SECURITIZING THE INTERNET: THE CASE OF TURKEY

Helin Alagöz Gessler[1]

Abstract
The rapid digital development in the last two decades has brought the cyberspace to national security agenda in Turkey as one of the significant challenges of the 21st century. Increasing regulation of the Internet and, in particular, online social networks by the state through digital controls and surveillance is being justified addressing the maelstrom of potential cyber threats. Nonetheless, increasing control of cyberspace contrasts with the commitment to the protection of the individual rights and liberties. This paper maps the Internet freedom in Turkey and asks to what extent Turkey is able to strike a balance between providing the security in cyberspace and protecting the Internet freedom in the country.

In order to analyze how digitization and the Internet have developed into a security issue in Turkey, the paper builds on the theoretical framework of securitization formulated by the Copenhagen School, which deals with the construction of the image of security threats. The paper argues that the perception of networked nature of cyberspace to create dissidence which may result in the destruction of state authority leads to hyper-securitization while neglecting the freedom of expression as well as freedom to access information.

The paper follows the methodology of qualitative case study mainly based on document analysis, assessment of the official internet regulations and media analysis.

1. Introduction

The rapid digital development in the last two decades has brought the cyberspace to national security agendas of many states as a significant challenge of the 21st century. Turkey was one of those states, which took quick action against the potential threats of the Internet, particularly through the legislation and amendments of the Law No. 5651 which regulates the Internet use. However, the law caused a lot of debates in terms of the Internet freedom. In 2016, in line with concerns about Turkey's Internet policy often expressed in national and international media, Freedom House has changed the Internet freedom status of Turkey from "partly free" to "not free".

This paper discusses the Turkish Internet policy and describes the current situation of the Internet in the country from the perspective of security studies. It argues that the perception of networked nature of cyberspace to create dissidence which may result in the destruction of state authority leads to hyper-securitization while neglecting the freedom of expression as well as freedom to access information.

The paper proposes an analytical approach that conceptualizes the Turkish Internet policy as a field of national security, which emerges through a discursive process of securitization. By combining

[1] Business and Information Technology School Berlin, Dessauerstr. 3-5, 10963 Berlin, helingessler@gmail.com

the Securitization Theory and the Internet, the paper highlights the performative function of discourses in the field.

Drawing on document analysis, the paper examines the facts stated in the annual Turkey reports of Freedom House about the Internet freedom between 2011 and 2016 in the light of the Securitization Theory.

2. Theoretical Background

2.1 The Copenhagen School and the Securitization Theory

In its simplest form, security refers to the safety of an entity. Over the last decades, security studies have to deal with two main problems. The first problem was the subject matter of security. Which entity should be prioritized to be secured? The state, individual or another unit? The second problem was the nature of threats that face us. From a realist perspective, the states were the referent objects and the military force was the nature of the threat. This view was commonly accepted, in particular, during the Cold War period. [17] Towards the end of the Cold War, due to changing geopolitical conditions, the traditional security approach started to be challenged as various new security threats of multiple referent objects appeared leading to the emergence of new theoretical approaches to security.

Barry Buzan, one of the central figures of the Copenhagen School of Security Studies, was the first who suggested to redefine the existing security concept. In his "People, States and Fear" (1983), he criticized the narrow focus of the traditional security concept and emphasized on the need for the reconceptualization of national security to address non-military threats to the global environment. He pointed out that security of potential referents might rely on the factors operating in military, political, economic, societal or environmental sectors; whereas traditional security approach solely referred to the military sector. [23] In the post-Cold War era, Buzan's view gained more ground when changing security concerns encouraged scholars to seek for alternative security theories.

Although Buzan can be considered as neo-realist concerning his reference to the anarchic structure of the international system [2], his writings contributed to the emergence of critical security theories based on Constructivism. Those criticized Buzan's analysis in 'People, States and Fear' for "privileging state" as the key referent object despite "extending security beyond the state". [17] Constructivists mainly differed from the traditionalist security scholars in seeing a two-way relationship between individuals and the social world. They stressed on the significance of the notion of identity as well as culture, norms and values in the process of specifying threats to national security since those have an impact on state interests.

However, in his subsequent works with his colleagues, Buzan also approached to the constructivist view of security by moving from the state to the society as the referent object and focusing on the concept of national identity and culture in 'Identity, Migration and the New Security Agenda in Europe' (1993) and in 'Security: A New Framework for Analysis' (1998) [24].

One of the main concerns of the Copenhagen School was the "process" of making a state policy, which was the point of departure for Ole Wæver, a colleague of Buzan, who introduced the notion of "Securitization". In this regard, states might resort to securitization to fight against a new threat. In the process of securitization, states need to create a discourse that would legitimize their actions to eliminate the perceived threat. Wæver defined security as the outcome of a "speech act".

Accordingly, Securitization is the discursive process which defines an issue as an existential threat, in other words, a security problem. He highlighted that Securitization only takes place when the elites identify an issue as a security problem and the public accept it [25]. To put another way, securitization was a function of social construction that requires legitimization of the issue concerned as a security issue. Thus, one might assume that an issue, which was formerly in the domain of low politics can be transferred to high politics through the process of securitization.

2.2 Extending the Realm of Securitization to Cybersecurity

The security of the Internet and the cyberspace were not counted by the Copenhagen School among the sectors, where securitization might take place. For Buzan, Wæver and de Wilde, Pentagon's reference to hackers in 1996 as "a catastrophic threat" and "a serious threat to national security" was not sufficient to talk about a cybersecuritization since it had "no cascading effects on other issues" [4]. Nevertheless, by the time the Copenhagen School made this assumption, the concept of cyber security was not voiced as frequently as today and it was not yet included in the national security agendas of many countries. The formation and evolution of cyber security discourse in response to growing significance of the role of the Internet in our daily lives brought about the need for understanding cyber security as a discursive modality.

The first attempt to add cyber security sector to the existing framework of securitization theory was made by Hansen and Nissenbaum in *Digital Disaster, Cyber Security, and the Copenhagen School*, where they employed the Securitization Theory to examine the distributed denial of service attacks (DDoS) on a series of government agencies, the news media and the two largest banks in Estonia in 2007. They theorized the cyber security "as a distinct sector with a particular constellation of threats and referent objects" [14].

Hansen and Nissenbaum argued that the political importance of ''network security'' and ''individual security'' stems from connections to the collective referent objects of ''the state,'' ''society,'' ''the nation,'' and ''the economy.'' These referent objects are articulated as threatened through *hypersecuritization*, everyday security practices, and *technifications*, which are three distinct forms of securitizations. They also stressed that the Estonian government achieved at least a partially successful *cybersecuritization* since it created a discourse which aimed to show those attacks especially to the international audience as ''the first war in cyberspace'' by coupling of ''network'' to ''state'' and ''society'' and highlighting that they were threatening the individual security [14].

In this context, two distinct cybersecurity perspectives may affect the process of *cybersecuritization* depending on the perception of "what needs to be secured". From the perspective of mainstream privacy research the online freedom of the individual citizens constitutes the focal point; whereas from the perspective of the state the protection of critical infrastructure is much more significant as it provides citizens with the services which enable them access the Internet.

3. Securitization of the Internet in Turkey

3.1 Reading the Reports of Freedom House on Turkey's Internet Freedom

The facts about Turkey's cyber circumstances are summarized in the Internet freedom reports of the Freedom House, which is an independent watchdog organization based in the United States.

Covering the key developments in Turkey those annual reports provide us with adequate source of data to study the securitization rhetoric on Turkish case.
The reports evaluate the level of Internet freedom in a country by looking at the scores of that country in three main fields which are divided into subcategories shown in Figure 3.1. Accordingly, 0 point equals to "most free" and 100 points equal to "least free".

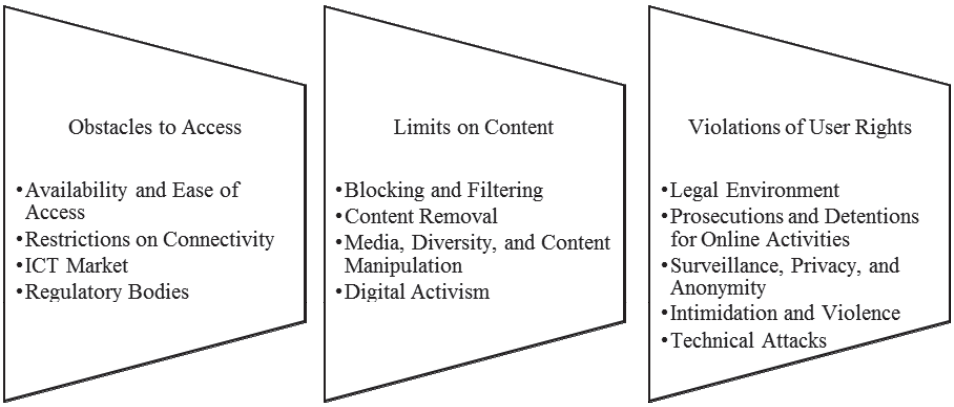

Figure 3.1: The Fields of Internet Freedom

Table 3.1 shows that Turkey has been following a negative trend in all of those categories over the past five years. The situation regarding the Internet freedom even exacerbated in 2016.

	2011	2012	2013	2014	2015	2016
Obstacles to Access (0-25)	12	12	12	14	13	13
Limits on Content (0-35)	16	17	18	18	20	21
Violations of User Rights (0-40)	17	17	19	23	25	27
Total (0-100) 0=most free, 100=least free	45	46	49	55	58	61
Internet Freedom Status	Partly free	Partly free	Partly free	Partly free	Partly free	Not free

Table 3.1: Internet Freedom Status in Turkey, 2011-2016
Sources: [8] [9] [10] [11] [12] [13]

As seen in Table 3.2, the reports between 2011 and 2016 confirmed the steady growth of the Internet penetration in Turkey, which is directly proportional to the population growth. The increasing Internet penetration was mainly through mobile broadband. From 2009 till 2016 all Turkish mobile phone operators offered 3G (third-generation) data connections. Three companies have begun to offer 4.5G[2] services as of April 2016.

[2] It was initially planned for 4G technology, however after President Erdogan's insistence on moving directly to 5G, it was changed to 4.5G.

	2011	2012	2013	2014	2015	2016
Population	73,6 million	75 million	74,9 million	76,1 million	77,2 million	78,7 million
Internet Penetration	36 %	42 %	45 %	46 %	51 %	54 %

Table 3.2: Population vs. Internet Penetration in Turkey, 2011-2016
Sources: [8] [9] [10] [11] [12] [13]

That being said, there is still the problem of digital divide in the country. Many users connected the Internet at their workplace, universities etc. since they had no Internet access at home (In 2016 % 61 of the Turkish population were Internet users and % 76 of the Turkish households had Internet access [22]). The factors such as high prices (in comparison with the minimum wage) and lack of technical literacy are counted among the main causes of the digital divide between the poor and rich or senior and young people. The 2016 Report underlines the telecommunications networks shutdowns during security operations, particularly in southeastern cities as the most significant obstacle to the Internet access increasing the digital divide between the region and the rest of the country [13].

The reports make serious criticisms of the limits on content. There is an immense increase (from 43,785 to 111,011) in the number of blocked websites due to civil code–related complaints and intellectual-property rights violations in the last three years [13]. They argue that most of those sites were blocked for political or social reasons including "news outlets or online communities that report on LGBTI (lesbian, gay, bisexual, transgender, and intersex) issues, ethnic minorities, specifically pro-Kurdish content, anti-Muslim content, or social unrest". All reports underscore an increasing government censorship of the Internet and social media blocking. Social media platforms such as Twitter, Facebook, and YouTube were several times blocked due to certain posts or accounts typically after terrorist attacks.[3] The reports point out that the blocking orders tend to coincide with important political events, such as an election, intelligence leak, hostage crisis, or corruption scandal, military operations, terrorist attacks [11]. The 2016 Report states:

> Prompted by a series of deadly terrorist attacks, the government repeatedly blocked or throttled social media platforms in a bid to halt the dissemination of images and videos surrounding the events. In addition, scores of news sites and Twitter accounts were blocked or removed, particularly those covering the conflict with Kurdish militants. Journalists, scholars, and public figures that are critical of the government faced coordinated harassment by progovernment trolls on Twitter [13].

The main legal reference for the blocking and removal of online content in Turkey is the Law No. 5651 (entitled "Regulation of Publications on the Internet and Suppression of Crimes Committed by Means of Such Publication") or so-called "Internet Law" enacted in 2007. It initially aimed at the protection of children from illegal and harmful Internet content such as material related to sexual abuse, drug use, provision of dangerous substances, prostitution, obscenity, gambling, suicide promotion, and prevention of crimes against Atatürk [19]. The law was applied through the Telecommunication and Communication Presidency (TİB), which was overseen by the main regulatory body for the ICTs in Turkey entitled the "Information and Communications Authority (BTK)". The TİB was shut down in August 2016 due to allegations of being masterminded by the Fetullahist Terrorist Organization (FETÖ) passing its authority to the BTK [16]. The BTK is currently the only responsible institution for the regulation of the policies made by the Ministry of

[3] The Freedom on the Net 2016 Report states: "Turkey accounted for almost 90 percent of all content that was locally restricted by Twitter in the second half of 2015. Turkey's regulator fined the company TRY 150,000 (US$ 51,000) for refusing to remove what it termed "terrorist propaganda".

Transportation, Maritime Affairs, and Communications. Having board members appointed by the government the BTK is criticized for a lack of transparency and a lack of independence from the executive [13].

Nonetheless, the Law No. 5651 has gone through amendments in February 2014 and March 2015 broadening the scope for censorship [26]. The law also outlined the responsibilities of content providers, hosting companies, public access providers, and ISPs reserving the right to take down domestically hosted websites and block or filter the websites based abroad through ISPs in case of proscribed content. The February 2014 amendments extended it from notice-based liability to include URL-based blocking orders to be issued by a criminal court judge and assigned the TİB with "broad discretion to block content that an individual or other legal claimant perceives as a violation of privacy, while failing to establish strong checks and balances". The March 2015 amendments made it possible for cabinet ministers to ask the TİB to block content when they consider that the content violates "the right to life, secure property, ensure national security and public order, prevent crime, or protect public health." In this case, the TİB has to follow the orders within four hours and inform the criminal court about it within 24 hours. The blocking must be rescinded unless a judge validates the decision within 48 hours [15].

Another field examined by the reports is the "Violations of User Rights". In this field, there is a particular emphasis on arrests and prosecutions for social media posts, which, in some cases, ended up with lengthy prison sentences for "insulting" public officials or spreading "terrorism propaganda". The reports highlight the government surveillance, the bulk retention of user data, and limitations on encryption and anonymity as key issues. In this context, the Law No, 5651 is criticized again since it binds the hosting and access providers to retain all traffic information for one year and maintain the accuracy, integrity and confidentiality of the data. A similarly controversial issue is the Law No. 6532 on Turkey's National Intelligence Organization (MIT), which grants intelligence agents "unfettered access to communications data without a court order". It is criticized for limiting the accountability of wrongdoing [13].

In the meantime, the reports stress on a lack of sufficient cybersecurity measures, put it differently, a security gap with the example of a 14-day cyberattack in December 2015 bringing approximately 400,000 websites offline and temporarily suspending retail banking services and upload of personal data such as identity numbers and addresses of almost 50 million Turkish citizens onto a website titled the "Turkish Citizenship Database" in a massive data leak in March 2016 [13].

3.2 Back to Securitization Discussion

As discussed in the first part of the paper, there are three crucial elements of a securitization process portrayed by the Copenhagen School. First, there must be an existential (even when it is not in reality) threat identified by a referent object. Second, the referent object must establish the need for action in order to eliminate the threat. Third, the rules governing the relationship between the referent object and the threat under normal conditions must be rejected [17]. Taking Turkish government as the referent object, the Internet as the sector of identified threat and the manner the government deals with the threat, the picture presented by the Internet Freedom reports puts forward the presence of a *cybersecuritization* in Turkey over the past years.

In parallel to the increase in the Internet penetration, there is a considerable increase in the telecommunications networks shutdowns, blockings and removal of political content of the social media as well as the number of arrested ICT users and other limits on online communication

activity. The government legitimizes its heavily criticized Internet policy with a discourse, which justifies the restrictions to online freedom of expression with the protection of national security. Moreover, increasing terror attacks following the 2015 general elections and the social polarization facilitate the *cybersecuritization* by creating a public perception of online threats to the national security and the need for resolving those threats.

Today, it is possible to argue that there is a securitization of the Internet overall in the world since our daily "real world" crimes moved online, making Turkey not an exception to this. Admitting the growing importance of cybersecurity due to cyber crimes which brings about a global tendency towards *cybersecuritization*, it can be argued that Turkey stands out with its strict Internet policy as an example of *hypersecuritization*. The term was introduced by Buzan to describe a situation of over-securitization by defining "a tendency both to exaggerate threats and to resort to excessive countermeasures". Buzan suggests to check the existence of "real threats" that are not exaggerated in order to identify the "exaggerated threats" [3]. Hansen and Nissenbaum distinguish *hypersecuritizations* from securitization by the former's instantaneity and interlocking effects [14].

As Freedom House reported in detail, blocking orders as well as arrestments tend to coincide with important political events in Turkey such as an election, intelligence leak, hostage crisis, corruption scandal or terror attacks and military operations. This brings Turkey's *cybersecuritization* into question as it enables the state not only to fight against cyber crimes but also to suppress the dissident individuals or social groups by cutting off their communication. Although the freedom of expression is explicitly protected by the Article 26 of the Turkish constitution[4] and no law "specifically criminalizes online activities like posting one's opinions, downloading information, sending email, or transmitting text messages, many provisions of the criminal code" such as the Article 125 and 255[5] and "other laws, such as the Anti-Terrorism Law, are applied to both online and offline activity" [13]. The broad terrorism definition of the Anti-Terror Law has been widely criticized for being abused by courts to prosecute critical journalists and academics.[6] In this context, Turkeys securitization of the Internet meets the criteria for a *hypersecuritization*.

4. Conclusion

Throughout this paper the Securitization Theory, its implications for cyberspace and the Turkish case of *cybersecuritization* were examined. An overview of the Internet freedom status of Turkey was given and it is described as an example of *hypersecuritization* of the cyberspace.

It is essential that the state takes measures for the sustainability of a secure cyber environment so that daily online practices can function seamlessly. However, the question of where and when the state should intervene the online user rights remains controversial, particularly in times of political instability.

---

[4] The Article 26 of the Turkish constitution states that "everyone has the right to express and disseminate his thought and opinion by speech, in writing or in pictures or through other media, individually or collectively." See Constitution of the Republic of Turkey, p. 12 [6].

[5] The Article 125 of the Turkish criminal code, "anyone who undermines the honor, dignity or respectability of another person or who attacks a person's honor by attributing to them a concrete act or a fact, or by means of an insult shall be sentenced to imprisonment for a term of three months to two years, or punished with a judicial fine." According to the Article 299 of the Turkish criminal code "Defaming a public official carries a minimum one year sentence, while insults to the president entails a sentence of one to four years" [21].

6 Article 7 of the Anti-Terror Law states that "those who make propaganda of a terrorist organization by legitimizing, glorifying or inciting violent methods or threats are liable to prison terms of one to five years…" [20].

In this regard, the developments in the last five years concerning the obstacles to access, limits on content and violations of user rights indicate that Turkey's *hypersecuritization* of the cyberspace imperils the Internet freedom. One should therefore consider whether a process of *desecuritization*, in other words, "the move out of a logic of security and into a political or a technical one" [14] can help improve the e-democracy in the country.

A new Data Protection Law enacted on 7 April 2016, which aligns Turkey's legislation with EU standards is encouraging since it can be used as an initiative for the *desecuritization* of the Internet in Turkey. In the upcoming years, it will be possible to analyze its impact on the Internet freedom of the country.

5. References

[1] BUZAN, B.: People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era, 2nd Edition, London: Harvester Wheatsheaf, 1983.

[2] BUZAN, B.: People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era, London: Harvester Wheatsheaf, 1991, p. 21.

[3] BUZAN, B.: The United States and the Great Powers: World Politics in the Twenty-First Century, Cambridge: Polity, 2004, p. 172.

[4] BUZAN, B., WÆVER, O. and DE WILDE, J.: Security. A New Framework for Analysis, Colorado: Lynne Rienner Publishers, 1998.

[5] COLEMAN, S. and BLUMLER, J. G.: The Internet and Democratic Citizenship, New York: Cambridge University Press, 2009.

[6] Constitution of the Republic of Turkey, available at https://global.tbmm.gov.tr/docs/constitution_en.pdf, [accessed 18 January 2017].

[7] DEGIRMENCI, N.: Turkey's First Comprehensive Data Protection Law Comes into Force, Inside Privacy, 8 April 2016, available at https://www.insideprivacy.com/data-security/turkeys-first-comprehensive-data-protection-law-comes-into-force/, [accessed 21 January 2017].

[8] Freedom House, Freedom on the Net 2011, available at https://freedomhouse.org/report/freedom-net/2011/turkey, [accessed 16 November 2016].

[9] Freedom House, Freedom on the Net 2012, available at https://freedomhouse.org/report/freedom-net/2012/turkey, [accessed 16 November 2016].

[10] Freedom House, Freedom on the Net 2013, available at https://freedomhouse.org/report/freedom-net/2013/turkey, [accessed 16 November 2016].

[11] Freedom House, Freedom on the Net 2014, available at https://freedomhouse.org/report/freedom-net/2014/turkey, [accessed 16 November 2016].

[12] Freedom House, Freedom on the Net 2015, available at https://freedomhouse.org/report/freedom-net/2015/turkey, [accessed 16 November 2016].

[13] Freedom House, Freedom on the Net 2016, available at https://freedomhouse.org/report/freedom-net/2016/turkey, [accessed 16 November 2016].

[14] HANSEN, L. and NISSENBAUM, H.: Digital Disaster, Cyber Security, and the Copenhagen School, International Studies Quarterly, No. 53, 2009, p. 1155-1175.

[15] Hurriyet Daily News, Approved article gives Turkish gov't power to shut down websites in four hours, 20 March 2015, available at http://bit.ly/1C3iuA8, [accessed 14 January 2017].

[16] Hurriyet Daily News, Turkey shuts down telecommunication body amid post-coup attempt measures, 17 August 2016, available at http://www.hurriyetdailynews.com/turkey-shuts-down-telecommunication-body-amid-post-coup-attempt-measures.aspx?pageID=238&nID=102936&NewsCatID=338, [accessed 14 January 2017].

[17] MALIK, S.: Framing a Discipline in HOUGH, P.; MALİK, S.; MORAN, A. and PİLBEAM, B. (Eds), International Security Studies. Theory and Practice, Cornwall: Routledge, 2015, p. 4.

[18] MATHEWS, J.: Redefining Security, Foreign Affairs, Vol. 68, No. 2, Spring 1989, pp. 162-177.

[19] Resmi Gazete (Official Gazette), Internet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (Regulating Broadcasting in the Internet and Fighting Against Crimes Committed through Internet Broadcasting), No. 26530, 23 May 2007, available at, http://www.resmigazete.gov.tr/eskiler/2007/05/20070523-1.htm, [accessed 2 November 2016].

[20] Terörle Mücadele Kanunu (Anti-Terror Law), available at http://www.mevzuat.gov.tr/MevzuatMetin/1.5.3713.pdf, [accessed 12 January 2017].

[21] Türk Ceza Kanunu (Turkish Criminal Code), available at http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf, [accessed 12 January 2017].

[22] Türkiye İstatistik Kurumu (Turkish Statistical Institute), "Household Usage of Information Technologies Survey of Turkish Statistical Institute, 2016," 18 August 2016, available at http://www.tuik.gov.tr/PreHaberBultenleri.do?id=21779, [accessed 2 February 2017].

[23] ULLMAN, R., Redefining Security, International Security, Vol. 8, No. 1, Summer 1983, pp. 129-153.

[24] WÆVER, O., BUZAN, B., KELSTRUP, M. and LEMAITRE, P. et al.: Identity, Migration and the New Security Agenda in Europe, London: Pinter Publishers Ltd., 1993.

[25] WÆVER, O.: Securitization and Desecuritization in Lipschutz, R. (ed.), On Security, New York: Columbia University Press, 1998, p. 24.

[26] World Intellectual Property Organization, Law No.5651 on Regulating Broadcasting in the Internet and Fighting Against Crimes Committed through Internet Broadcasting,, available at, http://www.wipo.int/wipolex/en/details.jsp?id=11035, [accessed 11 November 2016].