

## The Governance of Turkey's Cyberspace: Between Cyber Security and Information Security

Tuba Eldem

To cite this article: Tuba Eldem (2019): The Governance of Turkey's Cyberspace: Between Cyber Security and Information Security, International Journal of Public Administration, DOI: [10.1080/01900692.2019.1680689](https://doi.org/10.1080/01900692.2019.1680689)

To link to this article: <https://doi.org/10.1080/01900692.2019.1680689>



Published online: 07 Nov 2019.



Submit your article to this journal [↗](#)



Article views: 51



View related articles [↗](#)



View Crossmark data [↗](#)



# The Governance of Turkey's Cyberspace: Between Cyber Security and Information Security

Tuba Eldem 

Department of Political Science and International Relations, Fenerbahçe University, Ataşehir/İstanbul, Turkey

## ABSTRACT

This article explores Turkey's multifaceted cyberspace governance policy and argues that positioned between two opposites of cyberspace governance that has close military and security ties to the West, and domestic Internet policies more similar of Russia-China axis, Turkey should be considered as a swing state in global cyberspace governance debates. The article shows that despite her official discourse on multi-stakeholderism and its compliance with the emerging norms in the Euro-Atlantic alliance concerning cyber-security, cyber-crime, and cyber-defense; Turkey's domestic Internet policy converges towards the Russia-China axis characterized by the rise of information controls and increasing efforts to establish "digital sovereignty" to national cyber space.

## KEYWORDS



Turkey; cyberspace governance; cyber-security policy; internet policy; information security; swing states

## Introduction

Uncertainty and complexity are the most prominent aspects of cyberspace due to both its technical architecture (i.e. ICT's speed, scale, and potential for secrecy) and governing structure (i.e., multi-layered, non-territorial, multi-stakeholder). Such technical and structural uncertainties create novel challenges for policy-makers and scholars of international relations alike. To cope with increasing risks and threats in cyberspace, policy-makers around the world are scrambling to develop national cyber-security strategies, establish new institutions, and promote global cyber norms. In the midst of the ongoing discussions around the applicability of international law and norm of state sovereignty to cyberspace, the securitization of cyberspace (the transformation of the domain into a matter of national security) has been progressing at ever increasing pace. In some countries, far-reaching information control mechanisms, such as filtering and surveillance, were implemented under the disguise of information security and often at the expense of human rights. The ongoing contestation between those actors arguing for greater state oversight of cyberspace and those arguing for a distributed security across many actors – ranging from states, international organizations and the private sector to civil society – exacerbates the current uncertainty prevalent in the global governance of cyberspace.

Although the prominence of radically different understandings of cyberspace governance and cyber-security are widely recognized in the literature of international relations, it is rarely explored outside the cyber "great powers": the US, the EU, Russia, China and Iran. This article attempts to fill this gap by analyzing the governance of cyberspace in Turkey. Few scholars have engaged the issue from the international relations perspective (Bacakci, Doruk, & Celikpala, 2015). The literature on cyber-security in Turkey has tended to be more sector or issue-specific focusing on internet policy (Yesil, Sozeri, & Khazraee, 2017), online surveillance (Yesil & Sozeri, 2017); social media and trolling (Bulut and Yörük 2017; Saka, 2018); hactivism (Polat, Tokgöz, & Sayın, 2013), data protection (Gurkaynak, Yilmaz, & Taskiran, 2014) and critical infrastructures (Karabacak, Yildirim & Baykal, 2016). Others have been technical and proposed a national cyber-firewall system (Sari, 2019), a cyber-security agency organization (Goztepe, Kilic, & Kayaalp, 2014), or analyzed cyber-security from the macro-level (Senturk, Çil and Sağiroğlu, 2012).

This paper aims to fill this gap by providing a context for how national cyber-security is conceived and how cyberspace is governed in Turkey by analyzing both primary and secondary sources, including the national cyber-strategy and action papers, cyberspace legislation, government officials' statements, as well as reports

**CONTACT** Tuba Eldem  [tuba.eldem@fbu.edu.tr](mailto:tuba.eldem@fbu.edu.tr)  Department of Political Science and International Relations, Fenerbahçe University, Atatürk Mahallesi, Metropol İstanbul, Ataşehir Blv., Ataşehir/İstanbul, 34758 Turkey.

Color versions of one or more of the figures in the article can be found online at [www.tandfonline.com/lpad](http://www.tandfonline.com/lpad).

© 2019 Taylor & Francis Group, LLC

prepared by domestic and international cyber IT and social media firms, think-tanks, NGOs, research institutes, and international organizations. The article begins with a brief discussion of global cyberspace governance. It defines the key concepts, outlines main issues, and situates Turkey within the broader global cyberspace governance debates. The second and third sections set out the main institutions governing cyberspace in Turkey and outline Turkey's national cyber-security policy including cyber-crime and cyber-defense. The fourth section discusses Turkey's domestic Internet policy by analyzing pertinent legislation and its implementation. The final section concludes that although Turkey conforms with the emerging cyber-security, cyber-crime and cyber-defense norms in the Euro-Atlantic alliance, her internet policy resembles more of Russia as evidenced by the rise of second and third generation of information controls in national cyberspace.

### Global governance of cyberspace

Initially seen, as a space free from state regulation and intervention, cyberspace has become a key domain of power execution and a core issue of global politics (Nye, 2014). Connecting more than half of all humanity, cyberspace represents an essential element of political, social, economic, and military power worldwide. Data indicate that the growth of national economies is increasingly dependent on the so-called digital economy, which broadly refers both the ICT sector, including telecommunications, internet, IT services, hardware and software, as well as parts of traditional sectors that have been integrated with digital technology (G20, 2016). The digital economy currently stands at about 59% of GDP in the U.S., 46% in Japan, 30% in China, around 20% in Brazil, India, and South Africa (Zhang & Chen, 2019). The global internet population has grown from 400 million in 2000 to 4.4 billion in 2019 and accounts for 57% of the global population. Those 4.4 billion spend an average of 6 hours and 42 minutes online each day (We are Social, 2019). More than 26 billion devices are connected to "the Internet of Things" in 2019, and this number is projected to increase to 75.44 billion worldwide by 2025. Such an omnipresent hyper-connectivity leads to an impressive range of economic, privacy, and national security issues. The estimated global losses from cybercrime have already exceeded \$600 billion per year, a figure that is predicted to reach \$6 trillion annually by 2021 (CSIS, 2018, p. 6). Digital data fraud/theft and cyber attacks against critical infrastructures – are among the top 5 most likely global security risks that world will face in 2019 (WEF, 2019). Privacy problems are on a similar scale: 700 million

records of personal data were lost in 2015 (Finnemore & Hollis, 2016, p. 430).

The securitization of cyberspace (i.e., the transformation of cyber-security into a matter of national security) has been accelerated following the cyber attacks against Estonia in 2007, Georgia in 2008, and Iran in 2010. Since the incident in Estonia made the first major international headlines in 2007, more than 100 states have established governmental cyber capability, and more than 50 of them have defined their national cyber strategies (Hathaway & Klimburg, 2012, p. 2). More than 30 countries have developed military doctrines for cyberspace operations and offensive cyber warfare programs, mostly using 'Information Operations' and 'Information Warfare' as terminology (Ibid, 2012, p. 17). In military-strategic terms, cyberspace is accepted now as a domain equal to land, air, sea, and space (Deibert & Rohozinski, 2010, p. 16).

However, cyberspace creates novel security challenges due to both its governing structure (i.e. multi-layered, non-territorial, multi-stakeholder) and its technical architecture (i.e. ICT's speed, scale, potential for secrecy). Several scholars argue that the multi-layered, non-territorial, and decentralized organization of cyberspace eludes state control. Unlike other domains, such as the sea, land, air, or space, cyberspace is a human-made, multi-layered domain comprising of both "physical and virtual properties." Cyberspace refers both the "virtual environment of information and interactions between people" and the "interdependent network of information technology infrastructures including not only the Internet, but also telecommunications networks, computer systems, and embedded processors and controllers in critical industries" (UK, 2016, p. 75; US, 2008, p. 3; US NSC, 2010, p. 1). A number of different conceptualizations have been offered to define cyberspace in terms of layers, such as the physical network, logical network, and cyber-persona layers used in US Joint Publication 3-12, Cyberspace Operations (2018, p. 3). Deibert, Rohozinski, and Crete-Nishihata (2012) identify four constitutive layers of cyberspace: The foundational layer of cyberspace is the physical infrastructure, which refers to the machines – the routers, cables, cell-phone towers, and satellites – that establish the mechanical and electrical, magnetic, and optical lines of communication. The code layer includes the logical instructions and software that operate communications traffic, such as DNS and ISP. The regulatory level includes all the regulations (i.e. the norms, rules, laws, and principles that govern cyberspace). The ideational or informational level is the sphere through which videos, images, sounds, and text circulate (pp. 5-6).

The concept of cyberspace governance refers to the sum of all regulatory efforts put forward with regard to addressing and guiding the future development and evolution of cyberspace (Feick & Werle, 2012, p. 525). Several scholars argue that the multi-stakeholder, multi-layered global governance structure – which is distributed among a mix of public and private networks – constrains the leadership of states by limiting the points of control. Similar to its technical architecture, the governance of cyberspace is actually multi-layered distributed among several points of control in a variety of issue areas (Dutton & Peltu, 2007). The issues that fall under the cyberspace governance include a wide range of areas related to the exchange of information over cyberspace: spectrum allocation and DNS standards, copyright and intellectual property protection, content regulation, online privacy, cyber-security, cybercrime, cyber-espionage, cyber-defense, cyber security (Mueller, 2010, pp. 79; Nye, 2014, pp. 9–11; Finnemore & Hollis, 2016). Each of these issue areas involves numerous stakeholders, including states, the private sector, and civil society networks. Each issue area, thus, represents different control points and creates challenges for a state leadership and sovereign state control.

Despite the emerging norms and best practices in specific issue areas (Finnemore & Hollis, 2016), the global consensus on cyberspace governance norms is missing at least *partly* due to the division of the states into two opposing groups with diverse political systems and sets of values. The first group of countries – which could be referred as multi-stakeholderists including the United States and European countries – believe in an open and free cyberspace driven largely by global market competition with some government regulation and civil society participation. These countries favor a more open, pluralistic, and transnational policy-making framework allowing for a distributed security across many actors – ranging from states, international organizations, the private sector to civil society – which is often referred to as multi-stakeholderism. The Snowden disclosures in 2013 revealed mass surveillance practices, including top-secret exploitation and disruption programs of the “Five Eyes” spying alliance led by US. Since then, the legitimacy of the “Internet Freedom” agenda backed by the US and its allies has been widely contested (Deibert, 2015; Lyon, 2015; Parsons, 2015).

The second group of countries, which could be referred as cyber-sovereignists, is led by China, Russia and Iran and view national governments as the proper agents for defining and implementing international communication and information policy. They favor

a multilateral governance of cyberspace and prioritize state sovereignty over national “borders” in cyberspace with strict governmental controls on content (Budnitsky & Jia, 2018; Kerr, 2018; Maréchal, 2017; McKune & Ahmed, 2018; Nocetti, 2015; Pallin, 2017; Safshekan, 2017). Instead of cyber-security, many of these countries use the term of information security, which is often seen as “a Trojan horse for increased content control and Internet censorship” (Ebert & Maurer, 2013, p. 1055). Building on Russia’s efforts since 1998, four of the six members of the Shanghai Cooperation Organization (SCO), including China, Russia, Tajikistan and Uzbekistan, submitted a proposal in 2011 for an ‘International Code of Conduct for Information Security’ to the UN General Assembly. Although the code states that countries must respect “human rights and fundamental freedoms,” the Convention (2011) considers “actions in the information space aimed at undermining the political, economic, and social system of another government, and psychological campaigns carried out against the population of a State with the intent of destabilizing society” as one of the main threats in the information space (Article 4). It emphasizes in its Preamble that “political authority in connection with governmental policy issues related to the Internet is a sovereign right of States, and that the governments of States have rights and responsibilities as regards governmental policy issues related to the Internet on an international level.” To secure information, these countries favor a multilateral approach in governing cyberspace, preferably under an intergovernmental organization, which will give them the sovereign right to guide and steer cyberspace.

Caught in the middle are the “*swing states*” – countries that have the capacity for outsize influence on international processes due to their resources, but have not decided which vision for the future of the Internet they will support (Ebert & Maurer, 2013). According to many, the direction these countries may, together, decisively shape the trajectory of the global cyberspace governance regime. This paper argues that Turkey should be considered as a global swing state in global cyberspace governance debates as it’s positioned between two opposites of cyberspace governance: close military and security ties to the West, on the one hand, and domestic information control policies similar to the Russia-China axis. For instance, in 2012, Turkey voted in favor of a new set of International Telecommunications Regulations (ITRs), which was also backed by Russia and China and argued for expanding the state’s role in Internet governance. The proposal introduced during the 2012 World Conference on International Telecommunications (WCIT) in Dubai aimed at changing the multi-stakeholder

model by giving a greater role to the state-only International Telecommunications Union (ITU). The ITU system allowing each member state a single vote overpowers strong private actors' voices and empowers non-Western nations. Along with Mexico and South Korea, Turkey was one of only three OECD countries that voted in favor mostly given its limited resources, it felt largely left out of current model. However, Turkey later defined multi-stakeholderism as a preferred model for cyberspace governance in its National Security Strategy and Action plans published in 2013 and updated in 2016.

Turkey also endorsed the OECD's Principles for Internet Policy-Making at the Internet Governance Forum held in Istanbul in (IGF, 2014). The OECD principles includes amongst others, multi-stakeholderism, protection of the global free flow of information, and the open, distributed and interconnected nature of the Internet. In 2014, Turkey was also one of a core group of countries along with the United States and Sweden backing resolutions at the UN Human Rights Council (HRC) on "the promotion, protection and enjoyment of human rights on the Internet." Turkey reaffirmed "the same rights that people have offline must also be protected online" on July 1, 2016, and declined to vote for Russia and China-led amendments to the resolution. The amendments included deleting calls for states to adopt a "human rights based approach" for providing and expanding access to the Internet and removing key references to the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (Kart, 2016). Despite, its rejection of such calls, Turkey's domestic Internet policy especially since 2013 converges towards prioritizing information security promoted by Russia and China. This paper expands this argument in further sections after shedding light on the main institutions governing Turkey's cyberspace.

### Domestic institutions governing Turkey's cyberspace

The Ministry of Transport and Infrastructure (Ulaştırma ve Altyapı Bakanlığı, MTI) is the main institution for making policies on information and communication technologies and national cyber-security in Turkey. The MTI was given the authority to prepare national cyber-security policies, strategies, and action plans by the Council of Ministers (2012) Decision No. 28447 on the "Execution, Management and Coordination of National Cyber-security Activities," which also established the National Cyber Security Board (NCSB) to implement and coordinate national cyber-security strategy plans. The MTI ensures information security and privacy; safeguards the

infrastructures, systems, and databases of information and communication technologies; identifies critical infrastructures and strengthens these systems against potential cyber threats and attacks. In addition to implementing and coordinating national cyber-security activities, the NCSB identifies the measures for cyber-security, proposes the identification of critical infrastructures and determines which institutions and organizations are exempted from all or some of the provisions related to cyber-security. The MTI oversees the NCSB, which includes the undersecretaries of the Ministries of Foreign Affairs, Interior, National Defense, Transport, Maritime Affairs and Communications, as well as the undersecretaries of Public Order and Security, National Intelligence Organization, Head of Communication, Electronic and Information Systems of Turkish General Staff, Head of Information and Communication Technologies Authority, Head of the Scientific and Technological Research Council, Head of Financial Crimes Investigation Council, and Head of Telecommunications Communication Presidency.

The Information and Communication Technologies Authority (Bilgi Teknolojileri ve İletişim Kurumu BTK) is the main regulatory institution in cyberspace and the electronic communication sector. The BTK, was established as a department under the MTI in November 2008 with the Electronic Communication Law No. 5809 and was preceded by the Telecommunications Authority (TA) founded in January 2000 under the Telegram and Telephone Law. The BTK is tasked with authorizing, inspecting, resolving disputes, protecting consumer rights, regulating competition in the sector, issuing technical regulations, and managing and inspecting the spectrum.

The Telecommunications and Communication Presidency (Telekomünikasyon İletişim Başkanlığı, TIB) was founded with the Law No. 5809 in 2005 as a department under the BTK responsible for surveillance and interception of communications in Turkey. TIB's duties were broadened in scope by Internet Law No. 5651 on the "Regulation of Publications on the Internet and Suppression of Crimes Committed by means of such Publications" (2007) to include monitoring and regulating online content, service providers, access providers, and public Internet access providers. The TIB, has always been a controversial institution lying at the center of the freedom of access vs. censorship and surveillance vs. privacy (Bicakci Doruk & Celikpala, 2015, p. 26). It was subsequently shut down after the coup attempt due to suspicions that "Fethullah Terror Organization/Parallel State Structures" (FETÖ/PDY) members used TIB as a "headquarters for illegal wiretapping". The BTK was given all of TIB's responsibilities (The Emergency Decree No. 671). Now, the BTK is authorized to take "any necessary measure" to

“uphold national security and public order; prevent crime; protect public health and public morals; or protect the rights and freedoms.” The institution is also authorized to inform operators, access providers, data centers, hosting providers and content providers of said measure, who are then required to implement government orders within two hours.

At the operational level, the BTK has been working with the Turkish National Computer Emergency Response Center (USOM, TR-CERT) to oversee and carry out cyber-security activities. TR-CERT and sectoral and institutional Cyber Events Response Teams (CERTs) were established in November 2013 to respond to the cyber security incidents. Established under the BTK umbrella, TR-CERT is tasked with monitoring and issuing warnings and announcements for cyber-security incidents, providing national and international coordination to prevent cyber-attacks against critical sectors, and assisting the organizations responsible for forming their own sub-CERTs. The TR-CERT is divided into two subgroups for governmental CERTs and private sector CERTs. Institutional CERTs are responsible for the main governmental institutions and bodies. Sectoral CERTs specialize in critical infrastructure sectors such as transportation, energy, electronic communications, finance, water management, and critical governmental services. Although the CIRT falls under the MTI, there is no direct connection between them in day-to-day operations (See Figure 1).

The top authority for the defense of military networks and the top military CERT in Turkey is the Turkish Armed Forces (TAF) Communications and Information Systems

and Cyber Security Command (CDC). Founded in August 2013 and positioned under the Communications, Electronics and Information Systems Directorate of the Turkish General Staff, the TAF CDC is a joint command that has personnel from all services. The modernization program of the TAF CDC established a new Military-CERT command center, a dedicated cyber defense-training laboratory, a military network monitoring facility, and related support structures.

The Turkish National Police’s (TNP) Department of Combatting Cyber Crime (CCC) is responsible for investigating crimes committed using information technology and the examination of forensic data and digital evidence (Bicakci et al., 2015, p. 34). The department was founded in 2011 under the name of “Combating IT Crimes” and was renamed in 2013. It maintains 27,000 personnel active in 76 of 81 Turkish provinces, 562 of whom are experts in informatics and surveillance. The department has recently founded a special desk to investigate “insults against state authorities” (Kizilkoyun, 2018).

The National Intelligence Service (Milli Istihbarat Teskilati, MIT) is responsible for collecting the necessary cyber-intelligence to prevent cyber security threats. Law No: 6532 Amending the Law on State Intelligence Services and the National Intelligence Agency entered into force on April 26, 2014 and redefined the role of the MIT to include: “delivering the produced intelligence to relevant institutions on Foreign Intelligence, National Defense, Counter-terrorism, international crimes and cyber security topics by using all types of technical intelligence, human intelligence via utilizing

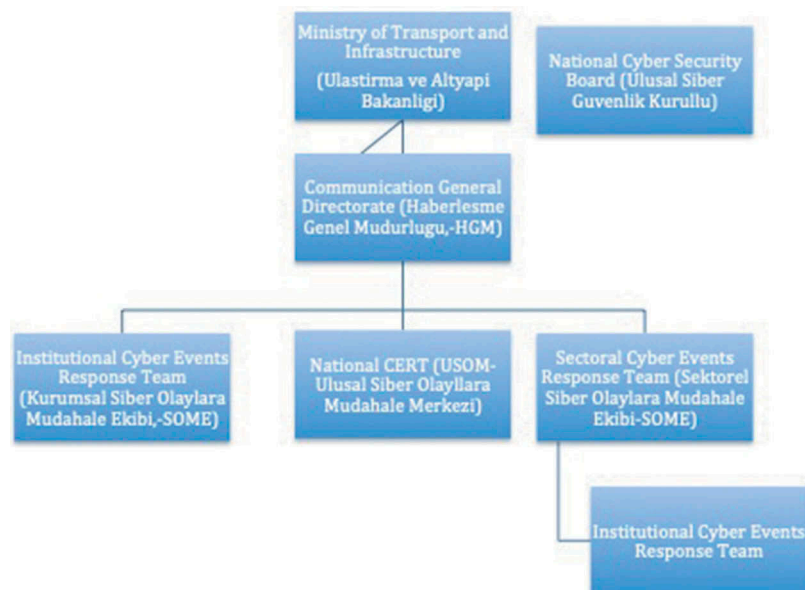


Figure 1. Organizational structure of cybersecurity governance in Turkey.

relevant tools, methods and systems with the process of collecting, recording and analyzing pertinent information, document, news and data.” MIT has since then has paid substantial effort to develop a cyber intelligence capability procuring technical equipment, reorganizing its departments, and recruiting experts in the all-relevant fields (Bicakci et al., 2015, p.34).

The Informatics and Information Security Research Centre (BILGEM) of the Scientific and Technological Research Council of Turkey (TUBITAK) is responsible for national research and development activities on information technology, information security, and advanced electronics. TUBITAK BILGEM maintains more than 1,600 staff and is composed of the following institutes: the National Research Institute of Electronics and Cryptology (UEKAE), the Information Technologies Institute (BTE), the Advanced Technologies Research Institute (İLTAREN), the Cyber-security Institute (SGE), and the Software Technologies Research Institute (YTE). Since 2007, TUBITAK BILGEM holds “cyber-security maneuvers” similar to war games carried out by conventional militaries, participates in NATO exercises with its products, and coordinates joint CERT exercises among institutional CERTs. In 2013, BILGEM designed and produced Turkey’s first Real-Time Operating System. BILGEM’s official website declares that thanks to the projects achieved by the affiliated institutes, “Turkey has become one of the few countries declaring its technological independence in the fields of information security and informatics.”

### Turkey’s cyber-security policy

Similar to the prevalent understanding in the Euro-Atlantic alliance, Turkey’s cyber-security strategy perceives cyberspace as crucial for both national security and economic prosperity and aims to develop a national cyber-security infrastructure to guarantee the complete security of all systems and stakeholders in the national cyberspace. Turkey’s first National Cyber Security Strategy (NCSS) published in 2013 gave priority to protecting the information systems of critical infrastructures such as electronic communication, energy, water management, critical public services, transportation, and banking and finance. Turkey’s revised NCSS and Action Plan (2016–2019) integrates cyber-security into its national security strategy and calls for the acquisition of administrative and technological competency for securing the national cyberspace. The Ministry of Transportation, Maritime and Communication (MTI, 2016, p. 11). In line with these two main objectives, it identifies three strategic sub-objectives that need to be addressed:

- Safeguarding the security, confidentiality, and privacy of all services, transactions and information/data
- Determining cyber-security actions to minimize the effects of cyber-security incidents, recovering systems quickly, and ensuring higher efficiency in the judicial investigation of cyber-crimes
- Developing national critical technologies and products (pp.11–12).

In order to achieve these goals, the action plan outlines five strategic action steps for 2016–2019: Strengthening the cyber defense and protection of critical infrastructures; combating cyber crime; enhancing awareness and human resources; developing a cyber-security ecosystem; and integrating cyber-security into national security (pp. 20–23).

To secure the cyberspace, Turkey’s national cyber-security strategy favors the multi-stakeholder governance model (MTI, 2013, p.15; 2016, p. 4). This understanding is best reflected in the revised NCSS vision statement, which ultimately endeavors to establish of “an ecosystem that has international competitive power in the field of cyber security, in which all stakeholders related to cyber security manage risks at cyberspace in a competent manner in cooperation with each other in order to benefit from information and communication technologies in the most efficient way for the purpose of contributing to wealth and security of society, as well as national economic growth and efficiency”. Highlighting the ongoing commitment to multi-stakeholderism, the revised NCSS was prepared in 2016 following a series of evaluation meetings with institutions that were considered responsible or associated in the previous action plan, including those that represented public institutions, critical infrastructure operators, the IT sector, universities and non-governmental organizations.

As outlined by the NSSF, the Turkish government has also recently placed increased emphasis on developing public-private partnerships in the national cyber-security domain. In October 2017, the Presidency of Defense Industries invited the private sector’s major cyber-security companies to create mutual trust and cooperation between public and private institutions and to discuss public-private partnership opportunities. The meetings resulted in the initiation of the Turkish Cyber Security Cluster project with the participation of all public agencies, organizations, and representatives from the private sector and academia. The project’s aim is to increase the number of Turkey’s cyber security companies and to foster national and domestic technologies in the area of cyber-security.

In order to achieve and maintain cyberspace security, Turkey’s national cyber-security strategy recognizes the

significance of international cooperation and information sharing and aims to harmonize domestic cyber-security legislation with international agreements and regulations (MTI, 2013, pp. 15–16). In 2014, Turkey ratified the Council of Europe's Cybercrime Convention with Law No. 6533, thereby harmonizing its national laws. The Convention harmonizes policies around dealing with crimes in cyberspace, including those relating to infringements of copyright, intellectual property rights, computer-related fraud and data theft, violations of network security as well as child pornography and hate crimes. On April 19, 2016, Turkey became a signatory of the Council of Europe's "Additional Protocol to the Convention on Cybercrime" (2006), which concerns the criminalization of racist and xenophobic acts committed through computer systems. Ratification of the additional protocol, though, is still pending.

Additionally, Turkey is aligned with the commonly accepted understanding of the applicability of international law to cyberspace. Under Turkey's Presidency, the G20 Leaders adopted a Communiqué on cyber-security in November 2015 in Antalya. The G20 Leaders' Communiqué emphasized the cyber-security consensus report prepared by the UN Group of Governmental Experts concerning norms, rules, or principles of the States' responsible behavior in the cyber-sphere, reaffirmed the applicability of international law, and in particular the UN Charter, to state conduct in the use of ICTs and endorsed the prohibition on cyber-espionage for commercial purposes (G20, 2015).

Turkey is generally supportive of international governance institutions, as the country has participated in several regional and international ICT security cooperation initiatives. In fact, Turkey organized the first International Cyber Security Exercise. In cooperation with ITU-IMPACT, BTK held the International Cyber Shield Exercise 2014 in Istanbul on May 14–15, 2014. The intent of this exercise was to contribute to ongoing global activities related to building confidence and security in the use of ICTs; to provide a platform for information sharing on key aspects pertaining to cyber-security; and to pay particular attention to the effective handling of incidents by Computer Security Incident Response Team and CERT. The event was connected with the ITU Global Cybersecurity Agenda and Hyderabad Action Plan Program 2 concerning cyber-security, ICT applications and IP-based network-related issues. The event saw the participation of 17 countries – Albania, Angola, Azerbaijan, Bosnia and Herzegovina, Bulgaria, Georgia, Italy, Jordan, Lithuania, Malaysia, Romania, Sri Lanka, Senegal, Spain, Sudan, Turkey, and Ukraine (ITU, 2014b). National CIRTs that were participants

engaged in a series of real-life cyber threat simulations to assess their capabilities to deal with incidents. The exercise brought together CIRT practitioners, senior government officials, cyber-security experts, related industry players, and other stakeholder groups from the ICT and security sectors.

To facilitate the sharing of cyber-security assets in wider Europe, Turkey also contributes to regional efforts such as the European Cyber Security Protection Alliance and the RACVIAC. In 2017, Turkey's MTI and Ministry Foreign Affairs co-organized a Cyber Security Advanced Training Course with RACVIAC in Antalya, Turkey. Turkey has also officially recognized partnerships regarding cybersecurity with a number of countries including Albania, Azerbaijan, Bosnia and Herzegovina, Bulgaria, Kosovo, Kyrgyzstan, Macedonia, Montenegro, Morocco, Niger, Republic of Sudan, Senegal, Serbia, Tunisia, Iran, Thailand, Egypt and Ukraine (ITU, 2014a, p. 2).

Concerning cyber-defense, Turkey joined the NATO Cooperative Cyber Defense Center of Excellence (CCD COE) as a sponsoring nation in 2015 and as per NATO's recognition of cyberspace as a domain of operations in the July 2016 Warsaw Summit, Turkey considers cyber defense as a distinct military domain. Turkey's cyber defense strategy rests on establishing and maintaining strong and resilient cyber defense capabilities that can cope with the increasing threats and hostility coming from the state or non-state actors in cyberspace. The Project Definition Document on Cyber-security – which was approved by the Minister of National Security in 2014 – requires the TAF CDC to acquire only nationally-produced software and hardware that are compatible for use in NATO joint exercises (Bicakci et al., 2015, p. 34). The TAF CDC prioritizes strengthening the national cyber defense capabilities through recruiting and training new personnel through cooperation with national defense contractors, universities, and technical institutes. The TAF CDC conducts coordination and joint activities with NATO cyber entities and organizations, contributes to international exercises such as NATO's Cyber Coalition, Locked Shields since 2010, and Crisis Management Exercise (CMX). The national cyber defense exercises are also carried out annually to measure the competence of the public institutions against cyber threats for both military and non-military cyber defense objectives. The main aim of the exercises is to train to act proactively against threats to national interests or citizens, to prevent attacks, to eliminate them, and to develop counter-measures (Seker and Tolga, 2018, p. 14).

Turkey cooperates with the members of the Euro-Atlantic alliance in certain areas where mutual interests overlap such as cyber-security, cyber-crime, cyber-defense; however, this is less the case when it



comes to Turkey's domestic Internet policy. The section below discusses the trajectory of Turkey's domestic Internet policy and argues that the country has increasingly prioritized "information security," territorialized controls, and sovereign rights in cyberspace since 2013.

### Turkey's internet policy

Turkish authorities have, over the last decade, extended their power to control the flow of information and regulate speech on the Internet. The Gezi protest movement in June 2013 that followed the uprisings in the Arab world has had a profound impact on the minds of Turkish ruling elite. Reflecting on the sustained use of digital technologies – micro-blogs such as Twitter, video platforms such as YouTube and social networks such as Facebook – in Istanbul, Turkish law enforcement agencies started to closely monitor the impact of the political use of networked technologies on social mobilization. The Gezi uprising was followed by a corruption scandal in December 2013, which was unearthed by leaked tapes and phone conversations. During the subsequent months, an ample amount of voice recordings – including those recorded in a highly sensitive top-level meeting at the Foreign Ministry – were released, and the probes to discover their origins spread to TUBITAK and BILGEM by the beginning of 2014. The government accused the Gulen Movement [now officially referred to as the Fethullah Gulen Terror Organization (FETO)], claiming that the network had infiltrated the top levels of Turkey's state structure and orchestrated the plot against the government. The election cycle that followed – a local election in March 2014, presidential elections in August 2014, and parliamentary elections in June and November 2015 – quickly reawakened anxiety among Turkish leadership over the 'power of networks' and triggered the use of extended of information controls in Turkey.

State control of the Internet began in 2007 through filtering social content and denying access to specific Internet resources by directly blocking access to servers, domains, keywords, and IP addresses. This was further complemented with the growth and spread of what Deibert and Crete-Nishihata (2012) refer to as second and third-generation cyberspace controls. These involved passing legal restrictions, issuing content removal requests, ordering the shutdown of websites and social media platforms, prosecuting internet users, as well as enhancing state surveillance and disinformation and smear campaigns led by a troll-army and automated bots.

### **Second generation controls: legal restrictions, content removals, securitization and prosecution of online content**

Turkey's first Internet Law No. 5651 entitled "Regulation of Publications on the Internet and Suppression of Crimes Committed by means of Such Publications" was approved in May 2007 with the stated objective of protecting families and minors (Akgul and Kirlidog 2015). The law set forth the criteria for blocking websites and further defined the responsibilities of content providers, hosting companies, mass-use providers (such as internet cafes), and Internet Service Providers (ISPs). It also designated the roles and obligations of Internet actors and handed power over to TIB to monitor online content and direct hosting and access providers. Article 8 delineated seven categorical crimes (incitement to suicide, facilitation of the use of narcotics, child pornography, obscenity, prostitution, facilitation of gambling, and slandering of the legacy of Atatürk – the founder of modern Turkey) for which a website may be blocked. This article also authorized TIB to combat such crimes. According to Article 8 of the law, although all blocking decisions were to be given by the judiciary, the TIB was authorized to block access if the content provider or the hosting provider resided outside Turkey. The ISPs were required to execute blocking decisions within 24 hours of receiving the order. Failing to do so would be punishable with imprisonment from six months up to two years (Kinikoglu, 2014, pp. 39–40).

As a result, approximately 3,700 websites were blocked between 2007 and 2009 (Akdeniz, 2010, p. 4). By May 2009, courts and prosecutors had issued 2,601 orders to ban websites in response to approximately 81,691 complaints, which was a significant increase from the roughly 1,475 bans ordered for 17,768 complaints in the previous year (US State Department, 2010). The restrictions on Internet access had accelerated to such an extent that on March 11, 2010, Reporters Without Borders added Turkey to the list of "countries under surveillance." The Ankara-based Association of Internet Technologies filed a complaint about website blocking to the European Court of Human Rights (ECHR), accusing the Turkish authorities of violating freedom of expression. The ECHR (2013) ruled that the Turkish Internet Law was against the European Convention on Human Rights (Akgul and Kirlidog, 2015).

Despite the ECHR ruling, Internet Law No. 5651 was hastily amended following the Gezi protests and the corruption investigations in late 2013. The amendments adopted in February 2014 (Law No. 6518 and Law No. 6527), September 2014 (Law No. 6518/89), and March 2015 (Law No. 6639/29) broadened the scope of regulators' powers to block content without a court order.

The Law No. 6639 empowered the TIB to block online content without a prior court order based on a complaint filed for breaching an individual's right to privacy and *extended* government control over the Internet. The Prime Minister and other relevant ministers are empowered to immediately request the removal of Internet content and/or blocking of a website when a court order for such action has been delayed and a risk to public or national security exists (European commission for democracy through law, 2016). The total number of blocked websites accordingly rose from about 40,000 in 2013 to more than 115,000 in 2016 (Yesil et al., 2017).

In addition to websites, several social media platforms have been blocked in Turkey due to a single case of offending content or on the grounds of copyright infringement. YouTube remained notoriously inaccessible between 2008 and 2010; the access to Google's blogger.com and blogspot.com were blocked for a few days in October 2008, and the image-sharing site Imgur has been blocked since 2015. Twitter became inaccessible on March 20, 2014 only hours after PM Erdoğan vowed to close down the social media platform at a campaign rally for the upcoming local elections. The ban was lifted on April 2 when the Constitutional Court ruled the ban illegal, but this was only after the local elections, which were held on March 30, 2014 (HDN, 2015). More than 10 VPN services, as well as the circumvention tool Tor, have been banned since November 2016. Wikipedia has been inaccessible since May 2017.

Governmental requests for the removal of content both on international social media platforms and on popular Turkish websites are also widespread. On March 24, 2014, Twitter declared that it had started to use its Country Withheld Content tool for the first time in Turkey. Since then, Turkey has been the country submitting the most removal requests to Twitter in terms of volume. Between 2014 and 2017, Turkey has accounted for more than 52% of removal requests worldwide. In the first half of 2018, the number of legal demands made by Turkey doubled, making up roughly 73% of the total legal requests internationally. In the first half of 2018, Twitter complied with 18% of Turkey's removal requests (Twitter, 2019).

Similar to the Russian "web brigades" that are made up of hundreds of thousands of paid users write positive comments about the Putin administration, an "army of trolls" was recruited to reassert ruling party's declining hegemony in the broader civil society shortly after the Gezi Park protests in 2013 (Bulut and Yörük 2017). Numbering around 6,000 individuals, Aktrolls scrutinized the Twitter, manipulated online discussions, promoted government propaganda, and orchestrated

harassment campaigns against anyone critical of the government on social media and spread fake news (Albayrak & Parkinson, 2013). With the goal to discredit, intimate, and suppress critical voices, Aktrolls label particularly journalists and celebrities as "traitors," "terrorists," "supporters of terrorism," and "infidels" (Saka, 2018). Since the Gezi protests, Twitter has been transformed into "a medium of government-led populist polarization, misinformation and lynching" (Bulut & Yoruk, 2017). Internet bots – which are software applications running automated tasks over the Internet – are also extensively deployed by the government to assist paid individuals (Yesil et al., 2017). According to the software company Norton, Turkey has the highest bot population in Europe, the Middle East, and Africa (Yesil et al., 2017, p.24).

Since 2013, Turkish authorities have used existing laws such as the Penal Code and the Anti-Terror Law in the online environment to penalize online content that fell outside the purview of the Internet Law. The Turkish Constitution guarantees freedom of communication (Article 22), thought and opinion (Article 25), expression and dissemination of thought (Article 26) as well as the press (Article 28). Yet these civil rights and freedoms are becoming increasingly subjected to undue restrictions in the name of protecting "national security," "public order and public safety," and "the proper functioning of the judiciary" (Article 26). Furthermore, Article 28 of the Turkish Constitution stipulates that it is an offence to write or print any news or articles that "threaten the internal or external security of the state or the indivisible integrity of the state with its territory and nation, which tend to incite offence, riot or insurrection, or which refer to classified state secrets."

In addition to these constitutional limitations, a series of articles in the Turkish Penal Code – particularly the broad provisions on criminal defamation – are widely employed to restrict freedom of expression online. The most commonly used articles in the Turkish Penal Code are Article 301: Denigration of the Turkish nation, Article 125: Defamation against public officers, Article 215: Praising a crime or a criminal, Article 216: Incitement to hatred or hostility, Article 220/6: Committing a crime in the name of a terrorist organization, Article 220/7: Assisting a terrorist organization, Article 285: Violating the confidentiality of the investigation, Article 299: Defamation of the president and Article 314: Membership of a terrorist organization. Broad and unclear provisions in the Anti-Terrorism Law such as Article 6/2: Printing or publishing of declarations or statements of terrorist organizations and Article 7/2: Making propaganda for a terrorist organization have also been widely used

since 2009 to prosecute and jail netizens. Although most of the prosecutions under the antiterrorism law were charged of having links to the Kurdish Communities Union (KCK), the urban wing of the outlawed separatist Kurdistan Workers' Party (PKK), or to FETO, several journalists, academics, and ordinary citizens with no link to terrorism were prosecuted or detained in connection with the independent reporting of the war in Syria, expressions of Kurdish identity, and nonviolent criticism of the government (Freedom House, 2018).

The prosecution of social media users also escalated immediately after the failed July 2016 coup as the Turkish National Police (TNP) introduced a smart phone app and a dedicated webpage that allowed citizens to report social media posts that they consider as terrorist propaganda (Yeni Şafak, 2016). The main opposition party declared that police prepared summary of proceedings for 17,000 social media users and addresses of 45,000 others are being tried to be located (Bianet, 2017).

### ***Third-generation information controls: enhanced technical capabilities and expanded state surveillance***

The end of peace process leading to the resumption of the armed conflict with the PKK and the escalation of ISIS attacks following the June 2015 elections strengthened the position of Erdoğan's government in the November 2015 elections. These developments also contributed to the ruling party's growing security-first outlook in domestic policy making during its fourth consecutive term in power. Citing security concerns, the Turkish government began utilizing new tools such as bandwidth throttling, which is the intentional slowing of an internet service by an ISP. This happened during times of security or political crises such as the detention of pro-Kurdish People's Democratic Party (Halkin Demokrasi Partisi, HDP) representatives in (Bianet, 2016), the military coup attempt in 2016, and terror attacks in Istanbul, Ankara, and Suruc between 2015 and 2016 (Yesil et al, 2017). In December 2016, the BTK ordered Turkish ISPs to block popular VPN services and the Tor Network to enable the full implementation of throttling and banning orders (BBC, 2016). Since 2016, news sites have come under distributed denial-of-service (DDoS) attacks and other technical attacks at politically sensitive moments such as in the middle of elections or after publishing controversial information (Freedom House, 2018). The HDP website was attacked two days before the June 2015 elections and could not be accessed for over 24 hours (Ibid).

State surveillance of cyberspace has been extended with an amendment made on Law no: 6532 on State Intelligence Services and the National Intelligence Agency (MIT). The amendments adopted in April 2014 empowered MIT to access any online and offline "information, documents, data, or records from public institutions, financial institutions, and entities with or without a legal character." This would mean that MIT would not only be able to get citizens' personal data from any public or private institution (banks, schools, hospitals, ISPs) but also to intercept and store private data on "external intelligence, national defense, terrorism, international crimes, and cyber-security" passing through telecommunication channels" without a court order (HRW, 2014). The leaking and publication of secret official information including on social media was criminalized by a prison term of up to nine years. The judicial accountability of MIT personnel was also limited by requiring the courts to obtain the permission from the head of the agency prior to investigation (Freedom House, 2018). The law established that no other legal obligation – national or international – could overrule an MIT request, and made the refusal to comply with a request punishable by up to five years in prison.

In March 2015, the Homeland Security Act amended several laws and further enhanced state surveillance over cyberspace. The amendment on the Law on the Powers and Duties of Police increased the amount of time in which investigators could conduct wiretaps and other signals intelligence operations without a court order from 24 to 48 hours. Additionally, in so-called urgent situations, the police are authorized to request user data from telecommunications companies to locate the user, and monitor and sift through their communications (Yesil et al., 2017).

The coup attempt orchestrated by FETO on July 15, 2016 created a major backlash and prompted a new wave of surveillance. Under a state of emergency that lasted from July 20, 2016 to July 20, 2018, the executive adopted a total of 32 decrees in the force of law with an aim to "cleanse the army, law enforcement and state institutions from 'the Fethullah Terror Organization/ Parallel State Structures.'" Three of these 32 decrees (i.e. Decree Laws 670, 671, and 680) have expanded governmental surveillance power (Ergun, 2018; Yesil et al., 2017). Decree Law No. 670 paved the way for the interception of the digital communications of users who are being investigated for coup-related reasons and the collection of their private data from all public authorities and private companies. As mentioned before, Emergency Decree No. 671 shut down TIB and instead authorized the BTK to take "any necessary

measure” to “uphold national security and public order; prevent crime; protect public health and public morals; or protect the rights and freedoms” and inform operators, access providers, data centers, hosting providers, and content providers of the said measure, who were then required to implement government orders within two hours. Decree Law No. 680 further expanded the authority of the Turkish National Police Department of Cybercrimes to “detect, surveil, evaluate the signals information, and record data transferred through telecommunications and internet, as well as traffic information between internet sources” without a court approval for 24 hours (Article 28).

In an attempt to enhance state control over online videos and internet broadcasting, the Turkish parliament with the majority votes of the ruling AKP and its political ally the Nationalist Movement Party (MHP) enacted an amendment to the Turkish radio and television legislation that brings service providers broadcasting on Internet under the supervision and authority of the Radio and Television Supreme Council (RTUK). The amendment enacted on March 21, 2018 under Law No. 7103 requires providers of broadcasting services through internet to obtain a license from RTUK. The amendment covers both local and foreign media service providers with “commercial communications broadcasting,” including Netflix as well as Deutsche Welle, BBC, and Voice of America. Social media platforms that deliver news on a regular basis, such as Medyascope.tv (which delivers audiovisual journalistic content via Periscope) are also subjected to the same regulations. In the absence of a license, a magistrate judge will be able to deny access to specific content within 24 hours following a complaint from the RTUK. Along with the licensing requirement, RTUK is able to demand the removal of content or the restriction of access to these platforms. This means that RTUK will have the authority to regulate and monitor every kind of sound and visual broadcasting shared on the Internet on a regular basis (HDN, 2018).

## Conclusion

Turkey’s regional identity as part of Europe or Asia came under growing contention both at home and abroad. For many, Turkey’s NATO membership is no longer enough to make Turkey part of “the West” in the post-Cold War era. The deterioration of Turkey’s relationship with the EU, ironically after the start of accession negotiations in October 2005, had exacerbated this confusion. Turkey’s cyberspace policy underscores this ambiguity and uncertainty surrounding Turkey’s regional identity and foreign policy alignments. On the one

hand, Turkey has strong diplomatic and security relationships with the Euro-Atlantic alliance that champions an open, decentralized, and distributed global communications network secured through the participation of various stakeholders. In line with the alliance, Turkey favors multi-stakeholderism to govern and secure cyberspace, recognizes the applicability of international law to cyberspace, and declares its commitment to the norms, rules, or principles of the responsible behavior of states in the cyber-sphere. Turkey also actively engages in information sharing, capacity building, and other international cooperation efforts for achieving and maintaining national and global cyberspace security. Turkey harmonized its cybercrime legislation in line with Budapest convention and as per NATO’s recognition of cyberspace as a domain of operations, Turkey considers cyber defense as a distinct military domain.

Turkey’s domestic Internet policy prioritizing digital sovereignty and information security over privacy and Internet freedoms brings Turkey, however, closer to Russia-China axis in global internet governance debates. The sustained use of digital technologies during the Gezi protests and also by the members of Gulenist network have quickly reawakened Turkish leaders’ anxiety over the “power of networks.” Ankara, has thus, in the recent years, taken a neo-Hobbesian view of cyberspace and attempts to exert sovereignty at this chaotic domain through employing second- and third-generation information controls. These practices, however, introducing friction and disruption to the cyberspace not only hinder Turkey’s objective of forming and sustaining a secure and resilient cyberspace eco-system, but also further detach her from the Euro-Atlantic alliance where her security and economic interests are still most strongly linked.

## Disclosure statement

No potential conflict of interest was reported by the authors.

## ORCID

Tuba Eldem  <http://orcid.org/0000-0001-6264-255X>

## References

- Akdeniz, Y. (2010). *Report of the OSCE representative on freedom of the media on Turkey and internet censorship*, Organization of Security and Cooperation in Europe. Retrieved from [https://www.osce.org/fom/41091?download=trueinternet\\_censorship.pdf](https://www.osce.org/fom/41091?download=trueinternet_censorship.pdf)
- Akgul, M., & Kirlidog, M. (2015). Internet censorship in Turkey. *Internet Policy Review*, 4(2), Retrieved from <http://policyreview.info/articles/analysis/internet-censorship-turkey>.

- Albayrak, A., & Parkinson, J. (2013, September 16). Turkey's government forms 6,000-member social media team. *The Wall Street Journal*, Available at <https://www.wsj.com/articles/turkeys-government-forms-6000-member-social-media-team-1379351399>.
- BBC. (2016, December 19). Turkey blocks access to tor anonymising network. Retrieved from <https://www.bbc.com/news/technology-38365564>
- Bianet. (2016, October 26). Internet outage in eastern and southeastern Turkey, <https://bianet.org/english/media/180001-internet-outage-in-eastern-and-southeastern-turkey>
- Bianet. (2017, January 16). Yarkadaş: Summary of proceedings prepared for 17,000 social media users. Retrieved from <http://m.bianet.org/bianet/society/182737-yarkadas-summary-of-proceedings-prepared-for-17-000-social-media-users>
- Bicakci, S., Doruk, E., Celikpala, M. (2015). The Cyber security scene in Turkey. In Bicakci et al. *A primer on cyber security in Turkey and the case of nuclear power* (pp. 22–51). Istanbul, Turkey: EDAM: The Centre for Economics and Foreign Policy Studies. doi:10.13140/RG.2.1.4774.9204.
- Budnitsky, S., & Jia, L. (2018). Branding internet sovereignty: Digital media and the Chinese–Russian cyber alliance. *European Journal of Cultural Studies*, 21(5), 594–613. doi:10.1177/1367549417751151
- Bulut, E., & Yoruk, E. (2017). Mediatized populisms| Digital populism: Trolls and political polarization of Twitter in Turkey. *International Journal of Communication*, 11(25), 4093–4117.
- Center for Strategic and International Studies (CSIS). (2018). *Economic impact of cybercrime: No slowing down*. Retrieved from <https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf>
- Deibert, R. (2015). The geopolitics of cyberspace after Snowden. *Current History*, 114(768), 9–15.
- Deibert, R. J., & Crete-Nishihata, M. (2012). Global governance and the spread of cyberspace controls. *Global Governance*, 18, 339–361. doi:10.1163/19426720-01803006
- Deibert, R. J., & Rohozinski, R. (2010, March). Risking security: Policies and paradoxes of cyberspace security. *International Political Sociology*, 4(1), 15–32. doi:10.1111/j.1749-5687.2009.00088.x
- Dutton, W. H., & Peltu, M. (2007). The Emerging internet governance mosaic: Connecting the pieces. *Information Polity*, 12, 63–81. doi:10.3233/IP-2007-0113
- Ebert, H., & Maurer, T. (2013). Contested cyberspace and rising powers. *Third World Quarterly*, 34(6), 1054–1074. doi:10.1080/01436597.2013.802502
- Emergency Decree Law No. 670, Official Gazette No: 29804. dated 17 August 2016, Retrieved from <https://www.resmigazete.gov.tr/eskiler/2016/08/20160817-17.htm>
- Emergency Decree No. 671, Official Gazette No: 29804. dated 17 August 2016, Retrieved from <https://www.resmigazete.gov.tr/eskiler/2016/08/20160817-18.htm>
- Emergency Decree No: 680, Official Gazette No: 29940. dated 6 January 2017, Retrieved from <http://www.resmigazete.gov.tr/eskiler/2017/01/20170106M1-2.htm>
- Ergun, F. D. (2018). *National security vs. online rights and freedoms in Turkey: Moving beyond the dichotomy*. Cyber Governance and Digital Democracy 2018/1, EDAM: The Centre for Economics and Foreign Policy Studies, Istanbul, Turkey, Retrieved from <http://edam.org.tr/en/national-security-vs-online-rights-and-freedoms-in-turkey-moving-beyond-the-dichotomy/>
- European commission for democracy through law. (2016, April 15). *Opinion no. 805/2015 on law on regulation of publications on the internet and combating crimes committed by means of such publications*. CDL-REF(2016)026, Strasbourg, Retrieved from [https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD\(2016\)011-e](https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)011-e)
- European Court of Human Rights (ECHR). (2013). *Case of ahmet yildirim v. . Turkey*, Strasbourg. Retrieved from <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-115705%22%5D%7D>
- Feick, J., & Werle, R. (2012). Regulation of cyberspace. In R. Baldwin, M. Cave, & M. Lodge (Eds.), *The Oxford handbook of regulation* (pp. 523–547). Oxford, UK: Oxford University Press.
- Finnemore, M., & Hollis, D. B. (2016). Constructing norms for global cybersecurity. *American Journal of International Law*, 110(3), 425–479. doi:10.1017/S000293000016894
- Freedom House. (2018). Turkey Internet Freedom. Retrieved from <https://freedomhouse.org/report/freedom-net/2018/turkey>
- G20. (2015, November 15-16). *Leaders' communiqué Antalya summit*. Retrieved from <http://g20.org.tr/g20-leaders-commenced-the-antalya-summit/>
- G20. (2016). *Digital economy development and cooperation initiative*. Hangzhou Summit, September 4th to 5th, Retrieved from <https://www.mofa.gov.jp/files/000185874.pdf>
- Goztepe, K., Kilic, R., & Kayaalp, A. (2014). *Cyber defense in depth: Designing cyber security agency organization for Turkey*. *Journal of Naval Science and Engineering*, 10, 1–24.
- Gurkaynak, G., Yilmaz, I., & Taskiran, N. P. (2014). Protecting the communication: Data protection and security measures under telecommunications regulations in the digital age. *Computer Law and Security Review*, 30, 179–189. doi:10.1016/j.clsr.2014.01.010
- Hathaway, M. E., & Klimburg, A. (2012). Preliminary considerations: On national cyber security. In A. Klimburg (Ed.), *National cyber security framework manual* (pp. 1–43). Tallinn, Estonia: NATO CCD COE Publication.
- HDN. (2015, January 1). *Top 10 comments by Erdoğan that made the headlines in 2014*. Retrieved from <http://www.hurriyetdailynews.com/top-10-comments-by-erdogan-that-made-the-headlines-in-2014-76312>
- HDN. (2018, February. 6). *Turkey's top media watchdog to regulate internet broadcasting, new draft bill foresees*. Retrieved from <http://www.hurriyetdailynews.com/turkeys-top-media-watchdog-to-regulate-internet-broadcasting-new-draft-bill-foresees-126897>
- HRW (Human Rights Watch). (2014 September 2). *Turkey: Internet freedom, rights in sharp decline*. Retrieved from <http://bit.ly/1r1kJOE>.
- IGF. (2014). *Connecting continents for enhanced multistakeholder internet governance (Istanbul, Turkey)*. Retrieved from <http://www.intgovforum.org/multilingual/content/igf-2014-4>
- ITU. (2014a). *Cyberwellness profile Turkey*. Retrieved from [https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country\\_Profiles/Turkey.pdf](https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Turkey.pdf)

- ITU. (2014b). International cyber shield exercise 2014, Istanbul, Turkey. Retrieved from [https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Turkey\\_cyberdrill\\_2014.aspx](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Turkey_cyberdrill_2014.aspx)
- Karabacak, B., Yildirim, S. O., & Baykal, N. (2016). Regulatory Approaches for Cyber Security of Critical Infrastructures: The case of Turkey. *Computer Law & Security Review*, 32, 526–539. doi: 10.1016/j.clsr.2016.02.005
- Kart, E. (2016, July 02). Turkey among initiators of significant UN resolution on Internet and human rights. Hurriyet Daily News. Retrieved from <http://www.hurriyetdailynews.com/turkey-among-initiators-of-significant-un-resolution-on-internet-and-human-rights-101162>
- Kerr, J. A. (2018). Information, security, and authoritarian stability: Internet policy diffusion and coordination in the former soviet region. *International Journal of Communication*, 12, 3814–3834. doi:10.1932/8036/20180005
- Kinikoglu, B. (2014). Evaluating the regulation of access to online content in Turkey in the context of freedom of speech. *Journal of International Commercial Law and Technology*, 9(1), 36–55.
- Kizilkoyun, F. (2018, June 15). *Anti-cybercrime department monitors 45 million social media users in Turkey*. Hurriyet Daily News. Retrieved from <http://www.hurriyetdailynews.com/anti-cybercrime-department-monitors-45-million-social-media-users-in-turkey-133362>
- Law No. 6518. (2014, February 6). Official Gazette no.28918. dated 19 February 2014. Retrieved from <https://www.resmigazete.gov.tr/eskiler/2014/02/20140219-1.htm>
- Law No. 6639. (2015, March 15). Retrieved from <https://www.resmigazete.gov.tr/eskiler/2015/04/20150415-1.htm>
- Law No: 6532. (2014, April 26). *On changing the law on the state's intelligence services and the national intelligence agency*. Official Gazette No. 28983.
- Lyon, D. (2015). The Snowden stakes: Challenges for understanding surveillance today. *Surveillance and Society*, 13(2), 139–152. doi:10.24908/ss.v13i2.5363
- Maréchal, N. (2017). Networked authoritarianism and the geopolitics of information: understanding Russian internet policy. *Media and Communication*, 5(1), 29–41. doi:10.17645/mac.v5i1.808
- McKune, S., & Ahmed, S. (2018). The contestation and shaping of cyber norms through China's internet sovereignty agenda. *International Journal of Communication*, 12, 3835–3855.
- Mueller, M. L. (2010). *Networks and states: The global politics of internet governance*. Cambridge, MA: MIT Press.
- Nocetti, J. (2015). Contest and conquest: Russia and global internet governance. *International Affairs*, 91, 111–130. doi:10.1111/1468-2346.12189
- Nye, J. S. (2014). *The regime complex for managing global cyber activities, global commission on internet governance paper series, 1*. Retrieved from <https://www.cigionline.org/publications/regime-complex-managing-global-cyber-activities>
- Pallin, C. V. (2017). Internet control through ownership: The case of Russia. *Post-Soviet Affairs*, 33(1): 16–33.
- Parsons, C. (2015). Beyond privacy: Articulating the broader harms of pervasive mass surveillance. *Media and Communication*, 3(3), 1–11. doi:10.17645/mac.v3i3.263
- Polat, B., Tokgöz, B. C., & Sayın, M. (2013). Hactivism in Turkey: The case of redhack. *Mediterranean Journal of Social Sciences*, 4. doi:10.5901/mjss.2013.v4n9p628
- Şafak, Y. (2016, December 12). *Emniyet Genel Müdürlüğü'nden Önemli Uyarı*. (Important Warning by the Turkish National Police). Retrieved from <https://www.yenisafak.com/teknoloji/emniyet-genel-mudurlugunden-onemli-uyari-2579166>
- Safshekan, O. (2017). Iran and the global politics of internet governance. *Journal of Cyber Policy*, 2, 266–284. doi:10.1080/23738871.2017.1360375
- Saka, E. (2018). Social media in Turkey as a space for political battles: AKTrolls and other politically motivated trolling. *Middle East Critique*, 27(2), 161–177. doi:10.1080/19436149.2018.1439271
- Seker, E., & Tolga, I. B. (2018). *National cyber security organisation: Turkey, the NATO CCDCOE national cyber security governance series*, Tallinn, Retrieved from [https://ccdcoe.org/uploads/2018/10/CS\\_organisation\\_TUR\\_112018\\_FINAL.pdf](https://ccdcoe.org/uploads/2018/10/CS_organisation_TUR_112018_FINAL.pdf)
- Sari, A. (2019). Turkish national cyber-firewall to mitigate countrywide cyber-attacks. *Computers and Electrical Engineering*, 73, 128–144. doi:http://dx.doi.org/10.1016/j.clsr.2016.02.005
- Senturk, H., Cil, Z. C., & Sagiroglu, S. (2012). Cyber security analysis of Turkey. *International Journal of Information Security Science*, 11(4), 112–125.
- The Council of Ministers. (2012, October 20). *Decision on the execution, management and coordination of national cyber security activities*. Oxford, UK: The Official Gazette no: 28447. Retrieved from <https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18.htm>
- The Ministry of Transportation, Maritime and Communication MTI. (2013, June 20). *The national cyber security strategy and 2013-2014 action plan*. The Official Gazette Nr. 28683, Retrieved from <https://www.uab.gov.tr/uploads/pages/siber-guvenlik/actionplan2013-2014.pdf>
- The Ministry of Transportation, Maritime and Communication (MTI). (2016). *2016–2019 national cyber security strategy*. Retrieved from <https://www.uab.gov.tr/uploads/pages/siber-guvenlik/ulusalsibereng.pdf>
- Twitter. (2019). *Transparency report*. Retrieved from <https://transparency.twitter.com/>
- UK. 2016. *National security strategy 2016–2021*. Retrieved from <https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021>
- United States. 2008. *National security presidential directive 54/homeland security presidential directive 23 (NSPD-54/HSPD-23)*. Retrieved from <https://fas.org/irp/offdocs/nspd/nspd-54.pdf>
- United States Department of State (2010, March 11). *Country Reports on Human Rights Practices 2009, Turkey*, <http://www.state.gov/j/drl/rls/hrrpt/2009/eur/136062.htm>
- United States Joint Publication 3-12, Cyberspace Operations. (2018). [https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3\\_12.pdf](https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf)
- United States National Security Council. (2010). *Cyberspace policy review: Securing America's digital future*. *Cosimo, Incorporated*.
- We Are Social. (2019, May 18). *Digital in 2019: Global internet use accelerates*. Retrieved from <https://wearesocial.com/global-digital-report-2019>
- World Economic Forum (WEF). 2019. *The global risks report 2019*. Geneva, Switzerland. Retrieved from [http://www3.weforum.org/docs/WEF\\_Global\\_Risks\\_Report\\_2019.pdf](http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf)

Yesil, B., & Sozeri, E. K. (2017). Online surveillance in Turkey: Legislation, technology and citizen involvement. *Surveillance and Society*, 15(3/4), 543–549. doi:10.24908/ss.v15i3/4.6637

Yesil, B., Sozeri, E. K., & Khazraee, E. 2017. *Turkey's internet policy after the coup attempt: The emergence of a distributed network of online suppression and*

*surveillance*. An Internet Policy Observatory Publication. Retrieved from [http://globalnetpolicy.org/wp-content/uploads/2017/02/Turkey1\\_v6-1.pdf](http://globalnetpolicy.org/wp-content/uploads/2017/02/Turkey1_v6-1.pdf)

Zhang, L., & Chen, S. (2019). China's digital economy: Opportunities and risks, *IMF Working Paper*, WP/19/16. doi: 10.5089/9781484389706.001