Populism & Politics
Article #26

Digital Authoritarianism in Turkish Cyberspace: A Study of Deception and Disinformation by the AKP Regime's AKtrolls and AKbots

IHSAN YILMAZ
BULENT KENES

NOVEMBER 13, 2023

DOI.ORG/10.55271/PP0026

BIO

IHSAN YILMAZ is Research Professor and Chair of Islamic Studies and Inter-cultural Dialogue at the Alfred Deakin Institute for Citizenship and Globalisation (ADI), Deakin University, Melbourne, Australia. He has conducted research on nation-building; citizenship; ethnic-religious-political identities and their securitization (Middle East, Pakistan, Indonesia); minority-majority relations (Australia, Turkey, the UK, and the USA); socio-legal affairs, identities, belonging and political participation of Muslim minorities in the West (the UK, Australia, and the USA); Islam-state-society relations in the majority and minority contexts; global Islamic movements; political Islam in a comparative perspective; Turkish politics; authoritarianization; Turkish diasporas (the UK, Australia, the USA); transnationalism; intergroup contact (Australia); and politics of victimhood (Australia, Turkey).

BULENT KENES (Ph.D.) is an academic and a journalist who has over 25 years of professional experience and founding executive director of European Center for Populism Studies (ECPS). He has managed multiple publications, both in Turkish and English. He has held top editorial positions at various media outlets. Kenes was editor-in-chief of Bugün daily (2006) and founding editor-in-chief of Today's Zaman (2007-2016; the paper was seized on March 4, 2016, by the Erdogan regime and formally closed in July 2016). Kenes was also among the founders of the Stockholm Center for Freedom. He served as voluntary chief editor from 2017-2019.

Funding: **This research was funded by Gerda Henkel Foundation, AZ 01/TG/21, Emerging Digital Technologies and the Future of Democracy in the Muslim World.**

ABSTRACT

This article explores the evolving landscape of digital authoritarianism in Turkish cyberspace, focusing on the deceptive strategies employed by the AKP regime through AKtrolls, AKbots and hackers. Initially employing censorship and content filtering, the government has progressively embraced sophisticated methods, including the weaponization of legislation and regulatory bodies to curtail online freedoms. In the third generation of information controls, a sovereign national cyber-zone marked by extensive surveillance practices has emerged. Targeted persecution of critical netizens, coupled with (dis)information campaigns, shapes the digital narrative. Central to this is the extensive use of internet bots, orchestrated campaigns, and AKtrolls for political manipulation, amplifying government propaganda and suppressing dissenting voices. As Turkey navigates a complex online landscape, the study contributes insights into the multifaceted tactics of Erdogan regime's digital authoritarianism.

By Ihsan Yilmaz & Bulent Kenes

Since the last decade, authoritarian governments have co-opted social media, compromising its potential for promoting individual liberties (Yilmaz and Yang, 2023). In recent years, President Recep Tayyip Erdogan-led Turkish government has staunchly endeavoured to control online platforms and manipulate digital spaces to consolidate power, stifle dissent, and shape public opinion. Given the large online user base and the declining influence of traditional media, the internet has become a crucial platform for opposition voices. In response, President Erdogan's "authoritarian Islamist populist regime" (Yilmaz and Bashirov, 2018) has implemented various measures to regulate and monitor the digital space to suppress dissent (Bellut, 2021).

Turkey's domestic internet policy under the Erdogan regime has shown a convergence towards information control practices observed in countries like Russia and China, despite Turkey's nominal compliance with Euro-Atlantic norms on cyber-security (Eldem, 2020). This convergence is characterized by increasing efforts to establish "digital sovereignty" and prioritize information security, often serving as a pretext for content control and internet censorship (Eldem, 2020). The Erdogan regime takes a neo-Hobbesian view of cyberspace and seeks to exert sovereignty in this realm through various information controls (Eldem, 2020). Under the Erdogan regime, there has been an increase in the surveillance of online activities, leveraging the surveillance and repression tools provided by social media and digital technologies. Once the regime established its hegemony over the state, it expanded its surveillance tactics to govern society.

In Turkey, a combination of actors including riot police, social media monitoring agents, intelligence officers, pro-government trolls, hackers, secret witnesses, informants, and collaborators work together to identify and target individuals deemed "risky." This surveillance apparatus follows the hierarchical structure of the Turkish authoritarian state, with President Erdogan overseeing its developments (Topak, 2019).

The article examines the Turkish government's pervasive use of trolls, internet bots, orchestrated campaigns, and transnational manipulations that have shaped the country's online environment. Social media platforms, especially Twitter, are central to these manipulation efforts in Turkey. While Twitter has taken action against thousands of accounts associated with the ruling party's youth wing, the resistance from the government highlights the significance of these online campaigns.

The use of fake accounts, compromised profiles, and silent bots further deepens the complexities of digital authoritarianism in Turkey. These accounts serve as vehicles for spreading disinformation, astroturfing, and manipulating social media trends. While efforts have been made to identify and remove such accounts, the adaptability of these manipulative actors poses a significant challenge. Many of these bots remain dormant for extended periods, resurfacing strategically to create and promote fake trends while evading conventional detection methods (Elmas, 2023). These software applications play a pivotal role in amplifying government propaganda, countering opposition discourse, and creating an illusion of widespread support. From replicating messages to retweeting content across hundreds of accounts, these automated bots have become instrumental in shaping online narratives and suppressing dissenting voices (Yesil et al., 2017; Eldem, 2023).

Digital Authoritarianism and Information Controls

The Erdogan regime appointed trustee to Zaman daily in Istanbul, Turkey on March 4, 2016. Photo: Shutterstock

Digital authoritarianism is extensive utilization of information control measures by authoritarian regimes to shape and influence the online experiences and behaviors of the public (Howells and Henry, 2021). These regimes have adeptly adapted to the mechanisms of internet governance by exploiting the vast reach of new media platforms. They employ various forms of censorship, both overt and covert, to suppress dissent and control the dissemination of information.

The literature on digital authoritarianism extensively explores how China has effectively utilized digital technology to maintain and strengthen its rule (Polyakova & Meserole, 2019; Dragu & Lupu, 2021; Sherman, 2021). While China relies on sophisticated surveillance systems and targeted persecution of individuals, the people of Russia experience the impact of digital authoritarianism through internet censorship, manipulation of information flow, the spread of disinformation, and the mobilization of trolls and automated bots (Yilmaz, 2023; Timucin, 2021).

In the realm of digital authoritarianism, disinformation has become a favored tool (Diamond, 2021; Tucker et al., 2017). Authoritarian regimes obscure information, engage in deception, and manipulate the context to shape public opinion (Bimber and de Zúñiga, 2020). It is important to note that digital authoritarianism is not a uniform strategy; different regimes adopt various approaches. Some directly restrict access to the internet, while others rely on heavy censorship and disinformation campaigns (Timucin, 2021; Polyakova & Meserole, 2019).

The Russian model of digital authoritarianism operates with subtlety. Manipulating social media networks is easier to accomplish and maintain compared to comprehensive monitoring systems (Timucin, 2021). In these cases, the open nature of social media becomes a double-edged sword, enabling the widespread distribution of both accurate information and misinformation while amplifying voices from various ends of the political spectrum (Brown et al., 2012).

Digital Authoritarianism and Information Controls in Turkey

During the third term of the AKP (Justice and Development Party) in 2011, Turkey witnessed a shift towards increasing populist authoritarianism. Since then, the dissidents and critics of the AKP government have been framed and demonised as the enemies of the Turkish people (Yilmaz and Bashirov, 2018).

Initially, the government targeted conventional media outlets, subjecting them to various tactics employed by President Erdogan (Yanardagoglu, 2018). Many critical media organizations were forced out of business, and their assets were taken over by pro-government entities. The persecutions both preceding and after the state of emergency in 2016 heightened, leading to the confiscation of media groups like the Gulen-linked Samanyolu Group, Koza Ipek Group, and Feza Publications (Timucin, 2021; BBC 2016). These actions effectively created a clientelist relationship between the government and the media, as anti-government entities were closed and transferred or sold to pro-government supporters (Yilmaz and Bashirov, 2018).

The government's dominance over traditional media outlets served as the foundation for Erdogan's digital authoritarianism, granting the government control over the "formal" form of digital media (Timucin, 2021). Faced with limitations in conventional media, the public turned to online sites, alternative media, and social media platforms in search of reliable news and information.

The Gezi Park protests in 2013 marked a significant moment in Turkey's social movements and the role of social media activism. These protests initially started as a peaceful sit-in at Gezi Park to oppose the demolition of trees for a shopping mall construction but quickly escalated into one of the largest civil unrests in Turkey's recent history. During the early days of the protests, traditional media outlets did not provide adequate coverage, leading people to seek alternative sources of information. Social media platforms played a crucial role as a source of news, organization, and political expression, particularly among urban, tech-savvy youth (Yesil et al., 2017). The number of Twitter users in Turkey skyrocketed from an estimated 2 million to 12 million during the protests (Ozturk, 2013; Varnali and Görgülü, 2015). Social media allowed for a more decentralized and inclusive form of communication during the protests, as it facilitated the rapid dissemination of information and bypassed traditional media gatekeepers (O'Donohue et al., 2020).

The corruption scandal in December 2013 was another event where social media played a crucial role in shaping public opinion and disseminating information.

Government opponents utilized social media platforms to share incriminating evidence of corruption involving President Erdogan, his party, and his cabinet. In response, the ruling AKP adopted a heavy-handed approach, detaining Twitter users and implementing bans on platforms such as Twitter and YouTube. The government positioned social media as a threat to Turkey's national unity, state sovereignty, social cohesion, and moral values (Yesil et al., 2017; Kocer, 2015).

In recent years, Turkey has made efforts to assert control over social media platforms and internet service providers. In 2020, a "disinformation law" was introduced, pressuring these entities to remove "disinformation" from online platforms. Proposed changes to Article 19 in 2022 aim to enhance control over the cyber space, granting more powers to the Information and Communication Technologies Authority (BTK) to regulate the internet. These developments indicate Turkey's increasing efforts to curb the flow of information, maintain a favorable narrative, and suppress dissenting voices, potentially impacting freedom of expression and the right to access information in the country.

The increasing level of digital governance in Turkey has manifested in various forms, leading to significant consequences. Content regulation has played a crucial role in the government's efforts to control the internet. Bodies such as BTK have been granted the power to block access to online content deemed threatening. This has created a climate of increased pressure on internet service providers to comply with the state's requests regarding content removal and access to personal user data. Failure to adhere to these obligations can result in penalties or even the revocation of licenses. There are also speculations that service providers may face bandwidth reduction and limitations on advertisements as a means of exerting further control.

Furthermore, cybercrime provisions intended to safeguard against hacking and online harassment have been instrumentalized by the state to gather user information for investigation, prosecution, and cooperation with "international entities." Individuals found guilty of online offenses can be brought to court and punished under specific articles of the Turkish Penal Code.

In summary, the government introduced legal restrictions, content removal requests, website and social media platform shutdowns, prosecution of internet users, state surveillance, and disinformation campaigns. These measures have resulted in a significant decline in internet freedom and the rise of digital authoritarianism in Turkey between 2013 and the controversial coup attempt in July 2016.

Technical Instruments and Surveillance Methods to Monitor and Control Cyberspace

The Erdogan regime has employed various technical instruments and surveillance methods to monitor and control online activities. Reports indicate that Western companies provided spyware tools to Turkish security agencies, which have been in use since at least 2012. These tools include Deep Packet Inspection (DPI) technology, enabling surveillance of online communications, blocking of online content, and redirecting users to download spyware-infected

versions of software like Skype and Avast. Additionally, the Remote-Control System and FinFisher spyware programs are used for extracting emails, files, passwords, and controlling audio and video recording systems on targeted devices (Privacy International, 2014; Yesil et al., 2017; CitizenLab, 2018; AccessNow, 2018).

The Erdogan regime also established a "Social Media Monitoring Unit," a specialized police force responsible for monitoring citizens' social media posts. There is also a group known as AKtrolls, who can act as informants and report social media posts of targeted users to security agencies, potentially leading to arrests. The AKP has also formed a team of "white hat" hackers, ostensibly for enhancing Turkey's cyber-defense. Furthermore, civilian informants have been mobilized for internet surveillance, with ordinary citizens encouraged to spy on each other online, creating a culture of "online snitching" (Yesil et al., 2017). This pervasive surveillance approach, utilizing both software and social-user-based surveillance, creates a climate of self-censorship and vigilance among users (Saka, 2021; Morozov, 2012).

The National Intelligence Organization of Turkey (MİT) has been granted extended surveillance powers, both online and offline, following the post-Gezi Park protests. Law No. 6532 allowed MİT to collect private data and information about individuals without a court order from various entities. The law also granted legal immunity to MİT personnel and criminalized the publication and broadcasting of leaked intelligence information. MİT operates within the authoritarian state's chain of command. Given MİT's lack of autonomy, it is highly likely that the Erdogan regime exploits the agency's expanded powers for unwarranted surveillance, political witch hunts of dissidents, journalists, and even ordinary online users, aiming to suppress any online criticism (Yeşil, 2016) .

In October 2015, the AKP implemented the "Rewards Regulation," which offered monetary rewards to informants who assisted security agencies in the arrest of alleged terror suspects. This measure encouraged journalists, NGOs, and citizens to monitor online communications and report dissenting individuals (Zagidullin et al., 2021).

The Turkish police introduced a smartphone app and a dedicated webpage that allowed citizens to report social media posts they deemed as terrorist propaganda. The main opposition party claimed that the police prepared summaries of proceedings for 17,000 social media users, and they were attempting to locate the addresses of 45,000 others (Eldem, 2023). Consequently, the state of emergency (SoE) decrees following controversial coup attempt in 2016 further tightened the government's control over the internet. Decree 670 granted "all relevant authorities" access to all forms of information, digital or otherwise, about alleged coup suspects and their families. Decree 671 empowered the government to take any necessary measures regarding digital communications provided by ISPs, data centers, and other relevant private entities in the name of national security and public order. Finally, Decree 680 expanded police powers to investigate cybercrime by requiring ISPs to share personal information with the police without a court order (Topak, 2019; Yesil et al., 2017; Eldem, 2023).

Prior to Turkey's presidential and parliamentary elections in 2023, Turkish prosecutors initiated investigations into social media users accused of spreading disinformation aiming to create fear, panic, and turmoil in society. The Ankara Chief Public Prosecutor's Office launched an investigation into the Twitter account holders who allegedly collaborated to spread disinformation, potentially reaching around 40 million social media users (Turkish Minute, 2023).

The Erdogan regime has significantly expanded its online censorship toolkit through legislative amendments passed in October 2022 (HRW, 2023). As an example of the restrictions imposed, on May 14, 2023, Twitter announced that it was restricting access to certain account holders in Turkey to ensure the platform remains available to the people of Turkey.

AKtrolls

The Erdogan regime responded to critical voices on social media during the Gezi Protests by employing political trolls. This strategy of political trolling, whether carried out by humans or algorithms, is closely associated with Russia and has been adopted by AKP's trolls, known as AKtrolls, who exhibit similarities to Kremlin-operated networks. The deep integration of political trolling within the political system and mainstream media in Turkey has been highlighted in a study by Karatas and Saka (2017). These trolling practices are facilitated through the collaboration of political institutions and media outlets. Trolls act as precursors, disseminating propaganda and testing public opinion before mainstream political figures introduce favored populist policies and narratives.

The AKP's troll army was initially established by the vice-chairman of the AKP and primarily consisted of members from AKP youth organizations. Over time, it has grown into an organization of 6,000 individuals, with 30 core members responsible for setting trending hashtags that other members then promote. Many of these trolls are graduates of pro-AKP Imam Hatip schools. It is worth noting that these trolls receive financial compensation, and there are indications that pro-AKP networks provide additional benefits to successful trolls, including entities like TRT (Turkish Radio and Television) and mobile phone operator Turkcell.

The first network map of AKtrolls was provided by Hafiza Kolektifi, a research collective based in Ankara, in October 2015. This map revealed the close connections among 113 Twitter accounts, including not only ordinary trolls but also politicians, advisors to President Erdogan, and pro-government journalists. The map was created based on the analysis of a popular and aggressive troll named @esatreis, who was identified as a youth member of the AKP. By monitoring the users followed by @esatreis using the Twitter Application Programming Interface (API) and conducting in-depth network analysis, two distinct groups were identified. The first group consisted of politicians, Erdogan's advisors, and pro-government journalists, while the second group comprised anonymous trolls using pseudonyms. The study demonstrated that @esatreis acted as a bridge between the troll group and the politicians/journalists, with Mustafa Varank, an advisor to Erdogan and currently the Minister of Industry and Technology, serving as a central connection node between these two groups (Karatas & Saka, 2017).

It was revealed that politicians and state officials maintained their own anonymous troll accounts, in addition to their official ones. Instances have surfaced where AKP officials were caught promoting themselves through fake accounts. For instance, Minister of the Environment and Urbanization Mehmet Ozhaseki and AKP's Bursa Mayor Recep Altepe were exposed for sharing supportive tweets mentioning themselves mistakenly from their official accounts instead of their fake ones. Another case involved AKP deputy Ahmet Hamdi Çamlı, who inadvertently opened his front camera while live-streaming parliamentary discussions with a fake account using a female name (@YesAdeley) and a teenager's profile photo. Within the AKP, different trolls seem to specialize in specific subjects aligned with the party's policies and strategies. For example, accounts such as @WakeUpAttack and @UstAkilOyunlari fabricate conspiracy theories related to international affairs, while @AKKulis shares tweets from state officials and provides updates on AKP's latest news and activities. Another troll account, @Baskentci, shared lists of journalists to be detained and media outlets to be shut down, as well as advanced information on post-coup attempt decisions (Tartanoglu, 2016).

AKP trolls specifically target and disrupt social media users who express opposition to the ruling party, openly identifying themselves as its supporters. While they are known within party circles, they remain anonymous to outsiders. However, some trolls, driven by rewards and recognition within their social networks, choose not to conceal their identities. In fact, Sözeri (2016) describes how certain pro-government journalists themselves act as political trolls and even lead the attacks. It is important to note that political trolls are not necessarily anonymous or isolated individuals. When aligned with a ruling party led by a president with increased powers, many trolls shed their anonymity, and some even threaten legal action when called out as trolls (Saka, 2021). Realizing that such tactics were not improving the AKP's popularity, the party changed its approach just before the 2015 general election by establishing the New Turkey Digital Office, which focused on more conventional forms of online propaganda (Benedictus, 2016).

The proliferation of digital disinformation coordinated networks of fake accounts, and the deployment of political trolls have had a significant impact on online discourse in Turkey, hindering the free expression of critical voices and fostering an environment of manipulation and propaganda. Much like the Russian "web brigades," which consist of hundreds of thousands of paid users who post positive comments about the Putin administration, Erdogan regime also recruited an "army of trolls" to reinforce the declining hegemony of the ruling party shortly after the Gezi Park protests in 2013 (Bulut & Yoruk, 2017). Their objective is to discredit, intimidate, and suppress critical voices, often resorting to labelling journalists and celebrities as "traitors," "terrorists," "supporters of terrorism," and "infidels." Consequently, Twitter has transformed into a medium of government-led populist polarization, misinformation, and online attacks since the Gezi protests (Bulut & Yoruk, 2017). The situation worsened after the events of 2016, exposing critical voices to open cyberbullying by trolls and intensifying their persecution (Saka, 2021).

One prevalent form of political trolling is the deliberate disruption of influential voices on Twitter who contribute to politically critical hashtags or share news related to potential emergencies. Trolls and hackers primarily target professional journalists, opposition politicians, activists, and members of opposition parties. AKtrolls repeatedly attack and disturb these individuals using offensive and abusive language, labelling them as terrorists or traitors, intimidating them, and even threatening arrest. However, ordinary citizens who participate on Twitter with non-anonymous profiles are also vulnerable targets for AKtrolls. Being targeted by trolls often leads to individuals quitting social media, practicing self-censorship, and ultimately participating less in public debates (Karatas & Saka, 2017).

AKtrolls specifically target critical voices that share undesirable content or use specific hashtags. They employ tactics such as posting tweets with humiliating, intimidating, and sexually abusive insults. Doxxing, the act of revealing personal and private information about individuals, including their home addresses and phone numbers, is also a common strategy employed by AKtrolls. In some cases, AKtrolls may have connections to the security forces, particularly the police. Additionally, hacking and leaking private direct messages have been popular tactics used to discredit opposing voices on Twitter. Pro-AKP hackers affiliated with the AKtrolls have targeted numerous journalists. The initial stage often involves hacking into the journalist's Twitter account and posting tweets that apologize to Erdogan for criticism or betrayal. Furthermore, AKtrolls frequently engage in collective reporting to Twitter in an attempt to suspend or block targeted Twitter handles (Karatas & Saka, 2017).

A significant event within the ruling AKP was the forced resignation of then-Prime Minister Ahmet Davutoglu by Erdogan. Prior to his resignation, an anonymous WordPress blog titled the "Pelikan Declaration" emerged, accusing Davutoglu of attempting to bypass Erdogan's authority and making various allegations against him. This declaration was widely circulated by a group of AKtrolls who later became known as the "Pelikan Group." It is worth noting that this group had close ties to a media conglomerate managed by the Albayrak Family, particularly Berat Albayrak, Erdogan's son-in-law and Turkey's former Minister of Economy, as well as his elder brother and media mogul Serhat Albayrak (Saka, 2021).

AKbots

The Erdogan regime extensively utilizes internet bots, which are software applications running automated tasks over the Internet, to support paid AKtrolls (Yesil et al., 2017). Researchers have demonstrated that during the aftermath of the Ankara bombings in October 2015, the heavy use of automated bots played a crucial role in countering anti-AKP discourse. Twitter even took action to ban a bot-powered hashtag that praised President Erdogan, leading Turkish ministers to claim a global conspiracy against Erdogan (Hurriyet Daily News, 2016; Lapowsky, 2015).

The use of automated bots differs from having multiple accounts in terms of scale. The presence of bots becomes noticeable when a message is replicated or retweeted to more than a few hundred other accounts. It is worth noting that as of November

2016, Istanbul and Ankara ranked as the top two cities for AKbot usage, according to the major internet security company Norton (Paganini, 2016; Yesil et al., 2017; Eldem, 2020).

Furthermore, DFRLab (2018) has revealed that many tactics, including doxing (revealing personal information), are employed through cross-platform coordination. It is important to recognize that in the Turkish context, the influence of AKtrolls extends beyond internet platforms and involves close cooperation with conventional media outlets under Erdogan's control (Saka, 2021). In October 2019, DFRLab identified a network of inauthentic accounts that aimed to mobilize domestic support for the Turkish government's fight against the Kurdish People's Protection Units (YPG) in Syria (Grossman et al., 2020). This network involved fabricated personalities created on the same day with similar usernames, several pro-AKP retweet rings, and centrally managed compromised accounts that were utilized for AKP propaganda. The tweets originating from these accounts criticized the pro-Kurdish HDP, accusing it of terrorism and employing social media manipulation. The tweets also targeted the main opposition party, CHP.

Additionally, the accounts promoted the 2017 Turkish constitutional referendum, which consolidated power in Erdogan, and sought to increase domestic support for Turkish intervention in Syria. Some English-language tweets attempted to bolster the international legitimacy of Turkey's offensive in October 2019, praising Turkey for accepting Syrian refugees and criticizing the refugee policies of several Western nations. The dataset of accounts included individuals who appeared to be leaders of local AKP branches, members of digital marketing firms, sports fans, as well as clearly fabricated personalities or members of retweet rings (Grossman et al., 2020).

In 2019, a significant proportion of the daily top ten Twitter trends in Turkey were generated by fake accounts or bots, averaging 26.7 percent. The impact was even higher for the top five Twitter trends, reaching 47.5 percent (Elmas, 2023). State-organized hate speech, trolls, and online harassment often go unchecked (Briar, 2020).

In 2020, Twitter took action to remove over 7,000 accounts associated with the youth wing of the ruling AKP. These accounts were responsible for generating more than 37 million tweets, which aimed to create a false perception of grassroots support for government policies, promote AKP perspectives, and criticize its opponents. Many of these accounts were found to be fake, while others belonged to real individuals whose accounts had been compromised and controlled by AKP supporters. Fahrettin Altun, Erdogan's communications director, issued threats against Twitter for removing this large network of government-aligned fake and compromised accounts (Twitter Safety, 2020; HRW, 2023a).

A study published in the ACM Web Conference 2023 identified Turkey as one of the most active countries for bot networks on Twitter. These networks were found to be pushing political slogans as part of a manipulation campaign leading up to the 2023 elections. Alongside the reactivated bots, the main opposition presidential candidate, Kilicdaroglu, warned about the circulation of algorithmically fabricated audio or

video clips aimed at discrediting him (Karatas & Saka, 2017).

Bots on social media engage in malicious activities such as amplifying harmful narratives, spreading disinformation, and astroturfing. Elmas (2023) detected over 212,000 such bots on Twitter targeting Turkish trends, referring to them as "astrobots." Twitter has purged these bots en masse six times since June 2018. According to Elmas' study, the percentage of fake trends on Twitter varied over time. Between January 2021 and November 2021, the average daily percentage of fake trends was 30 percent. After Twitter purged bots around November 2021, the share of fake trends decreased to 10 percent in March 2022. However, it started to rise again and reached 20 percent by November 2022. As of April 7, 2023, just before the 2023 Turkish election, the attacks continued, and the percentage of fake trends fluctuated between 35 percent and 9 percent (on weekends). Notably, many bots in the dataset were silent, meaning they did not actively post tweets. Instead, they were used to create fake trends by posting tweets promoting a trend and immediately deleting them. This silent behaviour makes it challenging for bot detection methods to identify them, with 87 percent of the bot accounts remaining silent for at least one month (Elmas, 2023).

In May 2023, during the election month, Turkey saw 145 million tweets shared from 12,479,000 accounts, with 23 percent of these identified as bot accounts by the Turkish General Directorate of Security. An examination of the top 10 trending hashtags revealed that 52 percent of accounts using these hashtags were bot accounts (Bulur, 2022). It was also reported that approximately 12,000 Russian- and Hungarian-speaking Twitter accounts had been reactivated, along with reactivated Turkish-speaking accounts, accompanied by numerous bot followers to amplify their posts. Although only 27 percent of the Turkish population is believed to use Twitter, the impact is significant, with 20 percent of the trending topics on Turkish Twitter in 2023 being manipulated and not reflective of public discourse. A dataset covering the period from 2013 to 2023 indicated that 20 to 50 percent of trending topics in Turkey were fake and primarily propelled by bots (Soylu, 2023, Unker, 2023).

Hackers

Photo: Shutterstock

The Erdogan regime's extensive investments in domestic and global information operations, include the recruitment of hackers worldwide. The regime has also established a "white hat" hacker team ostensibly for enhancing Turkey's cyber-defense (Yeşil et al., 2017). However, there are suspicions that this team has been utilized offensively to silence government critics (Cimpanu, 2016).

The private Cihan News Agency, known for its accurate and swift reporting of Turkish election results since the 1990s, faced a significant cyberattack for the first time during the local elections on March 30, 2014, raising concerns about election security (Haber Turk, 2014). Opposition newspapers, including Zaman, Taraf, and Cumhuriyet, which faced similar cyberattacks, pointed to Ankara as the source of these attacks, raising discussions about the state and service providers' negligence and potential involvement (Akyildiz, 2014).

A similar situation recurred during the 2015 general elections when concerns about the Erdogan regime manipulating election results intensified. On the evening of June 7, 2015, during the ballot counting, a cyberattack targeted the Cihan News Agency, disrupting its services. Zaman newspaper reported that the attack was linked to a special team established within TÜBİTAK, with connections to foreign countries established through TÜBİTAK computers and botnet networks used to direct the attacks and obscure the source (Internet Haber, 2015).

Starting from 2009, Erdoganist hackers also targeted numbers of western countries whose politicians expressed anti-Islamic views or criticized Erdogan regime in Turkey (Souli, 2018; Hern, 2017; Space Watch, 2018; Goud, 2018). In a striking illustration of how cyber activities often align with geopolitics, the Turkish hacktivist group Ayyildiz Tim faced accusations of hacking and taking control of the social media accounts of prominent US journalists in 2018. Their aim was to disseminate messages in support of President Erdogan. These cyber incidents unfolded amidst a period of notably strained US-Turkish ties. Additionally, Turkey grappled with an economic crisis, widely attributed to Erdogan's ill-advised economic policies, although he consistently laid the blame on the US. The US-based cybersecurity firm CrowdStrike exposed the activities of Ayyildiz Tim, a group active since 2002. There is evidence indicating potential ties between Ayyildiz Tim and security forces loyal to Erdogan (Space Watch, 2018; Goud, 2018).

In January 2023, a Turkish hacker collective known as "Türk hackteam" initiated a call for cyberattacks targeting Swedish authorities and banks, coupled with a warning, stating, "If you desecrate the Quran one more time, we will begin spreading sensitive personal data of Swedes" (Hull, 2023). Several prominent Swedish websites reportedly suffered temporary outages due to DDoS attacks, with responsibility for these attacks claimed by the Turkish hacker group Türk Hack Team. Identifying themselves as nationalists, they alleged their lack of affiliation with Erdogan, who had previously stated that Sweden should not expect Turkish NATO support after the Quran incident (Skold, 2023).

Meanwhile, in the lead-up to the 2023 presidential elections, Turkey's primary opposition leader and presidential candidate, Kilicdaroglu, made allegations that the ruling AKP had engaged foreign hackers to orchestrate an online campaign against him, employing fabricated videos and images (Turkish Minute, 2023a).

Demonstrating the Erdogan regime's keen interest in hacking endeavors, an annual event known as "Hack Istanbul" has been hosted by Turkey since 2018. This unique competition challenges hackers worldwide with sophisticated real-world cyberattack scenarios crafted under the guidance of leading global experts (Hurriyet Daily News, 2021). The Turkish Presidency's Digital Transformation Office has been responsible for organizing these hacking competitions, which offer substantial financial rewards. Furthermore, the regime has initiated Cyber Intelligence Contests as part of its training campaigns, effectively expanding the pool of individuals with cybersecurity skills (Cyber Intelligence Contest, 2021).

CONCLUSION

The evolution of information controls in Turkey began with first-generation techniques, such as censorship and content filtering, aimed at restricting access to specific websites and online platforms. However, as technology advanced, the government adopted more sophisticated methods. One prevalent tool has been the instrumentalization of legislation, through which laws have been enacted to curtail online freedoms and enable state surveillance. Additionally, regulatory bodies, originally intended to ensure fair practices, have been weaponized to enforce censorship and impose restrictions, eroding the independence of online platforms. Furthermore, the Turkish government has resorted to tactics like shutdowns, throttling, and content removal requests to suppress dissenting voices and control the flow of information.

In the third generation of information controls, Turkey has focused on establishing a sovereign national cyber-zone characterized by extensive surveillance practices. Advanced technologies have been employed to monitor online activities, creating a pervasive atmosphere of surveillance and curtailing privacy rights. Critical netizens, including activists, journalists, and dissidents, have faced targeted persecution, enduring harassment, intimidation, and legal prosecution to silence opposition and stifle open discourse. Moreover, regime-sponsored (dis)information campaigns have played a significant role in shaping the digital narrative.

Central to the concept of digital authoritarianism in Turkey is the extensive deployment of internet bots and automated tools. The use of internet bots, fake accounts, and orchestrated campaigns for political manipulation is indeed pervasive in Turkey, particularly in shaping public opinion, supporting government policies, and undermining political opponents. Numerous studies have revealed the extensive deployment of automated bots by the Erdogan regime and its supporters to amplify government propaganda, counter anti-government narratives, and create a false perception of grassroots support.

The deployment of individuals known as "AKtrolls" has been used to disseminate pro-government propaganda and attack dissenting voices. Automated bots have been utilized to amplify certain narratives while suppressing opposing viewpoints, distorting the digital discourse, and undermining the integrity of online discussions.

As the Turkish political landscape evolves, the role of social media in shaping public opinion and electoral outcomes remains a critical concern. The elections intensified the battle for online influence, with the government attempting to purchase accounts and engage with dark web groups. The landscape of online manipulation in Turkey is further complicated by the prevalence of fake accounts, compromised profiles, and silent bots that intermittently generate and promote false trends. Silent accounts, which quickly delete tweets, evade detection, making it challenging to identify them.

Additionally, the manipulation of social media in Turkey has a transnational dimension, with instances of foreign interference and coordinated campaigns coming to light. The use of extensive networks of fake or compromised accounts

to amplify certain political views or spread false information on social media has become increasingly prevalent, particularly during politically sensitive periods like elections. Many of these coordinated networks are dedicated to promoting pro-Erdogan perspectives, and the regime occasionally presents their artificial presence as evidence of grassroots support for its policies.

REFERENCES

— (2014). "The right to privacy in Turkey." Privacy International. https://privacyinternational.org/sites/default/files/2017-12/UPR_Turkey_0.pdf

— (2014). "Cihan Haber Ajansı'ndan 'siber saldırı' açıklaması." Haber Turk. March 30, 2014. https://www.haberturk.com/medya/haber/934450-cihan-haber-ajansindan-siber-saldiri-aciklamasi (accessed on November 2, 2023).

— (2015). "Cihan haber ajansını kim hacledi, olay iddia." Internet Haber. June 7, 2015. https://www.internethaber.com/cihan-haber-ajansini-kim-hacledi-olay-iddia-793015h.htm (accessed on November 2, 2023).

— (2016). "Zaman newspaper: Seized Turkish daily 'now pro-government'." BBC. March 6, 2016. https://www.bbc.com/news/world-europe-35739547 (accessed on May 11, 2023).

— (2016). "Turkish Ministers Accuse Twitter of Plotting against Erdoğan," Hurriyet Daily News. March 30, 2016. http://www.hurriyetdailynews.com/turkish-ministers-accuse-twitter-of-plotting-against-erdogan-97106 (accessed on May 11, 2023).

— (2018). "Turkish Hacktivist Group Ayyildiz Tim Hijack U.S. Journalist Social Media Account In Support Of Erdogan." Space Watch. https://spacewatch.global/2018/08/turkish-hacktivist-group-ayyildiz-tim-hijack-us-journalist-social-media-account-in-support-of-erdogan/ (accessed on November 1, 2023).

— (2018). "Bad Traffic: Sandvine's Packet Logic devices used to deploy government spyware in Turkey and redirect Egyptian users to affiliate ads?" CitizenLab. March 9, 2018. https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/ (accessed on May 18, 2023).

Bellut, Daniel. (2021). "Turkish government increases pressure on social media." DW. September 9, 2021. https://www.dw.com/en/turkish-government-increases-pressure-on-social-media/a-59134848 (accessed on May 15, 2023).

— (2018). "Alert: Finfisher changes tactics to hoot critics." AccessNow.

— (2018). "#TrollTracker: Journalist Doxxed by American Far Right," DFRLab, Medium (blog), June 17, 2018. https://medium.com/dfrlab/trolltracker-journalist-doxxed-by-american-far-right-7881f9c20a16 (accessed on May 11, 2023).

— (2020). "Disclosing networks of state-linked information operations we've removed," Twitter Safety, June 12, 2020.

https://blog.twitter.com/en_us/topics/company/2020/information-operations-june-2020 (accessed on May 13, 2023).

— (2021). "Registrations open for Hack Istanbul 2021 contest." Hurriyet Daily News. May 6, 2021. https://www.hurriyetdailynews.com/registrations-open-for-hack-istanbul-2021-contest-164490 (accessed on November 2, 2023).

— (2021). "Cyber Intelligence Contest." The Digital Transformation of the Presidency.https://cbddo.gov.tr/projects/4726/cyberintelligencecontest/ (accessed on November 2, 2023).

— (2023). "13 detained ahead of elections over defamation alleged by former presidential candidate," Turkish Minute, May 13, 2023. https://www.turkishminute.com/2023/05/13/13-detained-ahead-of-elections-over-defamation-alleged-by-former-presidential-candidate/ (accessed on May 13, 2023).

— (2023a). "Kılıçdaroğlu says Erdoğan gov't hired foreign hackers for online campaign against him." Turkish Minute. May 5, 2023. https://www.turkishminute.com/2023/05/05/kilicdaroglu-says-erdogan-govt-hired-foreign-hackers-for-online-campaign-against-him/ (accessed on November 1, 2023).

— (2023). "Turkey's Control of the Internet Threatens Election." Human Rights Watch (HRW). May 10, 2023. https://www.hrw.org/news/2023/05/10/turkeys-control-internet-threatens-election (accessed on May 12, 2023).

— (2023a). "Questions and Answers: Turkey's Control of the Internet and the Upcoming Election." Human Rights Watch (HRW). May 10, 2023. https://www.hrw.org/news/2023/05/10/questions-and-answers-turkeys-control-internet-and-upcoming-election#_Toc134065370 (accessed on October 29, 2023).

Akyildiz, Emir. (2014). "TİB ve Telekom saldırıyı seyretti." Haber Vesaire. March 31, 2014. https://www.habervesaire.com/039-tib-ve-telekom-saldiriyi-seyretti-039/ (accessed on November 2, 2023).

Benedictus, Leo. (2016). "Invasion of the troll armies: from Russian Trump supporters to Turkish state stooges," The Guardian, November 6, 2016. https://www.theguardian.com/media/2016/nov/06/troll-armies-social-media-trump-russian(accessed on May 13, 2023).

Bimber, Bruce and Homero Gil de Zúñiga. (2020). "The Unedited Public Sphere." New Media and Society 22: 700–15.

Briar, Narîn. (2020). "Negligent Social Media Platforms Breeding Grounds for Turkish Nationalism, Hate Speech," The Armenian Weekly, October 29, 2020. https://armenianweekly.com/2020/10/29/negligent-social-media-platforms-breeding-grounds-for-turkish-nationalism-hate-speech/ (accessed on May 18, 2023).

Brown, H.; E. Guskin & A. Mitchell. (2012). "The role of social media in the Arab uprisings." Pew Research Center. 28.

Bulur, Sertac. (2022). "EGM: Mayıs'ta 145 milyon tweet paylaşılan hesapların yüzde 23'ü bot hesap." Anadolu Ajansı. June 7, 2022. https://www.aa.com.tr/tr/gundem/egm-mayista-145-milyon-tweet-paylasilan-hesaplarin-yuzde-23u-bot-hesap/2607433 (accessed on October 23, 2023).

Bulut E. & E. Yoruk. (2017). "Digital populism: Trolls and political polarization of Twitter in Turkey," International Journal of Communication. 11: 4093–4117.

Cimpanu, Catalin. (2016). "Turkey Wants to Build Army of Hackers." Bleeping Computer. December 30, 2016. https://www.bleepingcomputer.com/news/government/turkey-wants-to-build-army-of-hackers/ (accessed on November 2, 2023).

Diamond, Larry. (2021). "Rebooting Democracy." Journal of Democracy. 32: 179–83;

Dragu, Tiberiu & Yonatan Lupu. (2021). "Digital authoritarianism and the future of human rights." International Organization. 75(4), 991-1017;

Ebert H. & T. Maurer. (2013). "Contested cyberspace and rising powers," Third World Quarterly. 34(6), 1054–1074. doi:10.1080/01436597.2013.802502.

Eldem, Tuba. (2020). "The Governance of Turkey's Cyberspace: Between Cyber Security and Information Security." International Journal of Public Administration. Vol. 43, No. 5, 452–465 https://doi.org/10.1080/01900692.2019.1680689

Elmas, Tugrulcan. (2023). "Analyzing Activity and Suspension Patterns of Twitter Bots Attacking Turkish Twitter Trends by a Longitudinal Dataset." ArXiv. April 16, 2023. https://arxiv.org/pdf/2304.07907.pdf

Goud, Naveen. (2018). "Turkey hackers sneak into social media accounts of US Journalists." Cyber Security Insiders. https://www.cybersecurity-insiders.com/turkey-hackers-sneak-into-social-media-accounts-of-us-journalists/ (accessed on November 1, 2023).

Grossman, Shelby; Fazil Alp Akis, Ayça Alemdaroğlu, Josh A. Goldstein & Katie Jonsson. (2020). "Political Retweet Rings and Compromised Accounts: A Twitter Influence Operation Linked to the Youth Wing of Turkey's Ruling Party," Stanford Internet Observatory, June 11, 2020.

Hern, Alex. (2017). "Twitter accounts tweet swastikas and pro-Erdoğan support in massive hack." The Guardian. March 15, 2017. https://www.theguardian.com/technology/2017/mar/15/twitter-turkey-accounts-hack-tweet-swastikas-pro-erdogan (accessed on November 1, 2023).

Howells, Laura and Laura A. Henry. (2021). "Varieties of Digital Authoritarianism: Analyzing Russia's Approach to Internet." Governance Communist and Post-Communist Studies. 54: 1–27.

Hull, Justina. (2023). "Turkiskt hackerforum manar till attacker mot svenska banker." SVT. January 27, 2023. https://www.svt.se/nyheter/inrikes/turkiskt-hackerforum-manar-till-attacker-mot-sverige (accessed on November 1, 2023).

Karataş, Duygu & Erkan Saka. (2017). “Online political trolling in the context of post-Gezi social media in Turkey.” International Journal of Digital Television. (2017). Volume 8 Number 3. doi: 10.1386/jdtv.8.3.383_1

Kocer, Suncem. (2015). “From the ‘Worst Menace to Societies’ to the ‘Robot Lobby’: A Semantic Views of Turkish Political Rhetoric on Social Media.” In: Lemi Baruh & Banu Baybars Hawks (Eds.). New Media Politics: Rethinking Activism and National Security in Cyberspace Account. Newcastle upon Tyne: Cambridge Scholars Publishing.

Lapowsky, Issie. (2015). “Why Twitter Is Finally Taking a Stand against Trolls.” Wired, April 21, 2015. https://www.wired.com/2015/04/twitter-abuse/ (accessed on May 11, 2023).

Morozov, Evgeny. (2012). The Net Delusion: The Dark Side of Internet Freedom. New York: Public Affairs.

O’Donohue, Andrew; Max Hoffman & Alan Makovsky. (2020). “Turkey’s Changing Media Landscape.” CAP. June 10, 2020. https://www.americanprogress.org/article/turkeys-changing-media-landscape/ (accessed on May 18, 2023).

Ozturk, Ozgur. (2013) “Gezi olaylarının Twitter kullanıcı sayısını arttırdı.” Hürriyet, December 8, 2013. http://www.hurriyet.com.tr/gezi-olaylarinin-twitter-kullanici-sayisini-arttirdi-25306778 (accessed on May 14, 2023).

Paganini, Pierluigi. (2016). “Which Are Principal Cities Hostages of Malicious Botnets?” Security Affairs. October 6, 2016. https://securityaffairs.co/wordpress/51968/reports/botnets-geography.html (accessed on May 11, 2023);

Polyakova, Anna & Chris Meserole. (2019). “Exporting digital authoritarianism: The Russian and Chinese models,” Policy Brief, Democracy and Disorder Series. Washington, DC: Brookings. 1-22.

Saka, Erkan. (2021). “Networks of Political Trolling in Turkey after the Consolidation of Power Under the Presidency” (pp. 240-255). In: Digital Hate. The Global Conjuncture of Extreme Speech. Indiana University Press. https://iupress.org/9780253059253/digital-hate/

Sherman, Justin. (2021). “Digital Authoritarianism and Implications for US National Security,” The Cyber Defense Review. 6:1. 107- 118.

Skold, Henrik. (2023). “Turkiska hackergruppens nya hot: Då släpper vi känslig data om svenskar.” SVT. Februari 1, 2023. https://www.svt.se/nyheter/utrikes/efter-koran-branningen-och-nato-turkiska-hackergruppens-nya-hot-da-slapper-vi-kanslig-data-om-svenskar (accessed on November 1, 2023).

Souli, Sarah. (2018). “Turkey’s band of pro-Erdoğan hackers keep trolling Europe.” Vice. March 17, 2018.

https://www.vice.com/en/article/wj7enx/turkeys-band-of-pro-erdogan-hackers-keep-trolling-europe (accessed on November 1, 2023).

Soylu, Ragip. (2023). "Turkey elections: Thousands of Russian Twitter accounts reactivated in Turkish." Middle East Eye. April 18, 2023. https://www.middleeasteye.net/news/turkey-elections-thousands-russian-speaking-accounts-activated-twitter (accessed on October 17, 2023).

Sozeri, Ceren. (2016)."Trol gazeteciliği." Evrensel, September 18, 2016. https://www.evrensel.net/yazi/77506/trol-gazeteciligi (accessed on May 11, 2023).

Tartanoglu, Sinan. (2016). "Muhtar İstihbarat Teşkilatı [Muhtar Intelligence Agency]," Cumhuriyet. December 23, 2016. http://www.cumhuriyet.com.tr/haber/siyaset/649959/Muhtar_istihbarat_Teskilati.html (accessed on May 18, 2023).

Timucin, Fatma. (2021). 8-Bit Iron Fist: Digital Authoritarianism in Competitive Authoritarian Regimes: The Cases of Turkey and Hungary. (Master's thesis, Sabanci University, Istanbul, Turkey, 2021). https://research.sabanciuniv.edu/42417/ (accessed on May 11, 2023).

Topak, Ozgün E. (2019). "The authoritarian surveillant assemblage: Authoritarian state surveillance in Turkey." Security Dialogue. 50: 454–72.

Tucker, Joshua A.; Yannis Theocharis, Margaret E. Roberts, and Pablo Barberá. (2017). "From Liberation to Turmoil: Social Media and Democracy." Journal of Democracy. 28: 46–59.

Unker, Pelin. (2023). "Twitter'da beş gündem etiketinden biri sahte." DW Turkce. May 12, 2023. https://www.dwturkce.com/tr/twitterda-seçim-manipülasyonu-beş-gündem-etiketinden-biri-sahte/a-65345776 (accessed on October 17, 2023).

Varnalı K. and V. Görgülü. (2015). "A social influence perspective on expressive political participation in Twitter: The case of #occupyGezi." Information, Communication & Society. 18(1): 1–16.

Yanardagoglu, Eylem. (2018). "Communication as Political Action: Gezi Park and Online Content Producer." In: Alternative Media in Contemporary Turkey: Sustainability, Activism, and Resistance. Murat Akser & Victoria McCollum (eds.). Rowman & Littlefield Publishers.

Yeşil, Bilge. (2016). Media in New Turkey: The Origins of an Authoritarian Neoliberal State. Champaign: University of Illinois Press.

Yesil, Bilge; Efe Kerem Sözeri & Emad Khazraee. (2017). "Turkey's Internet Policy After the Coup Attempt: The Emergence of a Distributed Network of Online Suppression and Surveillance." Internet Policy Observatory. February 28, 2017. https://repository.upenn.edu/internetpolicyobservatory/22 (accessed on May 11, 2023).

Zagidullin, Marat; Aziz, Nergis and Kozhakhmet, Sanat. (2021). "Government policies and attitudes to social media use among users in Turkey: The role of awareness of policies, political involvement, online trust, and party identification." Technology in Society. https://doi.org/10.1016/j.techsoc.2021.101708

Yilmaz, Ihsan. (2023). "Digital Authoritarianism and Religion in Democratic Polities of the Global South." In: Ihsan Yilmaz (eds.), Digital Authoritarianism and Its Religious Legitimization: The Cases of Turkey, Indonesia, Malaysia, Pakistan, and India. Singapore: Palgrave Macmillan.

Yilmaz, Ihsan & Fan Yang. (2023). "Digital Authoritarianism and Religious Populism in Turkey." In: Ihsan Yilmaz (eds.) Digital Authoritarianism and Its Religious Legitimization: The Cases of Turkey, Indonesia, Malaysia, Pakistan, and India. Singapore: Palgrave Macmillan.

Yilmaz, Ihsan and Galib Bashirov. (2018). "The AKP after 15 years: Emergence of Erdoganism in Turkey." Third World Quarterly 39: 1812–30.

ECPS
EUROPEAN CENTER for
POPULISM STUDIES

THIS ARTICLE IS AVAILABLE FOR FREE DOWNLOADING AT

https://www.populismstudies.org/digital-authoritarianism-in-turkish-cyberspace-a-study-of-deception-and-disinformation-by-the-akp-regimes-aktrolls-and-akbots/

EUROPEAN CENTER FOR POPULISM STUDIES (ECPS)

ADRESS: 155 Wetstraat / Rue De La Loi 1040 Brussels, Belgium
EMAIL: ecps@populismstudies.org
PHONE: +32 24658318

WWW.POPULISMSTUDIES.ORG