, 2014. http://www.cumhuriyet.com.tr/haber/turkiye/113117/MiT_kitalararasi_istihbarat_toplayacak.html (accessed February 25, 2019).

EGM Bilgi Teknolojileri Daire Baskanligi. *Bilgi Teknolojileri Daire Baskanligi.* http://www.bilgiteknolojileri.pol.tr/Sayfalar/default.aspx (accessed February 24, 2019).

EGM Siber Suclarla Mucadele Daire Baskanligi. “Ulusal Egitimler ve Ders Icerikleri.” Bilisim Suclari Akademisi Sube Mudurlugu, EGM Siber Suclarla Mucadele Daire Baskanligi.

Emniyet Genel Mudurlugu. *2018 Yili Performans Programi.* Ankara: Emniyet Genel Mudurlugu, 2018.

Emniyet Genel Mudurlugu. *Basin Aciklamasi.* February 24, 2016. https://www.egm.gov.tr/Duyurular/Sayfalar/Basin-Aciklamasi-24-02-2016.aspx (accessed February 24, 2019).

Emniyet Genel Mudurlugu. *Siber Suclarla Mucadele Daire Baskanligi.* http://www.siber.pol.tr/Sayfalar/hakkimizda.aspx (accessed February 24, 2019).

Gazete Yolculuk. *MIT ve YOK'ten ortak konferans.* February 27, 2019. https://gazeteyolculuk.net/mit-ve-yokten-ortak-konferans (accessed February 27, 2019).

Global News. *Khashoggi Case Sheds Light on Turkey’s History of Spying and Surveillance.* October 22, 2018. https://globalnews.ca/news/4581250/jamal-khashoggi-turkey-surveillance/ (accessed March 06, 2019).

Haber7. *Milli İstihbarat Teşkilatı yeniden yapılanıyor* . December 15, 2015. http://www.haber7.com/ic-politika/haber/1703695-milli-istihbarat-teskilati-yeniden-yapilaniyor (accessed February 27, 2019).

HaberTurk. *Turkler BM'yi 'hack'ledi.* July 27, 2009. https://www.haberturk.com/dunya/haber/161133-turkler-bmyi-hackledi# (accessed March 01, 2019).

Hurriyet. *MIT'in internet sayfasi yenilendi.* January 7, 2013. http://www.hurriyet.com.tr/gundem/mitin-internet-sayfasi-yenilendi-22309701 (accessed February 25, 2019).

Hurriyet. *Türk korsanlar BM sitesini 'hack'ledi* . August 12, 2007. http://www.hurriyet.com.tr/dunya/turk-korsanlar-bm-sitesini-hack-ledi-7074666 (accessed May 18, 2019).

Hurriyet. *Turkler Pentagon'u hackledi.* May 14, 2007. http://www.hurriyet.com.tr/gundem/turkler-pentagon-u-hackledi-6515485 (accessed March 01, 2019).

Internethaber. *Turk Silahli Kuvvetleri"nden askerlere PUBG uyarisi.* March 1, 2019. https://www.internethaber.com/turk-silahli-kuvvetlerinden-askerlere-pubg-uyarisi-2004466h.htm (accessed March 1, 2019).

Kara Kuvvetleri Komutanligi. *Muhabere Elektronik ve Bilgi Sistemleri.* http://www.kkk.tsk.tr/Siniflar/Mebs.aspx (accessed February 28, 2019).

Knack. *Brussels Hof van Beroep: 'PKK is geen terreurgroep'* . March 9, 2019. https://www.knack.be/nieuws/belgie/brussels-hof-van-beroep-pkk-is-geen-terreurgroep/article-news-1438437.html (accessed March 9, 2019).

MDAA. *Greeece's Capabilities.* June 25, 2018. http://missiledefenseadvocacy.org/intl-cooperation/greece/ (accessed May 17, 2019).

Milli Istihbarat Teskilati IK. *MIT Kariyer.* http://www.mit.gov.tr/iksayfasi/index.html (accessed February 27, 2019).

Milli Istihbarat Teskilati. *MIT Baskanligi Teskilat Yapilanmasi.* https://www.mit.gov.tr/teskilat.html (accessed February 24, 2019).

Milli ve yerli test ve egitim (istihbarat) gemisi UFUK (A-591) denize inis toreni. 2019.

Milliyet. *MIT'in havadaki kulagi ANKA-I.* 27 March 2018. http://www.milliyet.com.tr/mit-in-havadaki-kulagi-anka-i-gundem-2635272/ (accessed February 25, 2019).

Milliyet. *Türk hacker, facebook Google ve Apple'ı devirdi* . March 19, 2014. http://www.milliyet.com.tr/turk-hacker-facebook-google-ve/gundem/detay/1853869/default.htm (accessed March 1, 2019).

Milliyet. *Türk korsanlar BM'yi 'hack'ledi.* July 25, 2014. http://www.milliyet.com.tr/turk-korsanlar-bm-yi-hack-ledi/dunya/detay/1916807/default.htm (accessed May 18, 2019).

Milliyet. *Turkiye'nin ilk istihbarat gemisi denize indi.* February 9, 2019. http://www.milliyet.com.tr/son-dakika-turkiye-nin-ilk-istih-siyaset-2824996/ (accessed February 25, 2019).

Mynet. *Türk hackerlar Pentagon'u hackledi.* March 11, 2010. https://www.mynet.com/turk-hackerlar-pentagonu-hackledi-110100499780 (accessed March 1, 2019).

Nieuwsblad. *Turkse nationalisten hacken website FOD Defensie.* January 14, 2007. https://www.nieuwsblad.be/cnt/dmf14012007_057 (accessed March 1, 2019).

Oda TV. *7 nisan'da Israil internetten silinecek.* March 26, 2013. https://odatv.com/7-nisanda-israil-internetten-silinecek--2603131200.html (accessed March 1, 2019).

Posta. *Hacklenen Ankara Emniyeti'nin sifresini acikladilar.* March 6, 2012. https://www.posta.com.tr/hacklenen-ankara-emniyetinin-sifresini-acikladilar-111978 (accessed February 28, 2019).

Resmi Gazete. "Siber olaylara mudahale ekiplerinin kurulus, gorev ve calismalarina dair usul ve esaslar hakkinda teblig." 2013.

Sabah. *MIT'teki kripto FETO'culere operasyon.* September 19, 2018. https://www.sabah.com.tr/gundem/2018/09/19/mitteki-kripto-fetoculere-operasyon (accessed February 27, 2019).

Sabah. *Türk hackerlar NASA'yı hackledi!.* February 15, 2016. https://www.sabah.com.tr/gundem/2016/02/15/turk-hackerlar-nasayi-hackledi (accessed March 1, 2019).

Sabah. *TSK'ya siber saldırı!.* June 12, 2012.

https://www.sabah.com.tr/gundem/2012/06/12/tskya-siber-saldiri (accessed March 01, 2019).

Sayan, Omer Fatih, interview by Cuneyt Ozdemir. *Dr. Omer Fatih Sayan CNN Turk - 5N1K* (February 23, 2019).

Sol Haber. *Anyonymous ve Redhack Israil'i cokertti.* April 7, 2013. http://haber.sol.org.tr/devlet-ve-siyaset/anonymous-ve-redhack-israili-cokertti-haberi-71035 (accessed March 1, 2019).

Sozcu. *GES'i SIB yaparsaniz...*November 29, 2015. https://www.sozcu.com.tr/2015/yazarlar/saygi-ozturk/gesi-sib-yaparsaniz-997401/ (accessed February 27, 2019).

Sputnik. *Bakan Albayrak'ın siber saldırı açıklamasına, ABD Büyükelçiliği'nden yanıt* . January 10, 2017. https://tr.sputniknews.com/abd/201701101026708551-bakan-albayrak-

siber-saldiri-buyukelcilik/ (accessed March 6, 2019).

Sputniknews. *ABD'deki Yunan lobisi: Trump'ın Türkiye'ye F-35 ambargosundan mutluyuz.* August 14, 2018. https://tr.sputniknews.com/abd/201808141034746651-helen-amerikan-liderlik-konseyi-halc-turkiye-ambargosundan-mutlu/ (accessed May 17, 2019).

SputnikNews. *MIT'ten 18bin kisiye 'casusluga onlem' egitimi.* December 12, 2018. https://tr.sputniknews.com/turkiye/201812121036586422-mit-binlerce-kisi-casusluga-onlem/ (accessed February 27, 2019).

T.C. Cumhurbaskanligi Savunma Sanayii Baskanligi. *Organizasyon Semasi.* https://www.ssb.gov.tr/Website/ContentList.aspx?PageID=42 (accessed February 29, 2019).

T.C. Cumhurbaskanligi Savunma Sanayii Baskanligi. *Test ve egitim gemisi TCG Ufuk denize* *indirildi.* February 9, 2019. https://www.ssb.gov.tr/Website/ContentList.aspx?PageID=1681 (accessed February 25, 2019).

T.C. Icisleri Bakanligi Jandarma Genel Komutanligi. *Sozlesmeli Uzman Erbas Basvuru Kilavuzu (2018).* 2018. https://vatandas.jandarma.gov.tr/PTS_Aday/personel1/uzman_erbas/Ek_2_Basvuru_Kılavuzu.pdf (accessed February 28, 2019).

T.C. Milli Güvenlik Kurulu Genel Sekreterligi. *27 Ekim 2010 Tarihli Toplanti.* October 27, 2010. https://www.mgk.gov.tr/index.php/27-ekim-2010-tarihli-toplanti (accessed February 21, 2019).

T24. *2 yıl önce Türkiye genelinde kesilen elektriğin nedeni İran'ın siber saldırısı mı?* July 14, 2017. https://t24.com.tr/haber/2-yil-once-turkiye-genelinde-kesilen-elektrigin-nedeni-iranin-siber-saldirisi-mi,414375 (accessed March 6, 2019).

T24. *Eski MSB Genel Sekreteri: Elektronik sistemler MİT'e devredilmeseydi, Rus uçağı düşürülmeden engellenebilirdi* . November 30, 2015. https://t24.com.tr/haber/eski-msb-genel-sekreteri-elektronik-sistemler-mite-devredilmeseydi-rus-ucagi-dusurulmeden-engellenebilirdi,318548 (accessed March 5, 2019).

T24. *Microsoft'u Türk hackledi* . December 10, 2008. https://t24.com.tr/haber/microsoftu-turk-hackledi,20168 (accessed March 1, 2019).

Takvim. *Teknoloji bağımlılığı ile ilgili Meclis Araştırma Komisyonu kuruldu* . February 21, 2019. https://www.takvim.com.tr/guncel/2019/02/21/teknoloji-bagimliligi-ile-ilgili-meclis-arastirma-komisyonu-kuruldu (accessed March 6, 2019).

Terkoglu, Baris. *MİT'İN YENİ DAİRE BAŞKANI FBI'DA EĞİTİLDİ* . October 8, 2011. https://odatv.com/mitin-yeni-daire-baskani-fbida-egitildi-0810111200.html (accessed February 27, 2019).

TRT Haber. *MIT-Medya Bulusmasinda Neler Konusuldu.* January 5, 2012. https://www.trthaber.com/haber/gundem/mit-medya-bulusmasinda-neler-konusuldu-22952.html (accessed February 25, 2019).

TUBITAK. *BİLGEM Informatics and Information Security Research Center-.* http://bilgem.tubitak.gov.tr/en/kurumsal/bilgem-informatics-and-information-security-research-center (accessed March 5, 2019).

veTeknoloji. *Siber güvenlik strateji çalıştayı yapıldı.* June 20, 2012. https://www.veteknoloji.net/haber/siber-guvenlik-strateji-calistayi-yapildi-54137.html (accessed February 21, 2019).

Yeni Akit. *General atamasi Resmi Gazete'de yayimlandi.* February 22, 2019. https://www.yeniakit.com.tr/haber/general-atamasi-resmi-gazetede-yayimlandi-623845.html (accessed February 28, 2019).

Yeni Akit. *Türk hacker ABD istihbaratına sızdı! Şok eden 'Afrin' mesajı.* March 4, 2018. https://www.yeniakit.com.tr/haber/turk-hacker-abd-istihbaratina-sizdi-sok-eden-afrin-mesaji-431233.html (accessed March 1, 2019).

Yeni Akit. *Türk hackerlardan Belçika medyasına soğuk duş* . October 25, 2017. https://www.yeniakit.com.tr/haber/turk-hackerlardan-belcika-medyasina-soguk-dus-388736.html (accessed March 1, 2019).

Yeni Mesaj. *Ankara Valiliği "hacklendi"* . August 7, 2006. http://www.yenimesaj.com.tr/ankara-valiligi-hacklendi-H1147706.htm (accessed March 11, 2019).