2-28-2017

Turkey's Internet Policy After the Coup Attempt: The Emergence of a Distributed Network of Online Suppression and Surveillance

Bilge Yesil

Efe Kerem Sözeri

Emad Khazraee

Turkey's Internet Policy After the Coup Attempt: The Emergence of a Distributed Network of Online Suppression and Surveillance

Abstract
In July 2016, Turkey was shaken by a bloody coup attempt. Although the would-be putschists failed, their insurgency led to an unprecedented reshuffling of Turkey's political economic and socio-cultural landscapes. Notwithstanding the critical reverberations on the army, judiciary, law enforcement and civil society, the abortive coup set in motion a massive purge of civil servants, closure of media outlets, arrests of journalists, and blocking of websites and social media accounts.

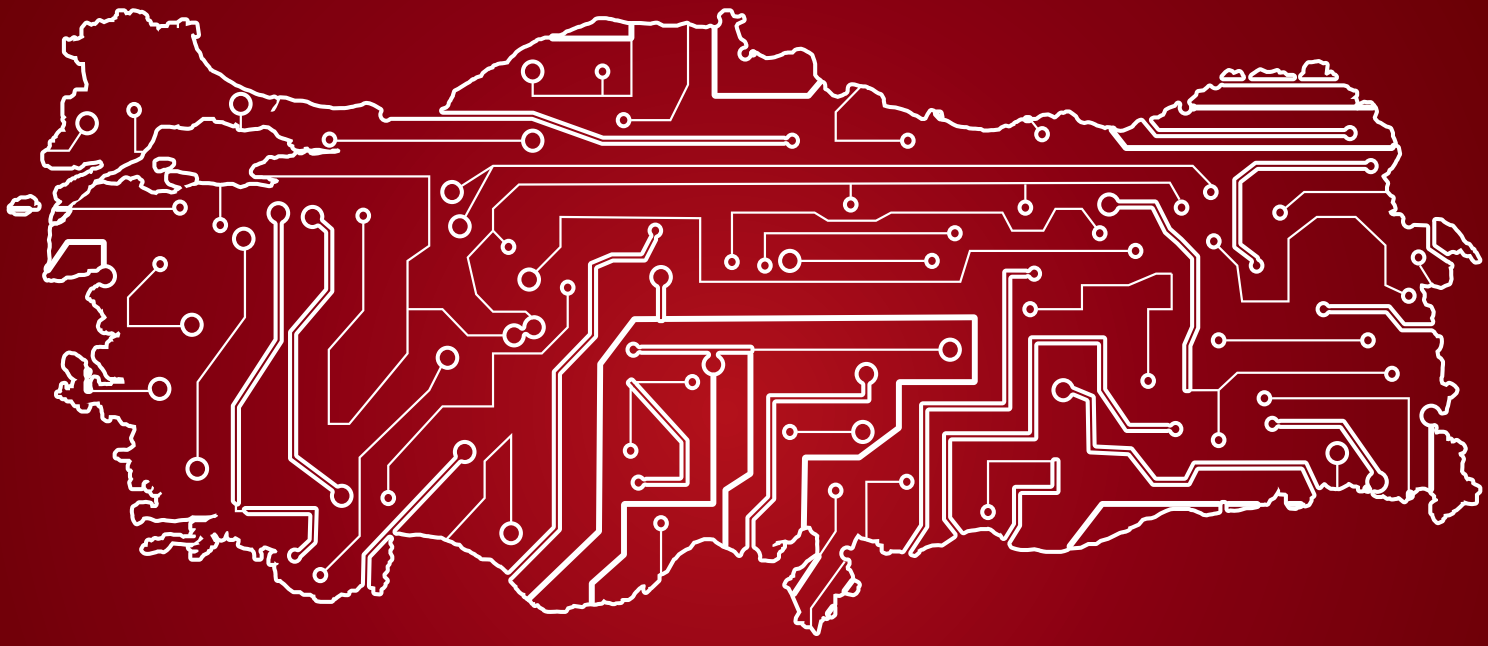
This report offers an examination of the evolution of internet policy in Turkey from the early 2000s to the post-coup conjuncture. It begins with an overview of internet legislation in Turkey during the 2000s under the AKP government (Justice and Development Party), and proceeds to discuss the deployment of different forms of control between 2013-2016 to contain the fallout from political and security crises and the potentially disruptive affordances of social media platforms. The report then focuses on the emerging policy developments and online restrictions in the aftermath of the coup attempt, which include 1) the closure of the TIB—Turkey's telecommunications authority, 2) direct government control of ISPs (Internet Service Providers) and interception of digital communications by way of decree laws, 3) facilitation of social media censorship by means of Twitter, Facebook and YouTube content removals and 4) coordinated online harassment campaigns by pro-government users against alleged coup planners, Kurdish activists and government critics in general.

Keywords
turkey, internet, censorship, coup, internet governance

Disciplines
Communication Technology and New Media | International and Intercultural Communication | Social Influence and Political Communication | Social Media

Turkey's Internet Policy after the Coup Attempt:

The Emergence of a Distributed Network of Online Suppression and Surveillance



An Internet Policy Observatory Publication

Bilge Yesil, Efe Kerem Sozeri
and Emad Khazraee

INTERNET POLICY OBSERVATORY

Annenberg SCHOOL FOR COMMUNICATION UNIVERSITY of PENNSYLVANIA

About the Authors

Bilge Yesil is an Associate Professor of Media Culture at the City University of New York, College of Staten Island. She is the author of Video Surveillance: Power and Privacy in Everyday Life (2009) and Media in New Turkey: The Origins of an Authoritarian Neoliberal State (2016).

Efe Kerem Sözeri is a PhD candidate at Vrije Universiteit Amsterdam and is writing his dissertation on Turkish migrants' political behaviors in Europe and Turkey. He received his MA degree from the same institution where he completed his thesis with a two-year scholarship. In addition to his academic work, Efe writes about press freedoms and censorship for the Daily Dot, Vocativ, and Global Voices in English; P24 and Bianet in Turkish, and TAZ in German.

Emad Khazraee is an assistant professor in the college of communication and information sciences at Kent State University. His research is formed around the interplay between social and technical phenomena. Currently, he is studying the relationship between digital technologies, new media, and social change.

The Internet Policy Observatory (IPO) is a project at the Annenberg School for Communication at the University of Pennsylvania. The overarching goal of the program is to deepen the reservoir of researchers and advocates in regions where Internet freedom is threatened or curtailed and to support the production of innovative, high-quality, and impactful internet policy research. The IPO facilitates collaboration between research and advocacy communities, builds research mentorships between emerging and established scholars, and engages in trainings to build capacity for more impactful digital rights research and advocacy.

For more information on the IPO, please visit globalnetpolicy.org.

The authors would like to thank Dr. Yaman Akdeniz and anonymous activists and researchers for sharing their insights and Laura Schwarz-Henderson for her guidance and support during the research and writing of this report.

Annenberg School for Communication
University of Pennsylvania
3620 Walnut St.
Philadelphia, PA 19104
www.asc.upenn.edu
215-898-7041

Contents

Introduction

In July 2016, Turkey was shaken by a bloody coup attempt. Although the would-be putschists failed, their insurgency led to an unprecedented reshuffling of Turkey's political economic and socio-cultural landscapes. Notwithstanding the critical reverberations on the army, judiciary, law enforcement and civil society, the abortive coup set in motion a massive purge of civil servants, closure of media outlets, arrests of journalists, and blocking of websites and social media accounts.

This report offers an examination of the evolution of internet policy in Turkey from the early 2000s to the post-coup conjuncture. It begins with an overview of internet legislation in Turkey during the 2000s under the AKP government (Justice and Development Party), and proceeds to discuss the deployment of different forms of control between 2013-2016 to contain the fallout from political and security crises and the potentially disruptive affordances of social media platforms.[1] Following this overview, the report focuses on the emerging policy developments and online restrictions in the aftermath of the coup attempt, which include 1) the closure of the TIB—Turkey's telecommunications authority, 2) direct government control of ISPs (Internet Service Providers) and interception of digital communications by way of decree laws, 3) facilitation of social media censorship by means of Twitter, Facebook and YouTube content removals and 4) coordinated online harassment campaigns by pro-government users against alleged coup planners, Kurdish activists and government critics in general.

To gain insights into these developments, this report draws extensively on literature both in Turkish and English and is based on the following methods: 1) document analysis of existing internet legislation, Turkish Official Gazette announcements concerning the decree laws, and government officials' statements, 2) quantitative analysis of open source data on social media censorship (crowdsourced data on banned websites; Twitter, Facebook and Google transparency reports; Lumen database on Turkish court orders; traffic data on throttling), 3) analysis of Twitter activity in the months before and after the coup attempt, and 4) select semi-structured interviews with internet activists and legal scholars.

The key finding of the report is that the AKP's post-coup strategies concerning the internet are culminating in a distributed network of government and non-government actors using hard and soft forms of control. While the AKP continues to deploy existing Internet Law, Anti-Terror Law and Press Law provisions and further expands its online hegemony by way of decree laws, its post-coup internet policy has also come to rely on the opaque activities of users and groups who are affiliated with government officials, party members and partisan media outlets and whose primary objective is to target and harass government critics on social media, and intimidate those who dissent. As these actors take on the responsibility of online monitoring, hacking and "snitching," it becomes increasingly difficult for users and activists to trace online restrictions to a specific government agency or legislation and to seek legal remedies.

[1] R. Deibert and R. Rohozinski, 'Control and Subversion in Russian Cyberspace' In *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, edited by R. Deibert, J. Palfrey, R. Rohozinski and J. Zittrain, Cambridge, MA: MIT Press, 2010, pp. 15-34.

Overview of Turkey's Internet Policy

I. 1993-2007: Absence of regulation

In the early 1990s, internet in Turkey was in the purview of academic and research institutions. Following the creation of a national backbone in 1996 and the consequent rise of a competitive ISP market, internet became a commercial medium in the latter half of the decade, registering steady growth in use and introducing various technological and socio-cultural changes. However, it remained largely unregulated primarily because of the then-coalition governments' disregard for the need to develop new policies for a new medium, and was primarily managed and controlled by the courts that focused on criminalization of certain online activities. The earliest examples of such court decisions can be traced back to separate cases in 1997 and 2001 when two individuals were prosecuted for their statements on online forums that allegedly criticized and offended the Turkish police and state institutions.[2]

On the other hand, the first website blocking took place in 2002 when a military court ordered a website to shut down due to the publication of documents concerning alleged corruption within the Turkish Air Force.[3] The first mass website blocking happened in 2005-2006 when more than a dozen websites were blocked by the courts on copyright infringement grounds because they provided hyperlinks to downloadable audio files or software to obtain such files.[4] These practices of ad hoc criminalization and prosecution in the late 1990s and early 2000s, and the absence of a systematic policy-making and public debate concerning the role of the internet in society set the stage for more stringent policies in following years.

II. 2007-2013: Regulation-cum-control

Turkey passed its first internet-specific legislation in 2007, which was titled "Law No. 5651, Regulation of Publications on the Internet and Suppression of Crimes Committed by means of Such Publications." It was propelled by fears around moral issues involving teen sexuality, pornography, drug use, video games and violence that swept the nation in the early 2000s, and was therefore designed to protect users from so-called illegal and harmful content. The "Internet Law" as it was commonly known, charged the Presidency of Telecommunications and Communication (TIB in its Turkish acronym) with administrative duties such as monitoring content and mandating hosting and access providers to combat categorical crimes. The law set forth 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 Ataturk—the founder of modern Turkey), and stipulated that a website could be blocked by court order or an administrative order issued by the TIB if it was found to be committing one of these crimes. It also obliged hosting and access providers to monitor online content that was transmitted through their infrastructure and required them to ban access to illegal content once they were served with a court order or a TIB-issued notice. According to the Internet Law, mass use providers (e.g. internet cafes) were required to obtain "activity certificates" from local authorities and to block access to illegal content by using the TIB-approved filters.

To penalize online content that fell outside the purview of the Internet Law, Turkish authorities deployed other legislation including the Penal Code to criminalize online speech that insults the Turkish nation, government agencies or the military; the Anti-Terror Law to curb political speech regarding the Kurdish issue and ethnic minority rights; and the Intellectual Property Law to penalize content providers for illegally publishing copyrighted material.

Given the combined use of the Internet Law with the above-mentioned legislation, the late

[2] K. Altintas, T. Aydin and V. Akman, 'Censoring the Internet: The Situation in Turkey', First Monday, June 3, 2002, http://firstmonday.org/ojs/index.php/fm/article/view/962/883, (accessed November 27, 2016).

[3] S. Özalp, 'Genel Kurmay Yolsuzluk.com Sitesini Kapattırdı', Türk İnternet, March 4, 2002. Accessed November 25, 2016 http://www.turk-internet.com/portal/yazigoster.php?yaziid=3352, (accessed November 27, 2016).

[4] M. Akgül and M. Kırlıdoğ, 'Internet censorship in Turkey', Internet Policy Review, Volume 4, Issue 2, DOI: 10.14763/2015.2.366, https://policyreview.info/articles/analysis/internet-censorship-turkey, (accessed November 27, 2016).

Table 1: Number of websites blocked in Turkey

Year	Annual	Cumulative
2008	1,310	1,310
2009	4,644	5,954
2010	2,593	8,547
2011	7,012	15,559
2012	7,082	22,641
2013	17,837	40,478
2014	25,061	65,539
2015	42,236	107,775
2016	8,030	115,805

2000s witnessed the construction of an extensive mechanism of control. Based on the above-mentioned political, social and cultural anxieties, the number of blocked websites grew exponentially, with 93 percent of them blocked by TIB's administrative orders.[5]

These 93% of blocked websites mentioned above were banned mainly on grounds of obscenity. They were identified via word-based filtering methods and comprised of content related to erotica, dating, and/or LGBTI rights. [6] In 2011, the TIB created a list of 138 words that included çıplak (naked), *itiraf* (confession), *escort, hot, anal*, etc., and asked Turkish hosting companies to ban domain names including any of these words.[7]

In addition to websites, Turkish authorities blocked several social networking and/or collaborative sites (e.g. YouTube, MySpace, Dailymotion, Vimeo, Blogspot, Last.fm) because of a single case of offending content or on the grounds of copyright infringement. While some of these sites were banned intermittently, YouTube remained notoriously inaccessible between 2008 and 2010, and continued to receive more than 30 court orders for closure until 2014.[8]

Regarding the introduction of filtering systems and the administrative decisions to ban certain domain names, Turkish authorities were especially concerned with the protection of children and families. For example, the Information and Communication Technologies Board (*Bilgi Teknolojileri ve İletişim Kurumu*, known by its Turkish acronym, *BTK*), the government agency responsible for the regulation of the telecommunications industry, launched a program dubbed the "Safe Use of the Internet" in 2011. The BTK required all users to install a filtering system in their computers and to choose from four packages (child, family, domestic, and standard). Faced with strong reaction from academics, legal scholars and civic organizations, the BTK modified the program to be non-mandatory and offered two filtering options instead (child and family).[9] Although the family filter is optional for individual users, it is mandatory for public access sites such as internet cafes. While the BTK declines to provide a complete list of websites blocked by the family filter, the mandatory filtering software used at internet cafes reportedly blocks more than 1.5 million websites.[10]

[5] In 2009, the TIB stopped releasing the number of blocked websites creating a serious transparency problem. Since then legal scholars, internet activists and a citizen initiative called EngelliWeb ("Disabled Web") have been tracking the number of blocked websites. The annual and cumulative number of blocked websites were calculated using the Internet Archive. The numbers pertaining to administrative orders were culled from EngelliWeb's own statistics. See: Internet Archive, Wayback Machine, https://web.archive.org/web/*/https://engelliweb.com/, (accessed November 27, 2016). Engelli Web, 'Kurum Bazından İstatistikler', November 27, 2016, https://engelliweb.com/istatistikler/, (accessed November 27, 2016).

[6] Kuşburnu, 'Türkiye'de Internet Sansürünün Son 6 Yılı', *Kame*, July 9, 2015, https://network23.org/kame/2015/07/09/turkiyede-internet-sansurunun-son-6-yili/, (accessed November 27, 2016).

[7] 'Turkey Forbids 'Forbidden' from Internet Domain Names,' *Hurriyet Daily News and Economic Review* (Istanbul), April 28, 2011, http://www.hurriyetdailynews.com/default.aspx?pageid=438&n =turkey-forbids-8216forbidden8217-from-internet-domain-names-2011-04-28, (accessed November 27, 2016).

[8] M. Akgül and M. Kırlıdoğ, op. cit.

[9] Freedom House, *Freedom on the Net 2012*: Turkey, September 24, 2012, https://freedomhouse.org/report/freedom-net/2012/turkey, (accessed November 27, 2016).

[10] Kuşburnu, 'Türkiye'de Kaç Websitesi Sansürlü?', *Kame*, September 20, 2015, https://network23.org/kame/2015/09/20/turkiyede-kac-websitesi-sansurlu/, (accessed November 27, 2016).

III. 2013-2016: Tightening the noose

Legal and technological restrictions that were primarily driven by the urge to protect family values and/or national unity during the 2000s began to intensify in the following decade. Faced with two major legitimacy crises, first the nationwide anti-government Gezi protests in June 2013, and then revelations about a massive corruption scandal in December 2013, the AKP government imposed further restrictions to combat the perceived threats of digital communications.

During the Gezi protests, various actors resorted to social media to organize, gather and share news, and express underlying disenchantment with the AKP government.[11] The AKP's response was generally to demonize the internet and social media platforms, as seen in Erdogan's labeling of Twitter as a "menace" and "a curse on societies" that harbors "all sorts of lies."[12] There were also announcements by government officials about imminent restrictions to be placed on online communications to maintain public safety and order and to prevent so-called cyber-crimes.[13]

Approximately six months after the Gezi protests, a massive corruption scandal broke out in December 2013 triggering the construction of a sprawling online control regime. The scandal mostly transpired on social media with Erdogan's opponents sharing transcripts and audio files of illegally wiretapped conversations between Erdogan, his son, cabinet ministers and pro-AKP businessmen. To curb the flow of damning information online, the AKP began to deploy a combination of first, second and third generation controls by introducing stricter legislation, banning Twitter and YouTube, surveilling and prosecuting users, and throttling social media platforms.

The AKP government's approach to ICTs during this period bears striking similarities to that of the Russian government in the aftermath of the 2011-12 protest movement, also known as the White Revolution. Having noticed the "opportunities for political engagement and mobilization afforded by social media," the Russian government engaged in a widespread crackdown. It introduced laws to limit political engagement online, "attempted to re-create the state through cyberspace, fostering self-censorship and disempowering publics," and increased the presence of pro-government forces online creating "distorted communication within the Russian public sphere."[14]

In what follows, we examine similar strategies of control that took place in the Turkish online sphere between 2013 and 2016.

1. Legislation

Shortly after the corruption scandal, the AKP-dominated Parliament passed a new law amending the provisions of the 2007 Internet Law. The new law authorized the TIB to issue a blocking order based on a complaint filed for breach of an individual's right to privacy and to do so without obtaining a court order. Per the new law, individuals and legal entities can directly apply to the TIB and request the removal of offending content. The TIB can then require the ISPs to remove the offending content

[11] 'A Breakout Role for Twitter? The Role of Social Media during the Turkish Protests' Social Media and Political Participation (SMaPP) Data Report, New York University, June 1, 2013, https://18798-presscdn-pagely.netdna-ssl.com/smapp/wp-content/uploads/sites/1693/2016/04/turkey_data_report.pdf, (accessed November 27, 2016). S. Kuzuloglu, 'Gezi Parkı Eylemlerinin Sosyal Medya Karnesi.' *Radikal*, June 19, 2013, http://www.radikal.com.tr/yazarlar/m_serdar_kuzuloglu/gezi_parki_eylemlerinin_sosyal_medya_karnesi-1138146, (accessed November 27, 2016). D. Ergurel, 'The Role of Social Networks in #OccupyGezi Protests.' *Today's Zaman*, June 2, 2013, https://web.archive.org/web/20141018012744/http://www.todayszaman.com/blog/deniz-ergurel/the-role-of-social-networks-in-occupygezi-protests_317224.html, (accessed November 27, 2016). D. Dlugoleski, 'We Are All Journalists Now.' *Columbia Journalism Review*, May 20, 2013, http://www.cjr.org/behind_the_news/turkey_counter_media.php, (accessed November 27, 2016).

[12] Z. Tufekci, 'Everyone Is Getting Turkey's Twitter Block Wrong.' *Medium*, 2014. https://medium.com/technology-and-society/everyone-is-getting-turkeys-twitter-block-wrong-cb596ce5f27, (accessed November 27, 2016).

[13] S. Ocak, "'Siber Suçlar" için resmi adım atıldı: SOME'ler geliyor' *Radikal*, June 20, 2013. http://www.radikal.com.tr/turkiye/siber_suclar_icin_resim_adim_atildi_someler_geliyor-1138417, (accessed November 27, 2016). 'Police is `Working on' Twitter, Interior Minister Says' *Bianet*, June 17, 2013. http://bianet.org/english/politics/147681-police-is-working-on-twitter-interior-minister-says, (accessed November 27, 2016).

[14] A. Klyueva, "Taming Online Political Engagement in Russia: Disempowered Publics, Empowered State, and Challenges of the Fully Functioning Society." *International Journal of Communication*, 2016, 4670.

within 4 hours. The new law also enables a URL-based blocking system, making it possible to block individual posts or all posts from a specific social media user.[15] If the offending website is hosted domestically, it can be taken down by the TIB; if it is hosted abroad, then the said content can be blocked and filtered through ISPs.[16] The new law even gave the president of the TIB the authority to block URLs without complaints having been filed at all. Another controversial provision required the ISPs to collect data on users' activities for up to two years and to provide authorities with this data on demand.[17]

In addition to passing a stricter Internet Law, the AKP amended the Law on State Intelligence Services and the National Intelligence Organization (Law No. 6532) to expand the surveillance of online users. The amendment gives the National Intelligence Organization (*Milli İstihbarat Teşkilatı*, known by its Turkish acronym, *MIT*) unfettered access to online and offline "information, documents, data, or records from public institutions, financial institutions, and entities with or without a legal character." In practice, the new law enables the MIT to obtain citizens' personal data from any public or private institution (banks, schools, hospitals, ISPs) without a court order. Moreover, the new law criminalizes "the leaking and publication of secret official information, punishable by a prison term of up to nine years" and gives the AKP yet another tool to prevent the press and online news sites from reporting on government corruption and official misconduct.[18]

2. Social media bans

To control online flows of information, the AKP has also resorted to banning social media platforms. Whereas the earlier bans in late 2000s were prompted by content that allegedly threatened national unity, family and moral values, etc., those that have taken place since 2014 are part and parcel of the AKP's broader initiatives to curb the dissemination of news and information about the corruption scandal, foreign policy failures, Kurdish issue and/or security crises. For example, the TIB blocked access to Twitter in March 2014 citing a court order based on privacy invasion complaints that had been filed by citizens, however the ban was actually motivated by the AKP's need to limit the dissemination of critical news and information ahead of the local elections. [19] A month later, an Istanbul court asked Twitter, YouTube and Facebook to remove the images of a prosecutor being held at gunpoint arguing that these images were helping to "spread terrorist propaganda." Facebook complied with the court decision, removed the said images before the deadline and averted the ban. Twitter and YouTube remained unavailable for several hours, but they too complied and removed the images afterwards.[20]

3. Content removal

Since 2013, the AKP government has banned social media sites promptly and without hesitation. Yet even in the absence of specific incidents, it pursues tight control over the flow of information by filing content removal requests with social media companies on a regular basis. As can be seen in transparency reports issued by Facebook, Google and Twitter, Turkey ranks among the top countries with the most removal requests.[21]

[15] Since the blocking of a specific URL on encrypted communications (e.g. websites that start with "HTTPS") is technically not possible without banning the whole domain name, the amendment included a specific provision that enabled the ISPs to block websites in their entirety. See: E.K. Sözeri, 'Ban against a single blog post leads Turkish ISPs to censor all of WordPress', *The Daily Dot*, April 1, 2015 http://www.dailydot.com/layer8/turkey-wordpress-censorship-block/, (accessed November 27, 2016).

[16] Freedom House, *Struggle for Turkey's Internet*, August 27, 2014, https://freedomhouse.org/sites/default/files/The%20Struggle%20for%20Turkey%27s%20Internet.pdf, (accessed November 27, 2016).

[17] W. Zeldin, 'Turkey: Law on Internet Publications Amended', *Library of Congress*, February 24, 2014. Retrieved from https://www.loc.gov/law/foreign-news/article/turkey-law-on-internet-publications-amended/, (accessed November 27, 2016).

[18] K. Roth, 'Turkey's Tyrant in the Making', *Foreign Policy*, May12, 2014, https://foreignpolicy.com/2014/05/12/turkeys-tyrant-in-the-making/, (accessed November 27, 2016); Freedom House, op. cit.

[19] Z. Tufekci, op. cit.

[20] E. Peker and S. Schechner, 'Turkey Briefly Blocks YouTube', *Wall Street Journal*, April 6, 2015, http://www.wsj.com/articles/turkish-court-bans-access-to-internet-sites-over-hostage-crisis-content-1428325451, (accessed November 27, 2016).

[21] Google, *Transparency Report: Turkey*, https://www.google.com/transparencyreport/removals/government/TR/, (accessed November 27, 2016). Facebook, *Government Requests Report: Turkey*, https://govtrequests.facebook.com/country/Turkey/2015-H2/, (accessed

Table 2: Number of content removal requests by Turkish courts or administrative entities

Year	Google	Facebook	Twitter
2010	100	-	-
2011	443	-	-
2012	12,122	-	16
2013	13,965	2,014	32
2014	3,533	5,517	2,946
2015	4,366	6,574	10,070
2016	-	-	14,953

An important point to note here is the inclination of these companies to comply with Turkish authorities' requests to avoid a total ban, loss of users and advertising revenues in Turkey's ever-growing digital market. For example, since March 2014 Twitter has used its "country-withheld content policy" tool to block certain users or tweets from being seen in Turkey.[22] Facebook has repeatedly shut down pages of Kurdish politicians and newspapers, general interest pages about Kurdish music and culture, and pages with pro-Kurdish content simply based on "community complaints."[23] According to a leaked internal guideline, Facebook prompts its editors to block any content that allegedly insults Ataturk or supports the Kurdish militia group PKK.[24]

Internet and free speech activists in Turkey describe Twitter's policy as hypocritical considering its position on global free speech.[25] Yaman Akdeniz, a prominent activist and legal scholar notes that since most content that is readily removed by Facebook and Twitter is specifically about political expression, the already-existing fears among dissidents, activists and journalists are worsened .[26] According to members of Turkey Blocks, an independent group that identifies and verifies reports of internet censorship, also note that Twitter, Facebook and Google are "on board" with Turkey's censorship practices because they collaborate with the authorities and hold Turkey to different standards in terms of content removal requests. They note that "Especially in the post-coup period, Twitter readily complies with Turkey's demands" which has "emboldened" Turkish authorities.[27]

Other enablers of government restrictions are the domestic ISPs. In 2008, upon TIB's request, the ISPs agreed to install DNS servers that sync directly with TIB's central server facilitating the automatic updating of list of websites to be banned under "catalog crimes" (such as child pornography or obscenity). [28] In 2014, the TIB expanded this infrastructure by introducing deep packet inspection (DPI) technologies and had the ISPs agree to maintain detailed traffic logs of their customers. The use of DPI also enabled the TIB and by proxy the government, to use more opaque tools to censor online content, such as blocking individual URL addresses instead of banning the entire domain, wholesale banning of news *topics* instead of banning news websites, and throttling access to social media platforms instead of nationwide bans.

November 27, 2016). Twitter, *Transparency Report: Turkey*, https://transparency.twitter.com/en/countries/tr.html, (accessed November 27, 2016). Note that Facebook does not provide number of requests, and that Twitter's 2016 data only covers the first half of the year.

[22] V. Gadde, 'Challenging the access ban in Turkey', Twitter, March 26, 2014, https://blog.twitter.com/2014/challenging-the-access-ban-in-turkey, (accessed November 27, 2016).

[23] Freedom House, *Struggle for Turkey's Internet*, August 27, 2014, https://freedomhouse.org/sites/default/files/The%20Struggle%20for%20Turkey%27s%20Internet.pdf, (accessed November 27, 2016).

[24] S. Spary, 'Facebook Is Embroiled in a Row with Activists Over "Censorship"', *BuzzFeed*, April 8, 2016, https://www.buzzfeed.com/saraspary/facebook-in-dispute-with-pro-kurdish-activists-over-deleted (accessed November 27, 2016).

[25] E.K. Sözeri, 'Uncovering the accounts that trigger Turkey's war on Twitter', *The Daily Dot*, January 31, 2015, http://www.dailydot.com/layer8/twitter-transparency-report-turkey-censorship/, (accessed November 27, 2016). J. Halliday, 'Twitter's Tony Wang: "We are the free speech wing of the free speech party"', *The Guardian*, March 22, 2012, https://www.theguardian.com/media/2012/mar/22/twitter-tony-wang-free-speech (accessed November 27, 2016).

[26] Email correspondence with Yaman Akdeniz, 2016.

[27] Skype interview with two members of Turkey Blocks, January 2, 2017.

28 E.K. Sözeri, 'Censorship reveals direct, likely illegal link between ISPs and Turkey's government', The Daily Dot, December 28, 2016, http://www.dailydot.com/layer8/turkey-censorship-nos-court-orders-illegal/, (accessed January 14, 2017), M. Akgül and M. Kırlıdoğ, op cit.

4. Surveillance of users

In addition to first and second generation controls, Turkish authorities have begun to deploy third generation controls, such as surveillance and hacking. For example, the Turkish National Police used online intrusion tools and services provided by Hacking Team, an Italian surveillance company, between 2011 and 2014.[29] Turk Telekom—the largest ISP that owns 80% of internet infrastructure in Turkey – has also been found to have procured deep packet inspection tools from Procera Networks, a U.S.-based company. [30] Turk Telekom also used to work with Phorm, a targeted advertising company, and deployed its deep packet inspection tools in violation of privacy laws.[31] Additionally, there are other unspecified government clients that have used (and/or continue to use) mass surveillance services provided by Asoto, Netclean and Nokia Siemens Networks.[32]

5. Prosecution of users

An important tool in the Turkish government's arsenal to suppress critical online speech is the prosecution of social media users based on their posts that allegedly insult the state and state officials and disseminate propaganda for terrorist organizations. According to the Penal Code, insulting state officials is punishable by a prison sentence of one or two years, whereas insulting the president (i.e. Erdogan) can lead to a prison sentence of up to four years (Article 125/3a and Article 299).[33] The Ministry of Justice statistics show that 1,953 individuals were prosecuted in 2015 on charges of insulting Erdogan, and 49 on charges of insulting state officials.[34] According to news reports, 34 of these cases involved social media posts by members of opposition parties, lawyers, academics, journalists, and members of NGOs.[35] Four users were handed 10-month prison sentences each; three placed under judicial control, and fourteen arrested pending trial. The rest were detained pending prosecution or summoned for questioning. Among the high-profile cases are an anchorwoman, a former editor-in-chief, and a columnist who were prosecuted for allegedly critical tweets concerning Erdogan, the state or state officials. [36]

In addition, state institutions and private companies have begun to take legal action against

[29] E.K. Sözeri, 'Turkey paid Hacking Team $600k to spy on civilians,' *The Daily Dot*, July 7, 2015, http://www.dailydot.com/politics/hacking-team-turkey/, (accessed November 27, 2016).

[30] It was in July 2014 when Turk Telekom's contract with Procera Networks was revealed. However, Procera released a statement noting that its activities were in accordance with the new Internet Law and the specific provision that required ISPs to store users' activity logs for two years. See W. Zeldin, op. cit., T. Fox-Brewster, 'Is An American Company's Technology Helping Turkey Spy On Its Citizens?', Forbes, October 25, 2016, http://www.forbes.com/sites/thomasbrewster/2016/10/25/procera-francisco-partners-turkey-surveillance-erdogan/, (accessed November 27, 2016). S. Güçlü, 'Türk Telekom'a 5 Yıl Önce Verilen Fiber Muafiyet Hakkı İşe Yaradı mı?', Türk İnternet, November 7, 2016, http://www.turk-internet.com/portal/yazigoster.php?yaziid=54478, (accessed November 27, 2016).

[31] E.K. Sözeri, 'Turkish government revealed to be spying on its citizens through ISPs', *The Daily Dot*, October 29, 2016, www.dailydot.com/layer8/turkey-procera-deal-isps-dpi/, (accessed November 27, 2016).

[32] Privacy International, *Surveillance Industry Index*, https://sii.transparencytoolkit.org/search?action=index&controller=docs&found_in_facet=Turkey&page=1, (accessed November 27, 2016).

[33] Venice Commission, Council of Europe, *Penal Code of Turkey (Law 5237, September 26, 2004)*, Opinion No. 831/2015, February 15, 2016. http://www.venice.coe.int/webforms/documents/?pdf=CDL-REF(2016)011-e, (accessed November 27, 2016).

[34] Turkish Ministry of Justice, *Ceza Mahkemelerinde TCK Uyarınca Yıl İçinde Açılan Davalardaki Suç ve Sanık Sayıları (2015)* (Distribution of court cases by Penal Code articles (2015), http://www.adlisicil.adalet.gov.tr/Istatistikler/1996/genel_tck_açılan2015.pdf, (accessed November 27, 2016).

[35] B. Molu and D. Irak, 'TCK md. 299 - Cumhurbaşkanına Hakaret Suçu kapsamında ifadeye çağrılan, gözaltına alınan, soruşturma açılan, tutuklanan kişilerin güncel listesi', April 7, 2016, http://bit.ly/tck_299, (accessed November 27, 2016).

[36] Committee to Protect Journalists, 'Turkish editor given suspended prison term for insulting Erdoğan on Twitter', June 19, 2015, https://cpj.org/2015/06/turkish-editor-given-suspended-prison-term-for-in.php, (accessed November 27, 2016). E.K. Sözeri, 'Dutch journalist arrested in Turkey for 'insulting' President Erdoğan online', The Daily Dot, Apr 26, 2016, http://www.dailydot.com/layer8/ebru-umar-insult-erdogan-twitter/, (accessed November 27, 2016). 'Turkish court acquits journalist over corruption case tweet', AFP, October 6, 2015, https://uk.news.yahoo.com/turkish-court-acquits-journalist-over-corruption-case-tweet-093039669.html, (accessed November 27, 2016).

social media users, exploiting Turkey's vaguely-defined defamation laws. In 2015, the state-run news agency, Anadolu Ajansı, sued more than fifty artists and journalists on charges of libel.[37] In 2016, Turkcell, one of Turkey's largest mobile network providers, sought 10,000 Turkish liras (USD 3,500) in damages from *each* Twitter user that tweeted the hashtag #TecavuzCell ("Rape Cell") as a means of protesting the company's sponsorship of a government-linked foundation embroiled in child abuse allegations.[38]

In addition to defamation charges, in 2015 Turkish authorities have accused more than 13,000 individuals with "disseminating terrorist propaganda" in relation to expression of political opinions or coverage of the Kurdish conflict.[39] That same year, 36 journalists and newspaper distributors were imprisoned on charges of terrorist propaganda.[40] Although official statements did not specify how many of these cases involve social media posts, [41] news reports stated that Kurdish journalists Idris Yılmaz and Vildan Atmaca were prosecuted for their pro-PKK Facebook pages, while Hayri Tunc was held in pre-trial detention for his Twitter and Facebook posts, and Hamza Aktan was detained for retweeting a BBC post regarding military operations in Southeast Turkey. [42]

6. Throttling and DNS poisoning

During the 2013-2016 period, the AKP government began to use new tools to limit the flow of news and information in the online public sphere. The first is bandwidth throttling, the intentional slowing down of internet service at the ISP level. According to Turkey Blocks, there have been at least seven cases of throttling since 2015.[43] As seen in the table below, the AKP government blocked URLs (including news sites) and throttled social media platforms at times of major political events and security crises to suppress critical reporting and to prevent citizens from mobilizing.[44]

[37] E. Önderoğlu, 'Erdoğan'ı Eleştiren Kendini Mahkemede Buluyor; İşte Davalar!', Bianet, April 30, 2015, https://bianet.org/bianet/medya/164185-erdogan-i-elestiren-kendini-mahkemede-buluyor-iste-davalar, (accessed November 27, 2016).

[38] E.K. Sözeri, 'A Turkish mobile provider got 13 court orders to erase this hashtag from the Internet', The Daily Dot, May 20, 2016, http://www.dailydot.com/layer8/turkcell-tecavucell-twitter-censorship/, (accessed November 27, 2016).

[39] The Anti-Terror Law stipulates that "any person making propaganda for a terrorist organization [by justifying, glorifying or inciting violent or threatening acts] shall be punished with imprisonment from one to five years. If this crime is committed through means of mass media, the penalty shall be aggravated by one half." (Article 7). Legislationline, *Law on Fight Against Terrorism (Law 3713, April 12, 1991)*, http://www.legislationline.org/download/action/download/id/3727/file/Turkey_anti_terr_1991_am2010_en.pdf, (accessed November 27, 2016), Turkish Ministry of Justice, *Ceza Mahkemelerinde Özel Kanunlar Uyarinca Yıl İçinde Açilan Davalardaki Suç Ve Sanik Sayilari (2015)* ("Distribution of court cases by Special Codes articles (2015)"), 2015, http://www.adlisicil.adalet.gov.tr/Istatistikler/1996/genel_%C3%B6zel_a%C3%A7%C4%B1lan2015.pdf, (accessed November 27, 2016).

[40] E. Önderoğlu, '2015 Medya: Gazetecilik Tehlikeli ve Sakıncalı Bir Meslek!', *Bianet*, January 29, 2016, https://bianet.org/bianet/medya/171582-2015-medya-gazetecilik-tehlikeli-ve-sakincali-bir-meslek, (accessed November 27, 2016).

[41] During the pre-coup period, Turkish officials refrained from openly referring to social media posts as evidence of "terrorist propaganda." In the post-coup period, however, officials have made explicit references to social media posts and stated that these posts can potentially be used as evidence in investigations.

[42] Committee to Protect Journalists, 'Turkish journalist arrested for posts on social media', February 8, 2016, https://cpj.org/2016/02/turkish-journalist-arrested-for-posts-on-social-me.php, (accessed November 27, 2016), Committee to Protect Journalists, 'In Turkey, two journalists accused of creating terrorist propaganda with social media posts', November 18, 2015, https://cpj.org/2015/11/in-turkey-two-journalists-accused-of-terrorism-ove.php, (accessed November 27, 2016), 'Turkey detains pro-Kurdish news editor over tweets', *AFP*, April 30, 2016, https://www.yahoo.com/news/turkey-detains-pro-kurdish-news-editor-over-tweets-002818986.html, (accessed November 27, 2016).

[43] I. Mater, 'TIB'siz Türkiye', *Bianet*, August 27, 2016, http://bianet.org/biamag/biamag/177985-tib-siz-turkiye, (accessed November 27, 2016).

[44] This table is based on information presented in Freedom House's "2016 Freedom of the Net: Turkey" and Turkey Blocks reports. Note that on July 15, 2016, the night of the coup attempt, social media was throttled as is generally the case, however this decision was promptly overturned in order to disseminate President Erdoğan's call to his supporters to take to the streets and resist the putschist soldiers. See: E.K. Sözeri, 'Why Turkey issued a social media ban during a coup attempt—and promptly lifted it', *The Daily Dot*, July 17, 2016, www.dailydot.com/layer8/turkey-coup-social-media-ban-lift/ (accessed November 27, 2016).

Table 3: Types of content restrictions imposed by the Turkish government in the pre-coup period

Date	Incident	Content restriction
April 3, 2015	Istanbul prosecutor taken hostage	166 URLs blocked including news articles, and Facebook, Twitter, YouTube content
July 20, 2015	Bomb attack in Suruç	173 URLs blocked including 38 news websites
October 10, 2015	Bomb attack in Ankara	Facebook and Twitter throttled
January 12, 2016	Bomb attack in Istanbul	Government issued media blackout
February 17, 2016	Bomb attack in Ankara	Facebook and Twitter throttled
March 13, 2016	Bomb attack in Ankara	Facebook and Twitter throttled, 214 URLs blocked
March 19, 2016	Bomb attack in Istanbul	Facebook and Twitter banned for 24 hours
June 28, 2016	Bomb attack at Istanbul airport	Facebook and Twitter throttled
July 15, 2016	Military coup attempt	Facebook and Twitter briefly throttled

The second tool deployed by Turkish authorities is DNS poisoning, a form of hacking or blocking social media sites by surreptitiously redirecting users to incorrect IP addresses. In March 2014, Turk Telekom hijacked Google DNS servers, which the Internet Society described as a "man-in-the-middle" (MiTM) attack" performed to "comply with [the] government's banning of [Twitter and YouTube]" by "giving users false information."[45] Not only were users blocked from their intended destination, but also the "IP addresses of [their] devices attempting to reach the two services using foreign DNS servers" were also logged by the government.[46]

IV. July 2016-present: Post-coup developments

As shown above, the AKP constructed a sprawling surveillance-control-censorship regime during 2013-2016 mainly in response to the political fallout from Gezi protests and the corruption scandal as well as security-related incidents such as terrorist attacks. In the aftermath of the failed coup, the AKP's internet policy was similarly shaped by political anxieties which ultimately expanded and fortified the existing online control regime.

In the immediate aftermath of the failed coup, the AKP government under the leadership of President Erdogan declared a State of Emergency, and embarked on a massive purge of security officers, civil servants, educational and media workers it accused of being affiliated with the religious movement of Fethullah Gulen— the alleged mastermind of the coup. Given the severity of the potential threats the coup would have caused had it succeeded, a "national consensus" emerged, uniting the AKP, opposition parties and various political actors and engendering the (false) belief that the State of Emergency would be used *only* to root out the coup planners. However, it soon became clear that Erdogan and his government would deploy the SoE to repress other perceived enemies, especially the Kurds, to consolidate their hegemony and stifle any remaining opposition—both online and offline.

[45] D. York, 'Turkish Hijacking of DNS Providers Shows Clear Need For Deploying BGP And DNS Security', *Internet Society*, April 1, 2014, http://www.internetsociety.org/deploy360/blog/2014/04/turkish-hijacking-of-dns-providers-shows-clear-need-for-deploying-bgp-and-dns-security/, (accessed November 27, 2016).

[46] S. Gallagher, 'Turkey now blocking social media by hijacking Google DNS', *Ars Technica*, March 30, 2014, http://arstechnica.com/information-technology/2014/03/turkey-now-blocking-social-media-by-hijacking-google-dns/, (accessed November 27, 2016).

In what follows, we focus on measures taken by the AKP in the post-coup period and their implications on online communications.

1. Legislation via decree laws

One of the unchecked powers granted by the State of Emergency is the ability to rule by decree. Since the coup attempt in July 2016, the AKP government passed fifteen decree laws (as of this writing) that enabled the reconfiguration of political, economic, social and cultural fields as per Erdogan's political priorities. Including, but not limited to the massive purge of tens of thousands of civil servants without due process, closure of hundreds of print and broadcast outlets, arrests of journalists, writers and members of the parliament, decree laws have also been deployed to impose further restrictions on the rapidly-deteriorating digital public sphere.

The passing and application of decree laws are supposedly limited to coup-related matters, however in practice they have resulted in digital surveillance of users and the shutting down of internet service at times of so-called security operations (see below). For example, Decree Law 670 enables the interception of digital communications of all users as part of the coup-related investigations and the collection of private data from all state institutions and private companies. Decree Law 671 amends the Law of Digital Communications and allows the BTK to overtake any privately-held digital communications company including cable or cellular network providers to "[maintain] national security and public order; prevent crime; protect public health and public morals; or protect the rights and freedoms [of citizens]."[47] Last but not least, and in a blow to personal privacy online, Decree Law 680 amends the Code of Police Conduct and enables the Department of Cybercrimes to gather and intercept internet traffic on any cyber-related investigation, and to obtain personal information from ISPs without a court order.

[47] E.K. Sözeri, 'Turkey uses emergency decree to shut down internet on 11 Kurdish cities to "prevent protests"', *The Daily Dot*, October 27, 2016, http://www.dailydot.com/layer8/turkey-cuts-kurdistan-internet/, (accessed November 27, 2016).

2. Closing of the TIB

One of the significant developments in the aftermath of the coup attempt was the closing of the TIB by decree law. Claiming that the agency had been infiltrated by Gulenists and served as a hub of illegal wiretapping over the years, the AKP government transferred the TIB's duties and responsibilities to the BTK. However, the closing of the agency responsible for the blocking of more than 100,000 websites and banning of social media platforms on various occasions is not necessarily good news for internet users, activists and digital rights lawyers in the country. As Yaman Akdeniz notes, the BTK is driven by the same "aggressive blocking mentality" as the TIB was. Akdeniz also underlines the partisan character of the BTK since it operates under the Ministry of Transport, Maritime Affairs and Communications, and its staff are government appointees.[48]

3. Throttling

In the post-coup period, the AKP government has continued to use throttling as a measure to restrict certain types of content. As table 4 shows, social media platforms and on certain occasions private messaging applications are throttled to limit online communications in the aftermath of terrorist attacks, security and military-related incidents.

4. Internet Shutdowns and Cloud/VPN Restrictions

During the post-coup period, the AKP not only escalated the implementation of its customary strategies (i.e implementation of legal restrictions, throttling, prosecution of online users), but also deployed internet shutdowns, cloud and VPN restrictions—drastic forms of control that are generally associated with dictatorships.

First came the internet shutdown in September 2016 as elected mayors in predominantly-Kurdish cities were physically removed from their posts

[48] 'Social media blocked in Turkey', *Turkey Blocks*, August 25, 2016, https://turkeyblocks.org/2016/08/25/social-media-blocked-turkey/, (accessed November 27, 2016). 'Elektronik Haberleşme Sektörüne İlişkin Yetkilendirme Yönetmeliğinde Değişiklik Yapılmasına Dair Yönetmelik', ("Amendment to the Authorization Regulation in the Digital Communications Sector") *Resmi Gazete*, http://www.resmigazete.gov.tr/eskiler/2016/06/20160611-1.htm, (accessed November 27, 2016).

Table 4: Types of content restrictions imposed by the Turkish government in the post-coup period

Date	Incident	Content restriction
August 20, 2016	Bomb attack in Gaziantep	Facebook and Twitter throttled for six hours
August 25, 2016	Unknown reason	Facebook, Twitter and YouTube throttled for seven hours
September 11, 2016	28 elected mayors removed from office in the Kurdish-majority Southeast	Landline and mobile internet access cut for 15 cities, for approximately 12 million citizens
October 7, 2016	Unknown reason	Twitter intermittently throttled
October 8, 2016	Email archive of Energy Minister leaked	Google Drive, Drobox, One Drive and GitHub blocked
October 26-31, 2016	Co-mayors of Diyarbakir (Kurdish-majority city) detained	Landline and mobile internet access intermittently cut for 11 cities in southeast region
November 4, 2016	Pro-Kurdish party (HDP) co-chairs and deputies detained	Twitter, YouTube, Facebook and WhatsApp throttled
November 4, 2016	Unknown reason	Access to popular VPN services banned permanently
December 3, 2016	Unknown reason	Wikipedia temporarily throttled
December 18, 2016	Unknown reason	Access to Tor Network banned permanently
December 19, 2016	Assassination of Russian Ambassador to Turkey	Facebook, Twitter and YouTube throttled; Dutch broadcaster NOS banned
December 22, 2016	Release of ISIS video on Turkish soldiers' execution	Facebook, Twitter and YouTube throttled
January 1,2017	Armed attack at Istanbul nightclub	Temporary gag order including social media and news websites (no throttling)

under the State of Emergency rulings. The AKP government via the BTK shut down internet service in ten cities to suppress the dissemination of news and information regarding possible civil unrest in the region. According to Turkey Blocks, internet access through landline and mobile telephony was unavailable for about 4-6 hours, affecting approximately 12 million people. This very first internet shutdown, albeit regional, was repeated in October 2016 when the co-mayors of Diyarbakir, the de facto capital of the Kurdish community, were arrested on charges of terrorism. This second shutdown affected approximately six million people in 11 cities in the southeast, and lasted two days (in Diyarbakir, the duration was five days).[49] As Rebecca MacKinnon notes "localized disconnection and restriction" is a tool used by governments to "ensure that people cannot use the internet or mobile phones to organize protests" in times of crisis.[50]

On November 4, the crackdown on Kurdish politicians, as 11 members of the parliament from the Peoples' Democratic Party (known by its Turkish acronym, HDP) were arrested in midnight house raids. Instead of a regional internet shutdown, the government implemented a nationwide throttling of Twitter, Facebook, YouTube, as well as WhatsApp (the first time an instant messaging service was restricted) justifying it as a "temporary security measure."[51] The

[49] 'New internet shutdown in Turkey's Southeast: 8% of country now offline amidst Diyarbakir unrest', *Turkey Blocks*, October 27, 2016, https://turkeyblocks.org/2016/10/27/new-internet-shutdown-turkey-southeast-offline-diyarbakir-unrest/, (accessed November 27, 2016).

[50] R. MacKinnon, 2011. "China's 'Networked Authoritarianism," Journal of Democracy, 22:2, p. 40

[51] 'Facebook, Twitter, YouTube and WhatsApp shutdown in Turkey', *Turkey Blocks*, November 4, 2016, https://turkeyblocks.org/2016/11/04/social-media-shutdown-turkey/, (accessed November 27, 2016). 'Slowdown in

throttling of social media and instant messaging services was indeed temporary, however the BTK ordered Turkish ISPs to block popular VPN services and Tor Network to enable the full implementation of throttling and banning orders.[52] Experts note that the decision to block Tor access will most likely be permanent as part of the government's broader plan to not only execute censorship orders but also to enable easier surveillance of users.[53]

Considering the above-mentioned developments, it is fair to argue that the Turkish government's post-coup internet policy is different from the pre-coup period in terms of both the types of measures (e.g. regional internet shutdowns) and the types of incidents that trigger these measures. For example, the blocking of online communications that occurred in July 2015 was prompted by a cross-border military operation in Southeast Turkey,[54] whereas those in September-November 2016 were specifically aimed at limiting (potential) civilian protests in the same region. Likewise, social media throttling in the pre-coup period transpired at times of security-related incidents (see Table 3), whereas in the post-coup period it was prompted by the leaking of damaging emails and information, and was complemented with the blocking of cloud drive services, VPN services and Tor access. This widening of the net *and* tightening of the mesh, so to speak, occurred in October 2016 when the government blocked access to drive services (Google Drive, DropBox, Microsoft One Drive) and the software repository GitHub in response to the leaking of the email archive of Berak Albayrak, the Minister of Energy and Natural Sources, and Erdogan's son-in-law. The decision to block said services was prompted by the publication of 57,000 emails that laid bare the relationships between the AKP, and business and media circles, as well as details about Albayrak's private life. [55]

5. Internet sovereignty and data localization initiatives

Another step Turkish authorities have taken in the post-coup period is the building of "a domestic search engine and email service compatible with national culture and values." Similar to Russian, Chinese and Iranian efforts at creating digital borders and launching country-specific social media platforms (China's WeChat and Russia's VKontakte),[56] the key objective of internet sovereignty is to control the flow of information that emanates from outside Turkey. In addition to online traffic control, Turkish authorities are also motivated by enhanced surveillance of online communications, as seen in the official statement pointing to the "need to store user data within Turkey's borders and ensure that communications could be fully analyzed domestically."[57]

To incentivize the establishment of local data centers, the government will provide favorable terms in regard to land use, corporate taxes and electricity costs. According to Decree Law No. 678, published in the official gazette in November 2016, the government's plan is to encourage Google, YouTube, Facebook and Twitter to establish data centers in Turkey and consequently make them

access to social media in Turkey a 'security measure,' says PM', *Hurriyet Daily News*, November 4, 2016, http://www.hurriyetdailynews.com/problems-in-access-to-social-media-in-turkey-a-security-measure-says-pm.aspx?pageID=238&nID=105744&NewsCatID=509, (accessed November 27, 2016).

[52] L. Franceschi-Bicchierai, 'Turkey Doubles Down on Censorship With Block on VPNs, Tor', *Motherboard*, November 4, 2016, https://motherboard.vice.com/read/turkey-doubles-down-on-censorship-with-block-on-vpns-tor, (accessed November 27, 2016).

[53] J. Kopstein, 'Tor Ban in Turkey Likely Permanent, Watchdog Group Says', *Vocativ*, January 03, 2017 www.vocativ.com/389232/tor-ban-turkey-permanent/, (accessed January 14, 2017).

[54] In July 2015, mobile internet access was cut in most of southeast Turkey for 60 hours during the aerial bombardment of ISIS and PKK positions in Northern Syria and Iraq. According to local news reports, the service interruption was based on an order issued by the Office of the Prime Minister. See, E.K. Sözeri, 'Turkey cuts internet access to Kurdish towns, removes elected mayors', *The Daily Dot*, September 11, 2016, www.dailydot.com/layer8/turkey-internet-access-kurdish-towns/ (accessed January 14, 2017).

[55] 'Turkey blocks web drives after email leak', *BBC*, October 10, www.bbc.com/news/technology-37608553, (accessed November 27, 2016).

[56] S. Gunitsky, 2015. "Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability," *Perspectives on Politics*, 13:1, p. 44

[57] 'Turkey to launch domestic Google, Gmail replacements aligned with local culture and values', *Turkey Blocks*, January 6, 2017, https://turkeyblocks.org/2017/01/06/turkey-building-domestic-search-engine-and-email/, (accessed January 14, 2016).

subject to local laws. According to reports in pro-government newspapers, data localization is part of a broader plan to store user data in order to "accelerate the process of identifying social media users that praise and provoke terrorism, closing their accounts, and blocking content."[58] As members of Turkey Blocks note, these initiatives signal a trend towards a "walled garden" model that denies access to foreign internet services and instead encourages local search engines and social media platforms, and is therefore isolationist in nature.[59]

6. Prosecution of social media users and the institutionalization of "snitching"

The prosecution of social media users is not a new phenomenon, however, in the post-coup period it has escalated both in terms of its pervasiveness and severity. According to the Ministry of Interior Affairs, 3,710 people were detained for questioning between July and December 2016 with 1,656 of them arrested, 1,970 released, and 84 under detention as of this writing. Charges included "inciting the public to hatred, animosity and agitation," "praising terrorism," "engaging in terrorist propaganda," "insulting state officials" and "undermining state sovereignty and public safety."[60] In addition, as per the statement of a member of the parliamentary commission on security and intelligence affairs, the government purportedly set up a "Social Media Monitoring Unit" which is currently in the process of preparing legal investigation notices for 17,000 users and finding the addresses of another 45,000.[61]

Shortly after the release of this information, a high-profile incident of social media-related prosecution occurred. Barbaros Sansal, fashion designer, LGBT activist and outspoken government critic became the target of pro-government trolls upon sharing a video message that included allegedly offensive remarks concerning the AKP, the Turkish state and society. Sansal was immediately extradited from Northern Cyprus to Turkey, only to be physically assaulted by angry mobs at the airport apron, and finally detained and arrested the next day.[62]

While online trolling played a role in bringing Sansal to the attention of law enforcement and the courts, there is no publicly available information as to how many of the above-mentioned detentions and arrests were initiated by police surveillance versus citizen informants. In a worrisome development, in December 2016 the Turkish National Police (TNP) launched a smart phone app and a dedicated webpage that allow citizens to report social media posts they consider to be terrorist propaganda. In its public announcements, the TNP has urged citizens to share all available information concerning the harmful content, the user, and to take a screen shot of the content in case it is deleted.[63] The news of the app was welcomed by pro-government media outlets, journalists, pundits, and online users, who wholeheartedly encouraged fellow citizens to report the alleged "social media terrorists;" becoming a symbolizing indicator of the government's changing internet policy and the ways it is implemented.

[58] B. Simsek, 'Sosyal medya terorune kokten cozum geliyor, *Sabah*, January 4 2017, http://www.sabah.com.tr/yasam/2017/01/04/sosyal-medya-terorune-kokten-cozum-geliyor, (accessed January 14, 2016).
[59] Skype interview with two members of Turkey Blocks, January 2, 2017.
[60] "Sosyal medyada buyuk gozalti," *Cumhuriyet*, January 18, 2017, http://www.cumhuriyet.com.tr/haber/turkiye/650063/Sosyal_medyaya__buyuk_gozalti_..._10_bin_kisiye_sorusturma_acildi.html, (accessed January 14, 2016).
[61] 'Sosyal medyaya buyuk operasyon,' *Cumhuriyet*, January 14, 2017, http://www.cumhuriyet.com.tr/haber/siyaset/660327/Sosyal_medyaya_buyuk_operasyon__17_bin_kisi_hakkinda_fezleke_hazirlandi__45_bin_kullanici_araniyor.html (accessed January 18, 2017)
[62] E. Toksabay, 'Turkish fashion designer arrested: reports', *Reuters*, January 3, 2017, www.reuters.com/article/us-turkey-security-designer-idUSKBN14N1PW, (accessed January 14, 2016).
[63] 'Sosyal medyada teröre destek verenler nasıl ihbar edilir?', *Yeni Safak*, December 23, 2016, http://www.yenisafak.com/teknoloji/sosyal-medyada-terore-destek-verenler-nasil-ihbar-edilir-2585434, (accessed January 14, 2016).

Figure 1: Message from Turkish National Police issued in July 2016: "Turkish National Police Warns Citizens: You can report social media profiles and pages that support terrorist activities and include criminal content by sending an email to the following accounts with links and screenshots."[64]

Figure 2: Tweet posted by A Haber, a pro-government television channel: "Report the terrorists to authorities by using your cellphone. New app from the police. 'Online reporting'"[65]

[64] T.C. Başbakanlık Basın Yayın ve Enformasyon Genel Müdürlüğü (Republic of Turkey Office of the Prime Minister, Directorate General of Press and Information), 'Emniyet Genel Müdürlüğü vatandaşları uyarıyor.' @ *Byegm on Twitter*, July 17, 2016, https://twitter.com/byegm/status/754682443458895872, (accessed January 14, 2017).

[65] 'Teröristi cep telefonundan ihbar et!.. Emniyetten yeni uygulama "online ihbar" http://www.ahaber.com.tr/webtv/teknoloji/teroristi-cep-telefonundan-ihbar-', @ *tvahaber on Twitter*, December 18, 2016, https://twitter.com/tvahaber/status/810479836217090048, (accessed January 14, 2017).

7. Pro-government presence online

Previous sections have documented various types of online restrictions that range from throttling to prosecution of users. Although the majority of these restrictions are not formally acknowledged or announced, they are nonetheless based on official decisions made by the government and carried out by the BTK and the courts. However, as this section details, there has been a palpable increase in pro-government presence online and consequently higher levels of intimidation and harassment against anti-AKP journalists, pundits and users.

a) Trolls

In the immediate aftermath of the Gezi protests in 2013, the AKP government became aware of the protestors' use of Twitter in mobilization and organization, and thus decided to form its own social media team. The initial objective of the 6,000-member team, comprised of anonymous pro-government influencers, was to promote a positive image of the government. However, this team soon came to be known as "AK Trolls" because their online activities turned abusive, harassing and threatening critical journalists.[66] In 2015, their online affiliations with government officials and pro-government journalists were revealed, as were their attempts at organizing physical attacks targeting independent news organizations and journalists.[67]

[66] A. Albayrak & J. Parkinson, 'Turkey's Government Forms 6,000-Member Social Media Team', *The Wall Street Journal,* September 16, 2013, www.wsj.com/articles/SB10001424127887323527004579079151479634742, (accessed January 14, 2017), E. Kizilkaya, 'AKP's social media wars', *Al-Monitor*, November 15, 2013, www.al-monitor.com/pulse/originals/2013/11/akp-social-media-twitter-facebook.html, (accessed January 14, 2017).

[67] E.K. Sözeri, 'Mapping Turkey's Twitter-troll lynch mobs', *The Daily Dot*, October 22, 2015, whttp://ww.dailydot.com/layer8/turkey-twitter-trolls/, (accessed January 14, 2017), C. Yeginsu, 'Opposition Journalists Under Assault in Turkey', *The New York Times*, September 17, 2015, https://www.nytimes.com/2015/09/18/world/europe/opposition-journalists-in-turkey-increasingly-face-violent-attacks.html, (accessed January 14, 2017), E.K. Sözeri, 'Dutch journalist arrested in Turkey for 'insulting' President Erdoğan online', *The Daily Dot*, April 26, 2016, http://www.

As documented by the International Press Institute (IPI), "government supporters and nationalists" were already using "threats of violence, verbal abuse, technical interference and legal threats" well before the coup attempt to either incite physical acts of violence against journalists or to simply "question their credibility or to silence them." On Twitter, it was common practice for pro-AKP accounts to label journalists as "traitors", "terrorists," "supporters of terrorism" and "kafir" (infidel).[68] The IPI notes that in the post-coup conjuncture, the Turkish National Police's social media reporting program, coupled with the ongoing State of Emergency, has only strengthened government supporters' harassment of journalists and granted them continuing impunity.[69]

In addition to online harassment, the pro-AKP social media teams launched an online propaganda scheme aiming to boost the morale of young (male) Turks while intimidating Kurds in response to the flaring up of armed conflict between the Turkish army and the PKK. Opening new accounts under pseudonyms such as "special force" and using the Turkish flag in their profile pictures, these pro-government trolls shared images of dead bodies, purportedly of Kurdish militia, emblazoning them with nationalist slogans.[70] It was later revealed that one such Twitter account was owned by none other than an AKP-affiliated governor in the region.[71] By the time "anti-terror" operations concluded and the government declared that the region had been cleansed of terrorists, all such Twitter accounts were curiously shut down.

To illustrate the pro-government presence online, we conducted an analysis of Twitter activity in the months before and after the coup attempt. Based on information collected by the DMI-TCAT,[72] the following graphs show Twitter activity by different user groups.

dailydot.com/layer8/ebru-umar-insult-erdogan-twitter/, (accessed January 14, 2017).

[68] IPI, 2017, "On the Line: Tracking Online Harassment of Journalists," http://onthelinedb.ipi.media/, (accessed January 12, 2017).

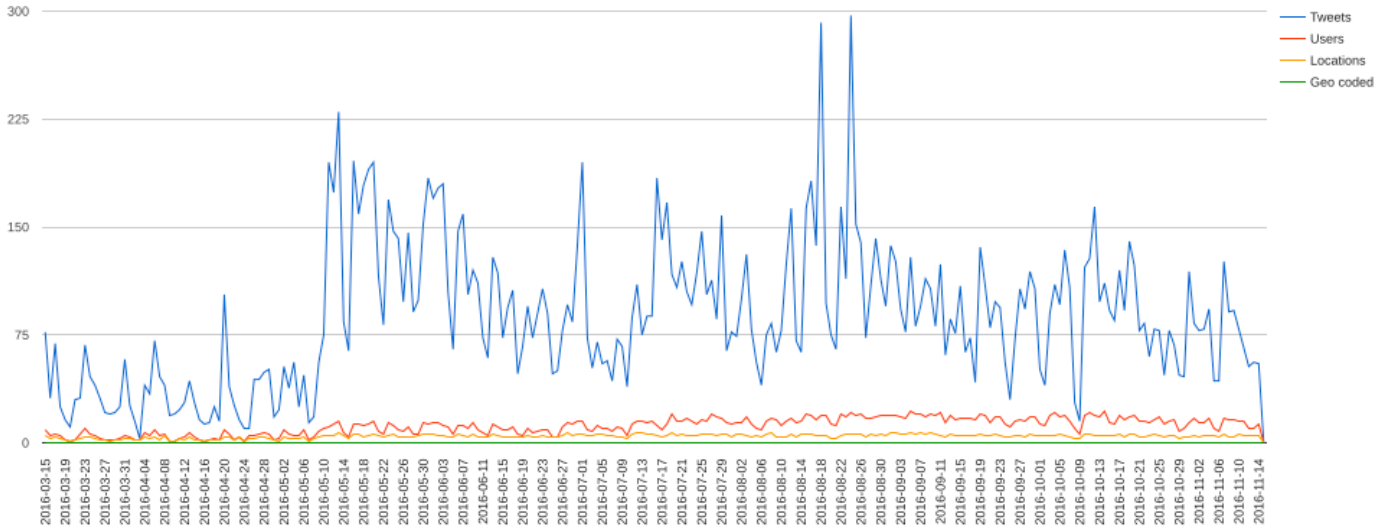
[69] IPI, op. cit.

[70] E.K. Sözeri, 'The rotten politics infecting Turkey's social media', *The Daily Dot*, March 30, 2016, http://www.dailydot.com/layer8/turkey-social-media-yeni-safak-facebook-twitter-manipulation/, (accessed January 4, 2017).

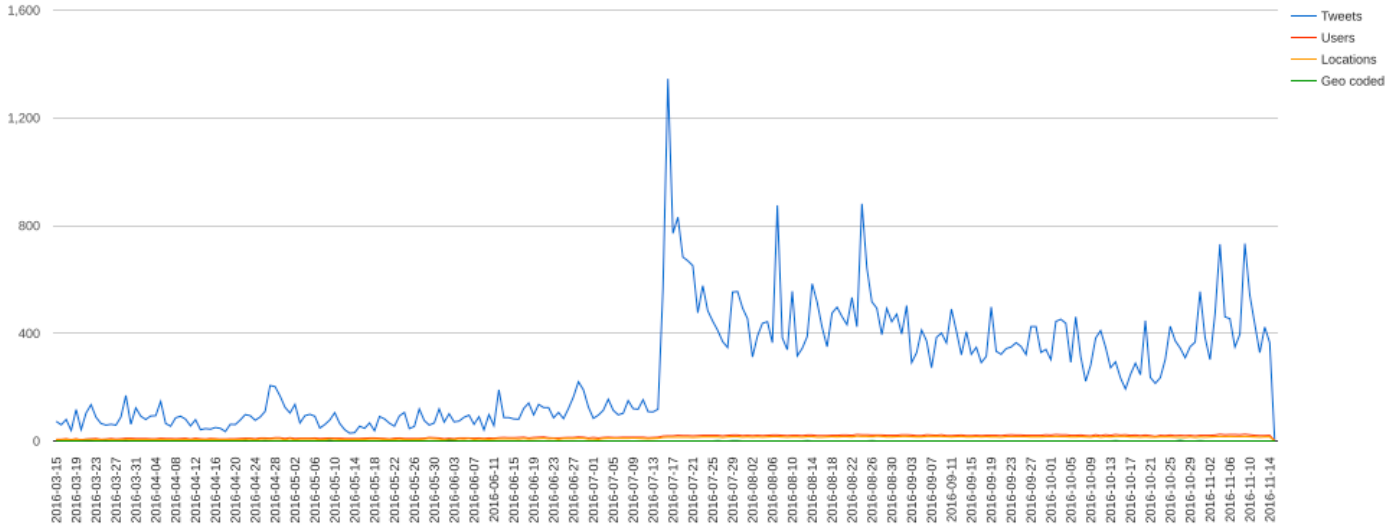
[71] 'JÖH-PÖH hesabının altından Beytüşşebap kaymakamı çıktı', *Sendika.org*, May 25, 2016, https://sendika14.org/2016/05/joh-poh-hesabinin-altindan-beytussebap-kaymakami-cikti/, (accessed January 14, 2017).

[72] Digital Methods Initiative, Twitter Capture and Analysis Toolset. See: E. Borra & B. Rieder, 'Programmed method: developing a toolset for capturing and analyzing tweets', *Aslib Journal of Information Management*, 2014, Vol. 66 Issue: 3, pp.262 – 278, http://dx.doi.org/10.1108/AJIM-09-2013-0094, (accessed January 14, 2017).

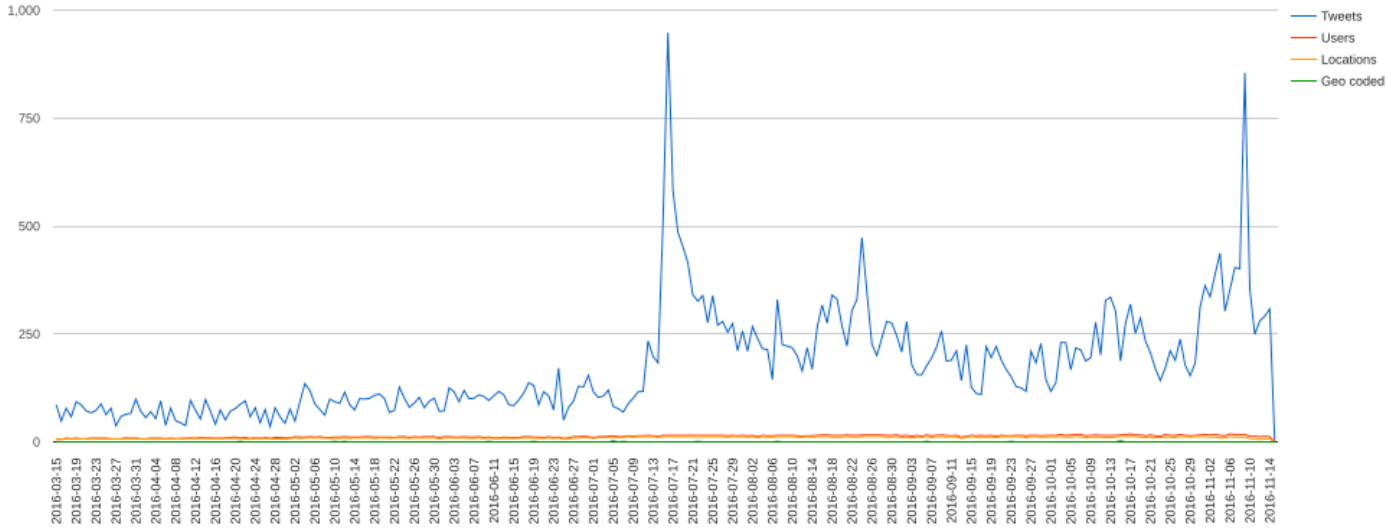
Graph 1: Pro-government accounts engaged in communication, propaganda campaigns



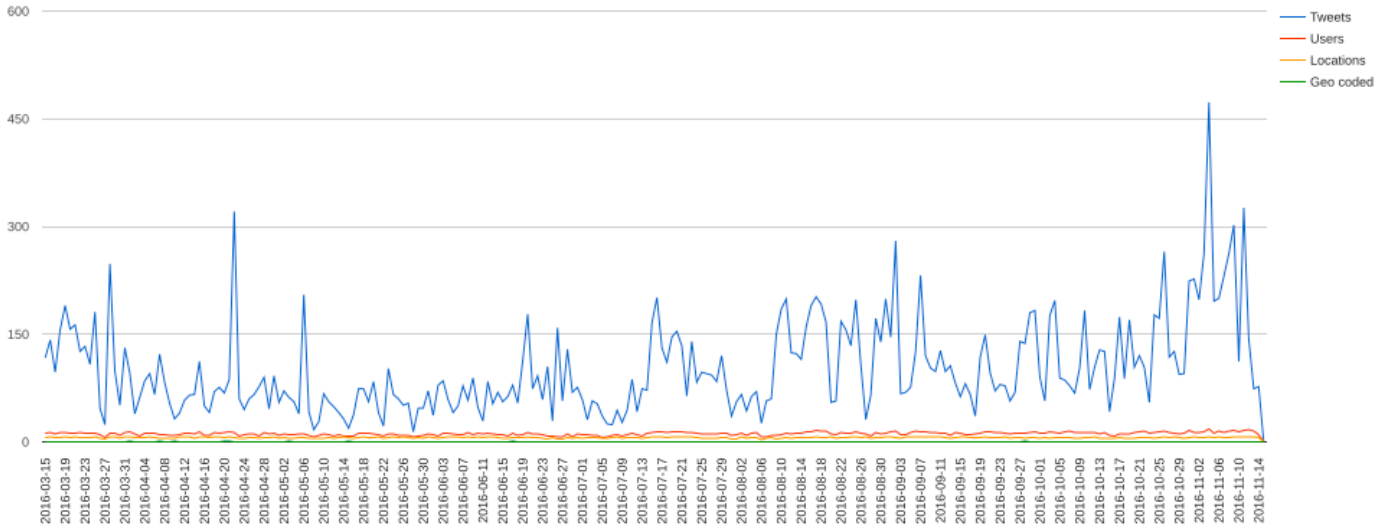
Graph 2: Pro-government trolls



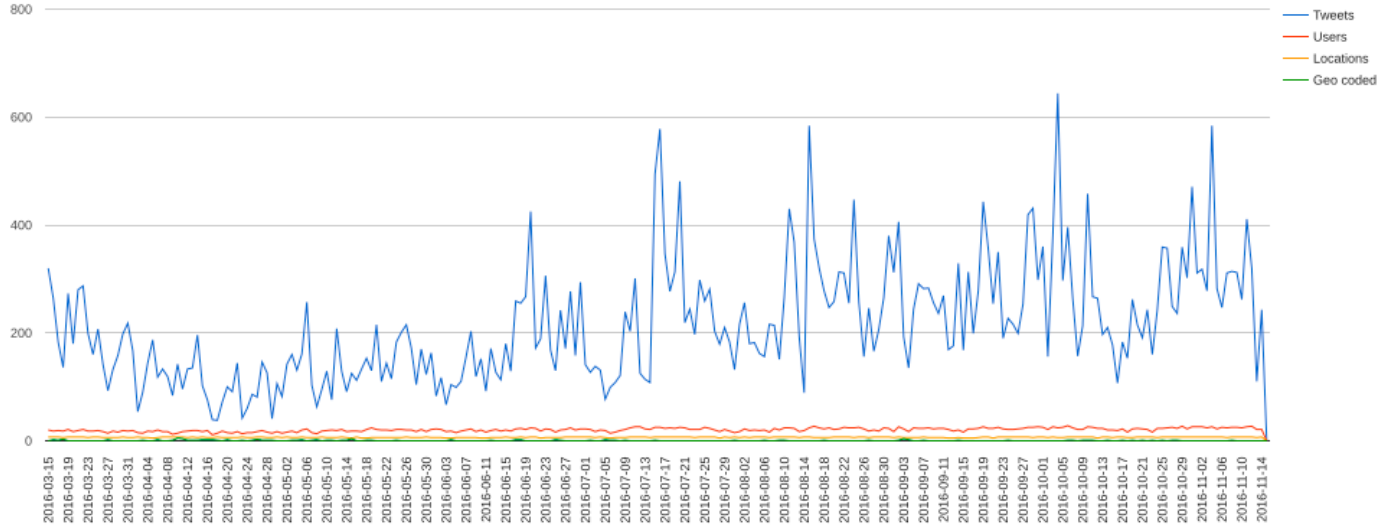
Graph 3: Pro-government journalists



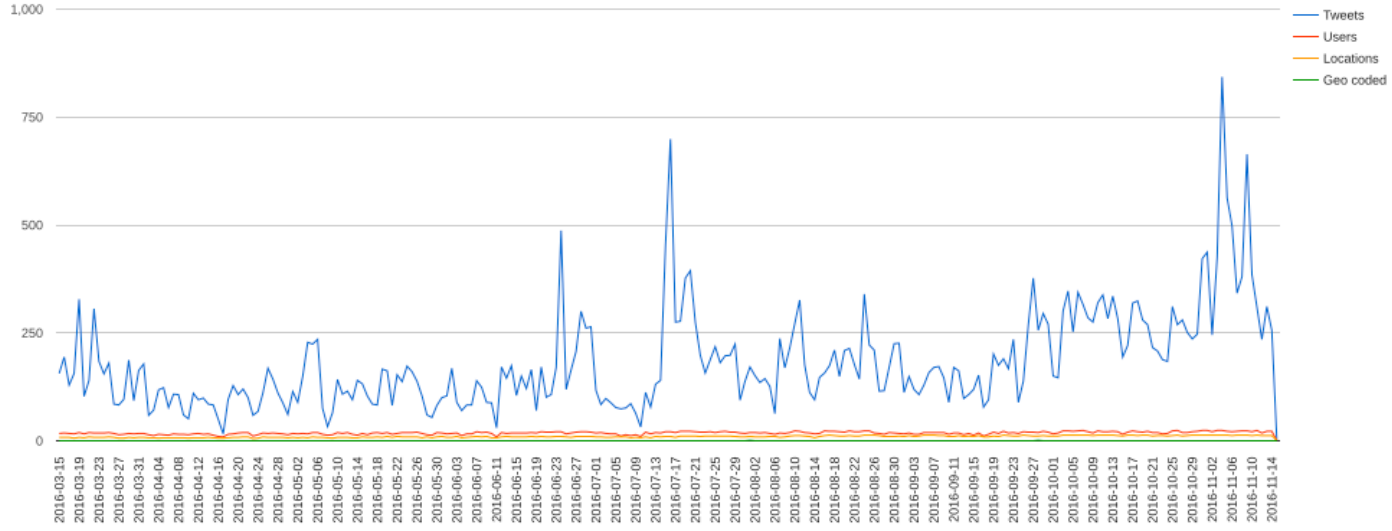
Graph 4: Human rights activists



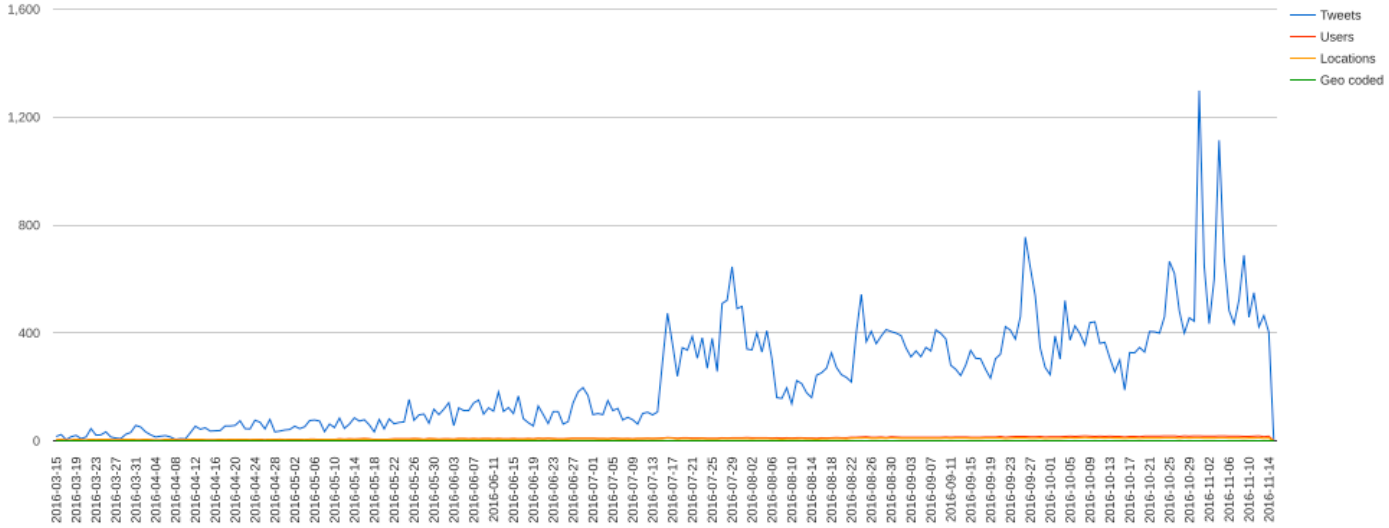
Graph 5: Independent journalists



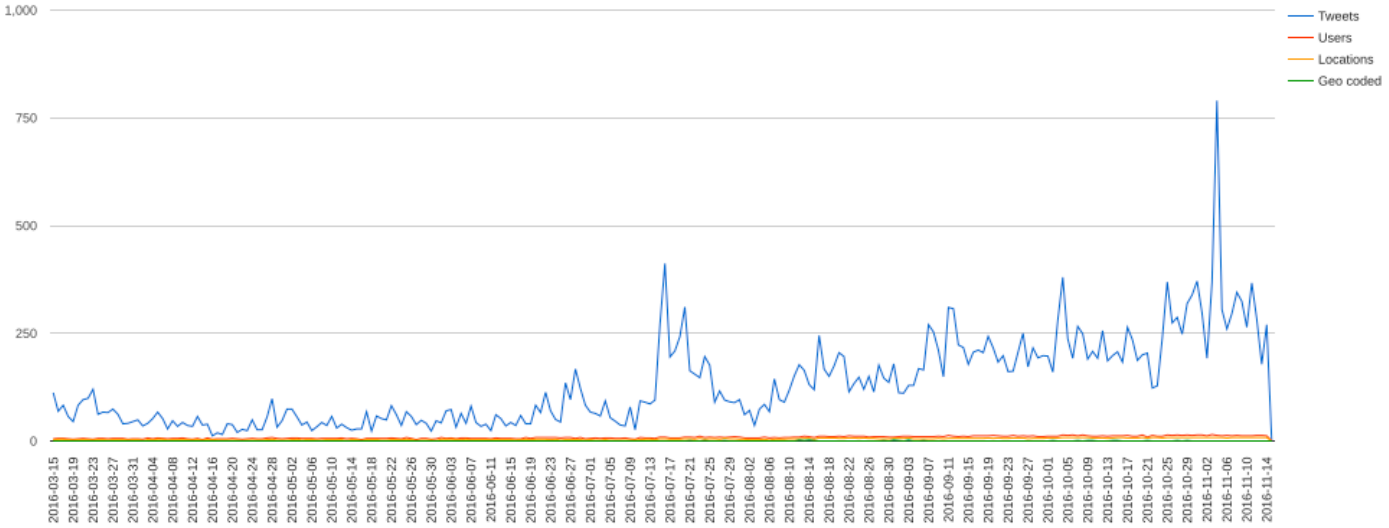
Graph 6: Foreign journalists based in Turkey



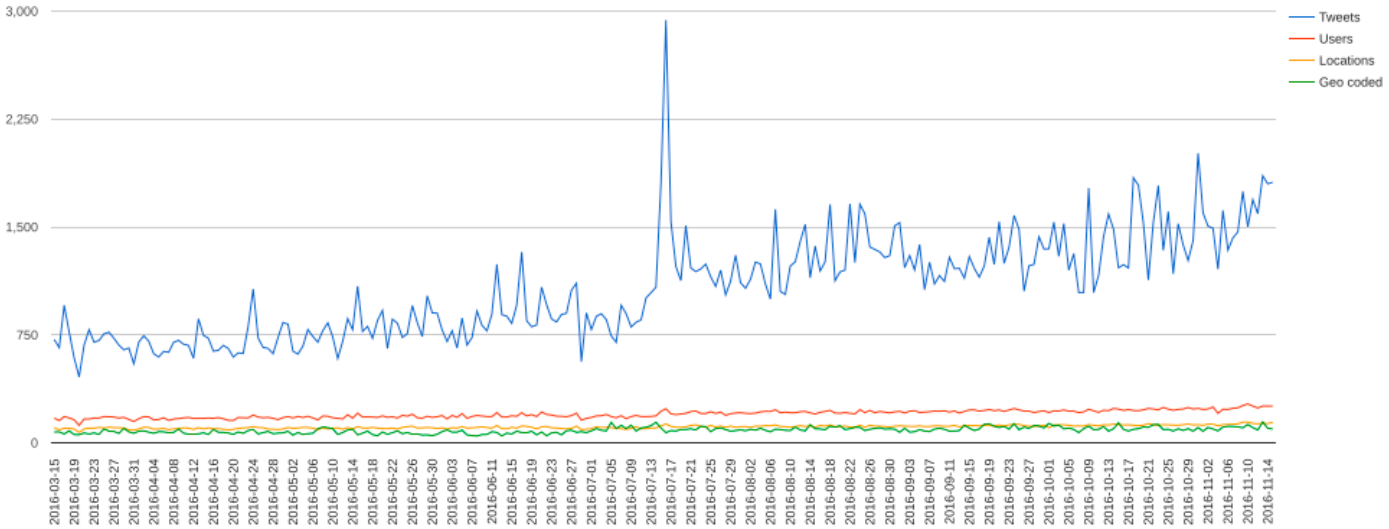
Graph 7: Gulen-affiliated journalists



Graph 8: Pro-HDP accounts



Graph 9: Random users



As seen above, the coup attempt of July 15, 2016 is certainly the most significant incident in the period we analyzed, prompting a strong reaction amongst almost all Turkey-based Twitter users, but especially pro-government trolls (Graph 2) and pro-government journalists (Graph 3). The top-tweeted incidents by pro-government communication and propaganda accounts, on the other hand, include the ouster of Prime Minister Davutoglu (May 5, 2016), PKK attacks (August 18, 2016), and the beginning of Turkish military operations in Syria (August 24, 2016) (Graph 1). This is because these accounts were carrying out communication and mobilization campaigns to garner popular support for Erdogan and his government's policies regarding these political, security- and military-related developments.

Pro-government trolls were most concerned with the coup attempt, Erdogan's massive rally (on August 8), PKK attacks, military operations in Syria, and the arrests of Kurdish deputies (in November) (Graph 2), whereas pro-government journalists tweeted most about the coup attempt and the arrests of Kurdish deputies (Graph 3).

Due to Twitter's limitations on data collection, the pre-coup period is under- represented for other groups analyzed for this research. However, activities of other groups during the post-coup period nonetheless give us some insights into the events they tweeted about. Independent journalists, for example were interested in sharing information about various developments, but most importantly the coup attempt, PKK attacks, closure of independent media outlets, and crackdown on Kurdish politicians (Graph 5). Likewise, foreign journalists based in Turkey tweeted most about the coup attempt and arrests of Kurdish politicians (Graph 6). Human rights activists' and pro-HDP accounts were most concerned with the arrests of Kurdish deputies (Graph 4).

Another important insight provided by this analysis is the overwhelming presence of pro-government users, be it communication and propaganda accounts, partisan journalists or trolls. Comparing the number of tweets posted by various groups, one can observe that pro-government users are the top tweeters regardless of the event in question. Obviously, their objective is to "overwhelm [their] adversaries" with too much information, and to "mobilize their supporters and bind them to the state."[73]

Finally, a curious finding is related to the spike in tweets posted by pro-government users in relation to the U.S presidential election.[74] Soon after Donald Trump was elected, Turkish social media was suddenly flooded with fake news concerning an alleged pedophilia scandal that involved the Clinton campaign.[75] Known as Pizzagate" and originally promulgated by Trump supporters in the U.S, this non-scandal proved to be popular amongst pro-AKP users for a couple of reasons. For example, the AKP supporters sought to dilute the ongoing debate in Turkey concerning a draft bill that would decrease sexual assault sentences, drown out critics' concerns about "child brides,"[76] and hoped to divert attention from the closure of an NGO that focuses on children's rights.[77]

b) The Pelikan network

In May 2016, a curious blog post, titled the "Pelikan Dosyasi" (in a reference to the Hollywood movie *Pelican Brief*) made headlines in Turkish media

[73] E.T. Brooking and P.W. Singer, "War Goes Viral: How Social Media is Being Weaponized." *The Atlantic*, Novemer 2016, p. 79

[74] Previously, pro-AKP media outlets depicted Trump in a negative light because of his Islamophobia and xenophobia. However, in the immediate aftermath of the coup attempt, the portrayal of Trump suddenly turned positive based on the assumption that, if elected, Trump would be willing to extradite Fethullah Gulen, the Muslim cleric whom the Turkish government accuses of masterminding the coup attempt. See, E.K. Sözeri, 'İktidar medyası, İslamofobik Trump'ı nasıl ve neden destekledi', *P24 Blog*, November 13, 2016, http://p24blog.org/yazarlar/1851/iktidar-medyasi--islamofobik-trump-i-nasil-ve-neden-destekledi, (accessed January 14, 2017).

[75] C. Kang, 'Fake News Onslaught Targets Pizzeria as Nest of Child-Trafficking', *The New York Times*, November 21, 2016, https://www.nytimes.com/2016/11/21/technology/fact-check-this-pizzeria-is-not-a-child-trafficking-site.html, (accessed January 14, 2017).

[76] E.K. Sözeri, 'How the alt-right's PizzaGate conspiracy hid real scandal in Turkey', *The Daily Dot*, November 23, 2015, http://www.dailydot.com/layer8/pizzagate-alt-right-turkey-trolls-child-abuse/, (accessed January 14, 2017).

[77] C. Kiper, 'Turkish govt shuts down 370 civic groups, raids offices', *AP*, November 12, 2016, http://bigstory.ap.org/article/6cfa6cb4529044c6bd7eb73339ff08de/turkey-halts-operations-370-civic-groups-raids-offices, (accessed January 14, 2017).

thanks to its unabashed criticism of the then Prime Minister, Ahmet Davutoglu.[78] Penned by a journalist close to Erdogan, the post exposed the ongoing power struggle between the two men. Shortly after the publication of the Pelican Brief, Davutoglu resigned and an Erdogan-loyalist ascended to the premiership. In addition to the intra-party struggles, the blog post also revealed the existence of a network of pro-Erdogan operatives on Twitter— one that is separate from the larger cadre of AK Trolls. Based on the leaked emails of Energy Minister Berat Albayrak, researchers were able to disclose the connections between these operatives, a pro-government columnist and a partisan think-tank, Bosphorus Global.[79] This newly-discovered network of online operatives were found to be running various public communication and information projects via 23 different Twitter accounts, and associated Facebook pages and websites. Most of these projects involved some sort of fact-checking service in several languages that aimed to correct critical coverage of the AKP government found in international media. They also targeted certain journalists and media outlets by "name and shame" tactics, as can be seen in following examples.[80]

Figure 3: @gununyalanlari, a government-linked fact-checking service claims that an article that apeared in Politico is "a lie."[81]

Figure 4: @FactCheckingTR, the English version of the government-linked fact-checking service makes a similar claim[82]

[78] M. Akyol, 'How mysterious new Turkish blog exposed Erdogan-Davutoglu rift', *Al-Monitor*, May 3, 2016, www.al-monitor.com/pulse/originals/2016/05/turkey-rift-between-erdogan-davutoglu.html

[79] E.K. Sözeri, 'Pelikan Derneği: Berat Albayrak, Ahmet Davutoğlu'nu neden devirdi?', *Medium*, November 3, 2016, https://medium.com/@efekerem/pelikan-derneği-berat-albayrak-ahmet-davutoğlunu-neden-devirdi-5fabad6dc7de, (accessed January 14, 2017).

[80] 'We condemn the international media organs and journalists that support military coup in Turkey. Here is a list of them:', *@FactCheckingTR on Twitter*, July 16, 2016, https://twitter.com/FactCheckingTR/status/754412571323723776, (accessed January 14, 2017).

[81] Alev Scott'un "AK Parti Mültecileri Muhalif Şehirlere Gönderiyor" Yalanı, @gununyalanlari on Twitter, April 7, 2016, https://twitter.com/gununyalanlari/status/718166702945472513, (accessed January 14, 2017).

[82] 'Politico falsely claims that AK Party government houses refugees in opposition towns

Figure 5: @FactCheckTR_AR, the Arabic version of the government-linked fact-checking service claims the Politico article in question is "a lie"[83]

One might argue that these Pelikan-affiliated fact-checking services are doing what any government would naturally do, that is communicating its own version of the events. However, in Turkey, these pro-government operatives who run these social media accounts and the so-called fact-checking services are not merely trying to set the record straight. They are also aiming to harass and intimidate journalists as seen in the detention of Dion Nissenbaum, Wall Street Journal's Turkey correspondent. In December 2016, an ISIS video in which two Turkish soldiers were burned alive began to circulate on social media. The AKP government questioned the veracity of the video and prohibited media outlets from reporting even its existence. However, Nissenbaum had shared a screenshot of the video in a tweet and was soon targeted by a member of the Pelikan network. This pro-government operative reported Nissenbaum to the Turkish National Police demanding his "immediate deportation."[84] A week later, Nissenbaum was detained for three days without access to lawyers. Upon his release, he left Istanbul on his own volition.[85]

c) Bots

The flooding of the Turkish Twittersphere with pro-government messages to push away dissidents also relies on the use of bots. According to Norton, Turkey has the highest bot population in the EMEA region (Europe, Middle East, Africa) with Istanbul and Ankara as cities with highest levels of bot infestation. In terms of bot density, Turkey ranks fifth with one bot per every 1,139 internet users.[86] Norton's data does not specify the percentage of bots that are linked to the AKP, however, in 2014 two researchers discovered 18,000 bots that were tweeting pro-AKP messages during the local election campaign.[87] Pro-government accounts have used bots on other occasions as well, such as after bombing attacks,[88] primarily to drown out critical users from online conversations and to push pro-

http://factcheckingturkey.com/refugees/claim-ak-party-government-houses-refugees-opposition-towns-194 @ *POLITICOEurope @AlevScott', @FactCheckingTR on Twitter,* April 6, 2016, https://twitter.com/FactCheckingTR/status/717709319312183296, (accessed January 14, 2017).

[83] « ادعاء: حكومة حزب العدالة والتنمية تُسْكِنُ اللاجئين في المدن المعارضة http://factcheckingturkey.com/ar/refugees/224 @AlevScott POLITICOEurope», *@FactCheckTR_AR on Twitter*, April 29, https://twitter.com/FactCheckTR_AR/status/726065932242657280, (accessed January 14, 2017).

[84] 'Wall Street Journal'ın temsilcisi katliam görseli RT'liyor. Türkiye'deyse derhal sınırdışı edilmeli!!' @ *DionNissenbaum @EmniyetGM, @Filiz_Gunduz on Twitter*, December 22, 2016, https://twitter.com/Filiz_Gunduz/status/812043102588456960, (accessed January 14, 2017).

[85] F. Schwartz and G. Fairclough, 'Wall Street Journal Reporter Dion Nissenbaum Returns to U.S. After Being Detained in Turkey,' *The Wall Street Journal*, December 31, 2016, www.wsj.com/articles/turkish-authorities-detain-wall-street-journal-staff-reporter-dion-nissenbaum-for-2days-1483191134, (accessed January 14, 2017).

[86] https://uk.norton.com/emeabots

[87] E. Poyrazlar, 'Turkey's Leader Bans His Own Twitter Bot Army,' *Vocativ*, March 26, 2014, http://www.vocativ.com/world/turkey-world/turkeys-leader-nearly-banned-twitter-bot-army/, (accessed January 16, 2017)

[88] Ankara Katliamı Sonrası Aktif Olan Botlar: AK Botlar ("Active Bots after the Ankara Massacre: AK Bots"), Hafıza Kolektfi, October 25, 2015, http://web.archive.org/web/20151130041806/http://hafizakolektifi.org/index.php/2015/10/25/ak-botlar, (accessed January 14, 2017).

government hashtags to the top of Trending Topic lists.[89]

d) White hat hackers

In January 2017, the BTK announced that it would set up an "army" of white hat hackers to safeguard Turkey from cyberattacks, and organized an online contest to select qualified candidates.[90] Although the TIB established the National Intervention Center against Cyber Attacks (known by its Turkish acronym USOM) in 2014 and the Ministry of Telecommunications already employs 372 "cyberattack intervention crews," the BTK maintains that there is still a need for an additional "cyber army."[91] However, it is not clear if these white hat hackers will engage in activities other than securing the country's information and telecommunications infrastructure. Given the expansion of online surveillance and suppression in recent years, the absence of a clear-cut job definition does indeed raise concerns.

[89] J. de Medeiros, 'Turkey's Twitter-Bot army and the Politics of Social Media' *entwickler.de*, Juen 30, 2014, https://entwickler.de/online/webmagazin/turkeys-twitter-bot-army-and-the-politics-of-social-media-1153.html (accessed January 19, 2017)

[90] B. Simsek, 'White Hat Hackers Team to Defend Turkey,' *Daily Sabah*, January 14, 2017, http://www.dailysabah.com/turkey/2017/01/14/white-hat-hackers-team-to-defend-turkey (accessed January 19, 2017)

[91] T. Sardan, 'Siber Saldiriya Karsi 372 SOME,' *Milliyet*, January 22, 2016, http://www.milliyet.com.tr/siber-saldiriya-karsi-372-some--gundem-2182421/, (accessed January 19, 2017)

Conclusion

In their analysis of censorship and control of the internet around the globe, Deibert and Rohozinski discuss first, second and third-generation controls. First-generation controls consist of internet filtering and blocking; second-generation controls involve the passing of legal restrictions, content removal requests, technical shutdown of websites, and computer-network attacks; and third-generation controls include warrantless surveillance, the creation of "national cyber-zones," state-sponsored information campaigns, and/or direct physical action to silence individuals or groups.[92]

As the preceding overview of Turkey's internet policy between the late 1990s and the present shows, there has been a marked shift from the use of first to third-generation controls, and from (more) formal and direct controls to (more) informal and indirect practices of suppression. This transformation is largely the result of the Turkish authorities' need to adapt to emerging digital technologies and their affordances such as public deliberation and political engagement. As March Lynch notes in his "authoritarian persistence" thesis, states adapt to the changes unleashed by new communication technologies and learn how to use the new powers of the internet as they go. In response to emerging cultures of critique and new forms of interaction between citizens and the state, authoritarian regimes work constantly to contain the mediated public sphere, and complement their existing filtering, blocking, surveillance systems with new strategies that de-centralize and distribute control across platforms.

Between 2007 and 2013, a period when so-called harmful online content and communications largely transpired on websites, blogs, and social networking and collaborative sites (e.g. YouTube, MySpace, Dailymotion, Vimeo and Blogspot), Turkish courts and administrative entities relied largely on first and second-generation controls. However, in the aftermath of Gezi protests and the corruption scandal in 2013, the AKP government became acutely aware of the role of social media platforms in political engagement and civic mobilization, and in building and expanding of online/offline solidarities. Similar to authoritarian regimes that consider the free flow of information a threat to their hegemony and continuously adapt their media and information management strategies to confine the networked public sphere, the Turkish government too resorted to third-generation controls. In the aftermath of the abortive coup in 2016, the AKP has intensified its attempts at controlling and taming the online public sphere by way of regional internet shutdowns, cloud and VPN restrictions, throttling, data localization schemes, online "snitching" and prosecution, and finally, covert but coordinated propaganda and trolling operations.

The shift from formal, direct, hard forms of control (e.g. legal and technical restrictions) to informal, indirect, soft ones (e.g. throttling, snitching, government-sponsored propaganda campaigns) also points to the emergence of a decentralized and distributed network of online censorship. In the 2000s, online controls were implemented by a centralized group of identifiable entities (TIB, BTK and courts) via identifiable (if not always officially acknowledged) strategies such as banning websites, forbidding words from domain names, and denying access to certain social media content. Beginning in 2013 and escalating since 2016, online controls have been carried out by a decentralized group that includes the BTK, the courts, citizen informants and government-affiliated trolls.

As noted above, the increasing agility and diversity of internet controls is a necessity on the part of authoritarian governments around the globe to maintain and bolster regime stability in the face of new political developments. In this regard, it is important to discuss the recent changes in Turkey's internet policy with reference to those in China and Russia—two authoritarian regimes (to varying degrees) whose online control strategies serve as a blueprint for budding autocrats around the world.

Analyses of China's ICT policies show that Chinese authorities rely on "public-private partnerships" with the technology industry and a combination of control, surveillance and activism. The deployment of paid users to assist the government in "monitoring content, making favorable comments, and pushing discussion toward pro-Party lines" is an indication of the emergence of a proactive censorship

[92] Deibert and Rohozonski "Control and Subversion"

regime as opposed to a reactive one.[93] Similarly, Russia has moved beyond "strategies of 'negative control' of the internet [i.e blocking, censoring, and suppressing the flow of communication] toward strategies of proactive co-optation [i.e. a deceptive blend of control, co-option, and manipulation on social media.]"[94] As Gunitsky notes, the Russian government, prompted by the anti-government protests in 2011-2012, resorted to use social media to maintain regime stability, and to this end, it mobilized its own supporters (military and business elites, regular citizens) and disseminated online propaganda, both of which have complemented each other and enabled the "planting of false information, monitoring of opposition websites, harassment of opposition members, and the shaping of online discourse and public consciousness."[95] Russian authorities also formed "web brigades" of hundreds of thousands of paid users to write positive comments about the government, and thus created a mechanism to "control the boundaries of acceptable online debate" not simply by "blocking dissent but by manipulating it."[96]

[93] S. Chestnut Greitens, 2013, "Authoritarianism Online: What Can We Learn from Internet Data in Nondemocracies?" *Political Science and Politics*, 46:2, p. 265
[94] Gunitsky, p. 42
[95] Gunitsky, op. cit., 46
[96] Gunitsky, op. cit., 47

As our analysis has shown, the Turkish government also opted for a more decentralized set of controls in the post-Gezi and post-coup conjunctures. Not content with the legal, financial and political silencing of critical voices in print and broadcast media, the AKP government directed its attention to the last bastion of free speech in the country, that is the networked online sphere. Buttressing its existing "negative" strategies implemented via the BTK and the courts, it began to devolve responsibility for internet control to partisan journalists, pundits and trolls. Additionally, it secured the active engagement of the Turkish National Police, partisan media outlets and NGOs, and its own voter base to monitor online communications and to file complaints against critical or dissenting websites, Facebook pages, and Twitter users. In the post-coup period, the AKP has opted *not* to develop its new censorship and silencing mechanisms into laws and regulations, a strategy that resonates with the Russian experience.[97] By maintaining a high-level of opacity to administrative and judicial decisions concerning the blocking and banning of content, and the prosecution of users, it has engendered a sense of uncertainty and uneasiness in the online public sphere.

[97] C. Vendil Pallin, 2017. "Internet control through ownership: the case of Russia," *Post-Soviet Affairs*, 33:1, p. 17