


The Moshe Dayan Center  
for Middle Eastern and African Studies



TEL AVIV UNIVERSITY

# TURKEYSCOPE

INSIGHTS ON TURKISH AFFAIRS

EDITORS: HAY EYTAN COHEN YANAROCAK & CENG SAGNIC

**Vol. 2, No. 6, May 2018**

## **From the Editors**

Dear Friends,

The Moshe Dayan Center for Middle Eastern and African Studies is proud to present the May 2018 issue of our monthly publication, Turkeyscope. In this issue, Dr. Tal Pavel, head of Cybersecurity Studies of the Academic College of Tel Aviv-Yaffo, and Dr. Hay Eytan Cohen Yanarocak contributed with an article on Turkish cyber policy. While emphasizing the importance of cyber warfare as a new emerging instrument for challenging states' national security, the article highlights the remarkable events that revealed Turkey's vulnerabilities in the field and seeks to address the current Turkish cyber policy to cope with these threats.

Liane Silver contributed to this issue as assistant editor.

## Turkey's Test with Cyberspace

Dr. Tal Pavel and Dr. Hay Eytan Cohen Yanarocak

Cyber security threats have manifested into serious national security threats challenging state sovereignty. Social-media-promoted riots, hacks, and information leaks have disrupted states' abilities to act through psychological warfare – an already apparent result of this new arena of cyber warfare.

Similar to other states in the Middle East, Turkey has experienced the impact of cyberspace through social-media-originated mass demonstrations and many other small- to large-scale cyber incursions.

The Gezi Park protests, which took place in Istanbul in May-August 2013, are considered a milestone in Turkish political history. Since institutionalized media in Turkey censored the police aggression that occurred during anti-government protests in Istanbul's infamous Gezi Park, many Turkish citizens turned to social media as their sole source of information. By using Twitter, Facebook, and YouTube, ordinary Turks were able to circumvent the state-imposed censorship. Thanks to smart phones, this new social phenomenon spread like an epidemic among the ordinary people during the anti-government protests of 2013 and in successive years. The simplicity of taking pictures, uploading, and commenting via various platforms such as Twitter turned many ordinary citizens into amateur journalists, thus damaging the state's monopoly over the flow of information. Although the Gezi Park riots came to an end in August of the same year, the event caused a significant shift in the mindset of the Turkish people.

Following the Gezi Park protests, the "December 17, 2013 Corruption Scandal" appeared as the second wave of this tsunami of social-media-linked flow of uncontrolled information. Phone recordings of senior government officials leaked through YouTube and Twitter rang the alarm bells for the Turkish government. On February 6, 2014, the Turkish parliament passed the famous "Internet Bill," which was later ratified by the former President Abdullah Gül on February 20. The bill allowed the Turkish government to store the data of Internet users for two years while the Directorate of Telecommunication and Communication (Telekomunikasyon ve İletişim Başkanlığı – TİB) was given the jurisdiction to shut down any internet site within four hours upon appeal without a court ruling. The Turkish government began to monitor social media, and dozens of users were apprehended as a result of initial online investigations. Alongside the deterrence this act created against social media users, Ankara also began to pressure Twitter to erase tweets that were deemed anti-government. Erdoğan's March 20, 2014 speech in Bursa, where he openly threatened to eradicate Twitter in Turkey altogether, reflected the *zeitgeist*.<sup>1</sup>

This virtual world served not only as the platform for criticizing the government but also as a vehicle for more sophisticated players to launch cyber attacks against Turkey. In March 2014, Istanbul and many other major cities experienced an unprecedented power outage. While many pointed to the possibility of a large-scale cyber attack, then Turkish Energy Minister, Taner Yıldız, accused a cat of walking into a power plant and causing the power outage, which lasted for over 24 hours.<sup>2</sup> The credibility of this statement remained disputed for months. Despite advocates of Yıldız's remarks within the government, the country's most important security body, the National Security Council (Milli Güvenlik Kurulu – MGK), did not fully accept his statements.

In 2015, the MGK leaked the main lines of the highly classified National Security Policy Document – also known as the Red Book – which provided detailed information about perceived threats against Turkey. Unlike previous documents, the 2015 Red Book mentioned cyber warfare among core threats against the country. The 2013 Gezi Park protests and the corruption scandal of 2014, as well as the 2014 large-scale cyber attack, were the catalysts for the adoption of the policy change in the Red Book.<sup>3</sup>

Despite the drastic change in threat perception at the state level, until 2017 the Turkish government did not take any substantial steps against external cyber threats. On the contrary, the government placed its focus on domestic politics and invested resources to strengthen its position in the domestic virtual arena, namely social media platforms. As such, in 2015, the Justice and Development Party (Adalet ve Kalkınma Partisi – AKP) formed its first so-called cyber army, consisting of 6,000 professional operators. Having witnessed AKP's weakness during the 2013 incidents, the party sought to design and create Twitter trend topics to influence the chatter on social media platforms. Notably, the ruling AKP succeeded to a great extent in counterbalancing its disadvantaged position courtesy of its newly designed “social media trolls,” most of whom were tasked with carrying out shaming and social media lynching campaigns against the opposition.<sup>4</sup>

While AKP's focus on domestic Turkish politics paid off at home, the Turkish state remained vulnerable to external cyber threats. This weakness was highlighted in the aftermath of Turkey's November 2015 interception of a Russian jet violating Turkish airspace. Rather than retaliate militarily against Turkey, the Russian administration determined to exert pressure by imposing economic sanctions. Moreover, Russia claimed to have sought to increase their pressure on Turkey by launching cyber attacks. The December 2015 “Denial of Service” (DDoS<sup>5</sup>) attack that hit 400,000 sites of the government and academy<sup>6</sup> was mainly attributed to Russian hackers.<sup>7</sup>

This steady deterioration in cyber security continued through the beginning of April 2016, when Turkey was shocked once again by a significant cyber attack. A 6.6 GB file was hacked and leaked, making public the personal details of 50 million Turkish

citizens.<sup>8</sup> Beyond the hack itself, the leak also presented a security problem by creating the potential for other crimes such as fraud and identity theft. Recognizing this challenge, Turkey's Science, Industry, and Technology Minister Fikri Işık told the press that Turkey was ready for any cyber attack, with measures taken by the Transportation Ministry.<sup>9</sup> Despite Işık's statement, the same year, the Turkish Akbank lost nearly 4 million dollars due to fraud carried out through the SWIFT system.<sup>10</sup>

These cyber attacks drew the attention of experts determined to assess the security of Turkish cyberspace. The January-September 2016 report by the information security company "FireEye" openly indicated that 77% of the malware found in Europe originated in Turkey.<sup>11</sup> Moreover, the same report highlighted the lack of information security consciousness<sup>12</sup> and mismanagement in Turkey by indicating the use of outdated operating systems.<sup>13</sup>

Seeing its vulnerabilities vis-à-vis external players, Ankara finally implemented the decisions of the 2015 Red Book by forming a formal Turkish cyber army in 2017. Despite the new vision adopted in the Red Book of 2017, the lack of trained manpower in the field of cyber emerged as a serious weakness. To cope with this deficiency, in January 2017 the Turkish Information and Communication Technologies Authority (Bilgi Teknolojileri ve İletişim Kurumu – BTK) formed a cyber security force, named the National Computer Emergency Response Center (Ulusal Siber Olaylara Müdahale Merkezi – USOM<sup>14</sup>), and recruited 25,000 white hackers to its ranks.<sup>15</sup> Despite this important step, in October 2017, Turkey's Prime Minister Binali Yıldırım pointed out that Turkey still lacked 30,000 cyber security experts.<sup>16</sup>

Various social-media-originated riots, scandals leaked to the Internet, and small- to large-scale cyber attacks revealed the Turkish government's failure to anticipate the importance of cyber warfare. Each action the government took in response to a serious security breach only highlighted the government's inability to cope with cyber threats. Furthermore, the government's emphasis on domestic rivals instead of external adversaries in the virtual arena provides a hint for understanding the mindset of the Turkish security apparatus, which seemingly does not feel threatened by an external power, rather choosing to concentrate its resources against perceived enemies in the domestic sphere. Even if the Turkish government takes all necessary steps to establish governmental bodies to cope with cyber challenges, it is still unknown whether Turkey will succeed in improving its cyber warfare consciousness to defend Turkey against future challenges.

*Dr. Tal Pavel holds a Ph.D. in Middle Eastern Studies from Bar Ilan University. His specialties and interests are the Internet, Cyber, and ICT in the Middle East and North Africa. Dr. Pavel heads the Cybersecurity studies in the Information Systems Program, School of Economics and Management, the Academic College of Tel Aviv-Yaffo, as well as acting as the editor and owner of Middleeasternet.com for Internet, Cyber, and ICT in the Middle East and North Africa.*

*Dr. Hay Eytan Cohen Yanarocak is a researcher at the Moshe Dayan Center for Middle Eastern and African Studies (MDC) at Tel Aviv University. He serves as the Turkey analyst for the Doron Halpern Middle East Network Analysis Desk's publication, Beehive, and is co-editor of Turkeyscope. hayeytan[at]tauex.tau.ac.il.*

## Notes

<sup>1</sup> "Erdoğan: Twitter mwitter, hepsinin kökünü kazıyacağız," *BBC Türkçe*, March 20, 2014,

[https://www.bbc.com/turkce/haberler/2014/03/140320\\_erdogan\\_twitter](https://www.bbc.com/turkce/haberler/2014/03/140320_erdogan_twitter).

<sup>2</sup> "Bakan Yıldız'dan elektrik kesintisi açıklaması: "Trafoya kedi girdi"," *CNN Türk*, April 1, 2014

<https://www.cnnturk.com/haber/turkiye/bakan-yildizdan-elektrik-kesintisi-aciklamasi-trafoya-kedi-girdi>.

<sup>3</sup>"Yeni MGK'dan yeni 'Kırmızı Kitap'a onay," *Radikal*, October 28, 2010,

<http://www.radikal.com.tr/politika/yeni-mgkdan-yeni-kirmizi-kitapa-onay-1026024/>.

<sup>4</sup> Leo Benedictus, "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>.

<sup>5</sup> In computing, a denial-of-service attack (DoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

<sup>6</sup> Efe Kerem Sozeri, "Turkish Internet hit with massive DDoS attack," *The Daily Dot*, December 17, 2015, <https://www.dailydot.com/layer8/turkey-ddos-attack-tk-universities>.

<sup>7</sup> Madhumita Murgia, "Could cyberattack on Turkey be a Russian retaliation?" *The Telegraph*, December 18, 2015, <https://www.telegraph.co.uk/technology/internet-security/12057478/Could-cyberattack-on-Turkey-be-a-Russian-retaliation.html>.

<sup>8</sup> Robert Tait, "Personal details of 50 million Turkish citizens leaked online, hackers claim," *The Telegraph*, April 4, 2016, <https://www.telegraph.co.uk/news/2016/04/04/personal-details-of-50-million-turkish-citizens-leaked-online-ha>.

<sup>9</sup> "Turkey taking measures against cyberattacks, minister says," *Hürriyet Daily News*, January 4, 2016, <http://www.hurriyetaidailynews.com/turkey-taking-measures-against-cyberattacks-minister-says-93393>.

<sup>10</sup> Can Sezer and Birsen Altayli, "Turkey's Akbank faces \$4 million hit from attempted cyber heist," *Reuters*, December 16, 2016, <https://www.reuters.com/article/us-akbank-cyber/turkeys-akbank-faces-4-million-hit-from-attempted-cyber-heist-idUSKBN1450MC>.

<sup>11</sup> Marsh & McLennan, "FireEye – Marsh & McLennan Cyber Risk Report - A perfect storm about to hit Europe?" <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-world-eco-forum.pdf>, page 7.

<sup>12</sup> Barçın Yinanç, "Awareness on information security low in Turkey," *Hürriyet Daily News*, April, 11, 2016, <http://www.hurriyetaidailynews.com/awareness-on-information-security-low-in-turkey-97595>.

<sup>13</sup> Chris Bing, "Why Turkey, a NATO ally, is a huge target for malware," *Cyberscoop*, February 3, 2017, <https://www.cyberscoop.com/malware-attacks-hit-turkey-disproportionately-high-levels-report-says>; Burak Bekdil, "Turkey's cyber security: A long way to go," *Hürriyet Daily News*, 3 March 2015, <http://www.hurriyetaidailynews.com/turkeys-cyber-security-a-long-way-to-go-79076>.

<sup>14</sup> "USOM ve Kurumsal Siber Olaylara Müdahale Ekibi," *BTK.gov*, December 15, 2017, <https://www.btk.gov.tr/usom-ve-kurumsal-siber-olaylara-mudahale-ekibi>.

---

<sup>15</sup> “Türkiye'nin siber ordusu kuruldu, 500 beyaz hacker ile imzalar atıldı,” *Güneş*, November, 18, 2017, <http://www.gunes.com/gundem/turkiyenin-siber-ordusu-kuruldu-500-beyaz-hacker-ile-imzalar-atildi-832040>.

<sup>16</sup> “Turkey's need for cybersecurity experts grows amid increasing threats,” *Daily Sabah*, October 20, 2017, <https://www.dailysabah.com/turkey/2017/10/21/turkeys-need-for-cybersecurity-experts-grows-amid-increasing-threats>.