conflict & communication online, Vol. 18, No. 1, 2019
www.cco.regener-online.de
ISSN 1618-0747

Behlül Çalışkan

Digital security awareness and practices of journalists in Turkey: A descriptive study

Kurzfassung: Diese Studie zielt darauf ab, die spezifischen Herausforderungen und Bedrohungen der Sicherheit zu untersuchen, mit denen Journalisten in dem komplexen politischen Klima der Türkei konfrontiert sind, und das Niveau des digitalen Sicherheitsbewusstseins der Journalisten zu messen, die im Verlauf ihrer Arbeit digitale Technologien nutzen. In der Studie werden Forschungsfragen zu den digitalen Sicherheitsrisiken, dem Umfang der genutzten Digitaltechnik, den eingesetzten digitalen Sicherheitstools und dem Umfang der erhaltenen digitalen Sicherheitstrainings anhand von Daten beantwortet, die mittels einer Online-Umfrage erhoben wurden. Die Studie zeigt, dass Journalisten in der Türkei Sicherheitsrisiken ausgesetzt sind, die von persönlichen Bedrohungen bis hin zu physischen und digitalen Angriffen reichen und dass sie sich stark auf digitale Technologien stützen. Die Studie kommt zu dem Schluss, dass ihnen das Bewusstsein für digitale Sicherheitsrisiken fehlt und nur ein kleiner Prozentsatz Sicherheitstrainings erhalten hat, um sich selbst und ihre Quellen in der physischen und/oder der digitalen Welt zu schützen.

Abstract: This study aims to measure the level of digital security awareness of journalists in Turkey who use digital technology in the course of their work. In the study, research questions are answered using data collected by means of an online survey in relation to the digital security risks faced, the extent to which digital technology is used, the digital security tools employed and the extent of digital security training undertaken. The study reveals that journalists in Turkey are faced with security issues ranging from personal threats to physical and digital attacks and that they rely heavily on digital technology. The study concludes that they lack awareness of digital security risks, and only a small percentage have undertaken safety training to protect themselves and their sources in either the physical or digital worlds.

1. Introduction

Given the level of insecurity surrounding the use of digital and mobile technology by journalists and bloggers, protection of users' identity and privacy is seen as crucial, particularly when citizens and journalists use online platforms, social networks and mobile devices to post comments or reports about crime, corruption or violence (Sierra, 2013, p. 5). Nonetheless, digital technology can also offer tools to minimize the dangers, whether physical, digital, or psychological, that reporters and editors face on the job (Ramos, 2016, p. 1).

However, before being encouraged to use these digital security tools, journalists should be acquainted with the broader questions of digital security, the extent of their own knowledge, how such tools could be usefully employed in the context of their own work and to what degree they should be relied upon. The subject of this study is the digital surveillance awareness and security practices of journalists. In this context, the study aims to examine the specific challenges and threats to digital security that journalists face in the complex technological and political climate of Turkey. In order to understand journalists' attitudes towards mass surveillance, the study will measure their level of digital security awareness and the practices of journalists using digital technology in the course of their work, and will seek to assess the gap between journalists' use of digital technology and their digital security practices. In the study, research questions in relation to the digital security risks faced, the extent to which digital technology is used, the digital security tools employed and the range of digital security training undertaken are answered using data collected by means of an online survey.

2. Media landscape of Turkey

The press in Turkey has never been completely free throughout the history of the Republic. However, pressure on the press has increased at an unprecedented rate since 2011 and has led several analysts to describe Turkey as an "illiberal democracy", with some identifying these developments as Turkey's authoritarian turn (Yeşil, 2016, p. 10). This pressure on the press that was already exerted in various forms before 2011 may be summarized under three categories: media ownership structures, takeover of mainstream media and censorship.

The AKP government's actions to reshape the media can best be seen in the changes of media ownership patterns between 2002 and 2011. The media assets of powerful groups changed hands and were transferred to more government-friendly owners or conglomerates led by then Prime Minister Recep Tayyip Erdoğan's family members (Akser & Baybars-Hawks, 2012). An additional coercive tool has been tax investigations, which have been used to punish media outlets that dare to challenge the government. The once-dominant Doğan Media

Group was subjected to enormous fines and forced to sell off several media properties, including one of the country's leading papers (Corke, Finkel, Kramer, Robbins, & Schenkkan, 2014). This change of media ownership continued after 2011. Finally in March 2018, Turkey's largest media conglomerate, Doğan Media Group, was sold to a pro-government conglomerate, which has other investments in the media sector. Following these changes, the total shareholdings of pro-government companies in the most important Turkish TV stations and daily newspapers increased to 90%, resulting in the end of diverse mainstream media in Turkey.

In addition to the reshuffling of media ownership structures, 2008-2010 witnessed a legal harassment of journalists charged with coup attempts and spreading terrorist propaganda during major political investigations, such as those of Ergenekon and the KCK (Yeşil, 2016, p. 88). Both investigations targeted secular, social democrat, leftist and Kurdish journalists, and dozens were imprisoned. After two major wins in the 2010 constitutional referendum and 2011 general elections, this pressure was directed at all government-critical journalists in the mainstream media, and several journalists were dismissed for their criticism of the AKP's policies. Today, Turkey has become the world's worst jailer of journalists, with 73 behind bars, according to the Committee to Protect Journalists (CPJ). Dozens more still face trial, and fresh arrests take place regularly (Beiser, 2017). Although CPJ was unable to establish a link to journalism in several other cases, other press freedom groups using different methodologies report higher numbers. The European Federation of Journalists monitors jailed journalists under the scope of a special project entitled "#JournalismIsNotaCrime", whose aim is the freeing of jailed journalists, the development of trade union rights and the defense of freedom of expression in Turkey. It noted on its website in May 2018 that there were 156 imprisoned journalists in Turkey (European Federation of Journalists, 2018). The Media and Law Studies Association, a Turkish non-profit organization, regularly monitors the status of journalists and media workers imprisoned in Turkey. According to data it published online, 177 journalists were in jail as of July 2018 (Media and Law Studies Association, 2018).

The media have always struggled with censorship in Turkey, but in recent years specific incidents have clearly shown that both media companies and journalists have repeatedly faced censorship and self-censorship (Filibeli & İnceoğlu, 2018). Filibeli and İnceoğlu's argument relies on two well-known cases which clearly demonstrate the state of Turkish media in terms of censorship and self-censorship. The Roboski Airstrike by two Turkish F16 fighters that caused the deaths of 34 civilians in 2011 led to one of the most important examples of censorship in Turkey. The main Turkish news channels didn't make any reports on the event, and even after people learned about the airstrike on social media, there was no coverage of the incident on either television news channels or on newspapers websites. A second example of censorship in Turkey was one which occurred during the Gezi Park protests. In the early days of the protests, the main news channels in Turkey did not allude to them at all, and at least 59 journalists were fired during the Gezi protests for criticizing the government.

Since widespread use of social media during the Gezi Park protests and distribution of the leaked tape recordings of Erdoğan's phone calls via YouTube in 2013, the government has continuously attempted to block online information sources in Turkey. A few weeks before the local elections in 2014, access to Twitter was blocked in accordance with a court order that came after complaints had been filed by citizens in relation to personal issues, and only a week after the Twitter ban, YouTube was banned because of a leaked conversation between high-level public authorities discussing possible military action in Syria. Another nationwide block on Wikipedia began in April 2017, which is still in force (Yeşil, 2016, pp. 118-119; Freedom House, 2018). Turkish authorities' efforts to control online media can be seen in the sharp increase in the number of their content removal requests, with a 966 percent increase in the number of items that Turkish courts have asked Google to remove, a 100 percent increase in requests to Facebook and 156 percent increase to Twitter in 2014 (Yeşil, 2016, p. 119). Lastly, at the suggestion of the ruling party, a law on Internet broadcasting was introduced, requiring online video streaming services to apply for a license from the regulator, RTUK. Access can be blocked if permits are not secured. RTUK checks the content, and has the power to issue fines. Although some independent websites continue to operate, they face tremendous political pressure and are routinely targeted for prosecution; more than 150 media outlets were closed in the months after the 2016 attempted coup (Newman, Fletcher, Kalogeropoulos, Levy, & Nielsen, 2018).

In addition to the country-specific challenges, journalists in Turkey must also contend with global problems faced by all journalists worldwide such as "online surveillance", which is the core of this study. The following section will address this phenomenon.

3. Problem definition

Although surveillance is a particularly modern concept that Michel Foucault describes as a rational way for regulating society, and Karl Marx views as an element of the struggle between labor and capital, it became more evident in the period following the 9/11 attacks, also known as the "new media age". Edward Snowden's revelation on the extent of surveillance of foreign citizens' personal communications by the National Security Agency (NSA) and other agencies has been described as "one of the most significant leaks in U.S. political history" (Walker, 2014, p. 246). Snowden's revelation demonstrated the superior capabilities of major intelligence agencies, which enable them to gain unauthorized access to virtually any personal computer or electronic communications device in the world and collect communication data. This poses a considerable security threat to journalists reporting news about the interests of governments, government agencies and intelligence agencies. Although most countries do not have such sophisticated surveillance technologies, nearly every country has a surveillance capacity that can sometimes be used against journalists, potentially resulting in severe consequences.

Whether professional journalists or ordinary citizens, we also participate in surveillance activities through our online interactions, especially in relation to our social media and cellphone use, without necessarily being aware of it, according to Lyon (2015, p. 9). However, Snowden himself was aware of the extent of mass surveillance and also of the secure tools used to counter it, tools that he employed while copying NSA documents and communicating with journalists in order to leak those files before contacting the filmmaker, Laura Poitras. To describe the contents of the information he planned to give her, Snowden first sent a note to then *Guardian* journalist, Glenn Greenwald, asking for his public encryption key so he could send him an e-mail securely. But, although he wrote almost daily about national-security issues, and had likely been on the government's radar, Greenwald didn't have one. He didn't even know what PGP was, had no idea how to install it or how to use it, and found it time-consuming and complicated (Reitman, 2013). So, Snowden sent another anonymous e-mail to Poitras, who later filmed their encounter in Hong Kong and the story behind the reporting of the NSA leaks. She already knew how to use secure tools while communicating online in relation to sensitive issues (Greenberg, 2014).

As this example also demonstrates, journalism is undergoing a fundamental transformation, and one of the key reasons for this transformation is the changing nature of technology. Since the mid-1990s a number of studies have explored the implications of the internet for journalistic practice (Fenton, 2010; Miller, 1998; Reddick & King, 1997; Singer, 1998, 2001, 2003; and Deuze, 1999). These studies reported that the internet furnishes newsrooms with new ways of collecting and reporting information. Developments in computer and mobile communication technology, and the expansion of the internet have removed many geographic, social and political barriers to news and information exchange. The internet has become a virtual meeting place for individuals to exchange information and ideas, discuss important issues and connect with each other, offering people the opportunity to use their right of expression and organization in a way never seen in any other period of history (Fenton, 2010, pp. 557-558).

On the other hand, as the increasing digitalization of journalism provided unprecedented advantages to journalists and audiences, it also revealed some worrying trends. It has been shown that news media can be controlled and monitored to limit access to information and freedom of expression. These mass surveillance practices have made the safety of journalists more complex and challenging than ever before. Today, digital security has become a vital issue for those working in journalism, their families and their resources. The difficulties that journalists face online are no different from threats that exist in the physical world. A UNESCO study on digital safety for journalism states that death threats are now being sent via e-mail and in response to web-based content, not to newspapers or TV broadcasters. A media office or printing house can still be bombed, but now the website of a media company may be exposed to "Denial-of-Service" attacks, resulting in it being unable to service incoming requests due to the sheer volume of traffic. Other threats have also acquired new dimensions within the digital domain. As more data are generated, stored, transmitted and searched, threats such as gender-based violence have now increased (Henrichsen, Betz, & Lisosky, 2015, p. 8). In addition, new privacy and freedom of expression issues have emerged. For example, journalists' movements are monitored by mobile-phone-linked geographic location data, their personal lives are visible in social media, and meta-data about their communication activities are collected. It is also acknowledged that digital security is undergoing constant change, and it is becoming cheaper than ever to launch digital attacks. As such, with the digitalization of journalism, security risks have also been transferred from the online to the offline worlds.

According to Citizen Lab's Ronald Deibert (Henrichsen, Betz, & Lisosky, 2015, p. 20), this led to a dangerous weaponization of cyberspace, and the resultant insecure environment may result in independent media being trapped, harassed and exploited to the same degree to which they can be empowered. In addition to media workers, who are often not fully aware of how new technologies threaten privacy and security (Sierra, 2013, p. 4), journalists who have recently joined the profession and contribute to informing public opinion have become persons of interest to actors wishing to control the flow of information (Henrichsen, Betz, & Lisosky, 2015, p. 13). State or non-state actors can attempt to influence the flow or content of information by denying, disrupting, manipulating, or monitoring access to a range of electronic data. Methods vary, because exploitation and attacks are influenced by a variety of factors, including the economic, social and political contexts where information controls are applied. The control of information is also influenced by the types of communications infrastructure that countries have, such as the number of Internet Service Providers, telecommunication companies, degrees of market competition and the overall level of internet penetration and growth (The Citizen Lab, 2013). Twenty-one of the world's top-25 news organizations have been the target of likely state-sponsored hacking attacks, according to research by Google security engineers. The attacks were launched by hackers, either working for or supporting a government, and specifically targeted journalists. While small news organizations, citizen journalists and bloggers were also targeted, the attacks are not limited to a particular region and are global in both origin and focus (Wagstaff, 2014).

Beyond cyber-attacks, media workers also come under physical attack because of journalistic activities they conduct online (Villareal, 2017, p. 267). From 2011-2013, of the 276 journalists who were killed, the primary platforms of 37 of these were internet-based. According to the Committee to Protect Journalists (CPJ), 44% of the 70 journalists recorded as killed in 2013 were journalists who worked for online media platforms. Meanwhile, such "online journalists" accounted for half (106) of the prisoners CPJ recorded as imprisoned in 2013. However, dangers threaten not only those who publish online. They apply to all actors whose journalistic activities interface with electronic technology, whether through their use of computers to process information, their utilization of telecoms or the internet for news gathering and research, or simply as a result of their reliance on email for communication (Henrichsen, Betz, & Lisosky, 2015, pp. 8-14).

Not surprisingly, in a country with an almost 70%-internet-usage rate as of 2017 August (Turkish Statistical Institute, 2017), Turkey exercises strict control over the online activities of both journalists and ordinary citizens. Yeşil, Sözeri and Khazraee (2017) present an overview of Turkey's internet policy over recent years, based on Deibert and Rohozinski's scheme on Internet control and surveillance. In this scheme, first-generation controls consist of internet filtering and blocking; second-generation controls involve enacting legal restrictions, content removal requests, technical shutdown of websites, and computer-network attacks; and third-generation controls include warrantless surveillance (Deibert & Rohozinski, 2010, p. 17). Accordingly, in Turkey, 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. Between 2007 and 2013, a period when so-called harmful online content and communications were the primary concern on websites, blogs, and social networking and collaborative sites, Turkish courts and administrative entities relied largely on first and second-generation controls (Yeşil, Sözeri, & Khazraee, 2017).

However, after the Gezi Park protests in 2013, the government became aware of the role of social media platforms in political engagement and civic mobilization. In accordance with several pieces of legislations introduced before and after 2013, Internet service providers are now required to monitor online content transmitted through their infrastructure and to ban access to illegal content when served with a court order or an administrative notice. ISPs are also required to collect data on users' activities for up to two years and provide authorities with these data on demand. Another new piece of legislation authorizes the National Intelligence Agency to collect personal data, documents and information about individuals without a court order; obtain data from private companies, public authorities, professional organizations and other legal persons; and to gain access to data stored in IT devices, equipment and hardware, whether they are publicly or privately owned. Law enforcement agencies are allowed to carry out wiretapping in urgent situations for a forty-eight-hour period without a court order, and in urgent situations the police can request user data from telecommunications companies to locate the user, and monitor and evaluate their communications. Car rental companies and hotels are required to keep daily records of customers' identities and contact information, and to computerize all records, and to have their computer terminals connected to the computer terminals of law enforcement officials (Yeşil & Sözeri, 2017).

In the aftermath of the coup attempt in 2016, the government shifted to third-generation controls and has intensified its attempts at controlling the online public sphere by means 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 (Yeşil, Sözeri, & Khazraee, 2017).

While the digital world makes journalism a risky profession, it also has the potential to make it safer. Digital technology provides tools to minimize the physical, digital, or psychological hazards encountered by reporters and editors during their work. The increasing use of mobile devices by journalists is accompanied by a number of applications that apply security layers to their work. Of these, Tor, a privacy protecting and anonymizing network application is perhaps the most potent. Tor is free software that provides protection against threats to personal security and privacy, private business activities and individual relationships, as well as network surveillance and state security practices known as traffic analysis. The Tor network enables users to connect to the Internet via a series of virtual tunnels instead of through direct connections, thereby allowing users to share information over public networks without sacrificing the privacy of the organizations or individuals involved. Individual users employ Tor to prevent websites from tracking them or their family members, to connect to news sites or instant messaging services, or to access these sites or services when blocked by local Internet providers. Journalists also use Tor to communicate securely with whistle-blowers and dissidents. Tails is an operating system that runs on any computer via a DVD, flash memory or SD card, protects the privacy of users and allows them to remain anonymous. PGP and GnuPG are used to encrypt data, decrypt encrypted data, or securely sign data, as well as to ensure the privacy and authenticity of e-mails sent or received.

After Laura Poitras realized the depth and extent of Snowden's leaks, Poitras bought a new laptop, paying with cash, and used it only with the Tails operating system – free software designed not to leave any trace of communications on the computer and to route all network data over the Tor anonymity network. Poitras later explained that she used the Tails computer only to communicate with Snowden, and only in public places with WiFi connections, never at her home or office. Aside from her communications with Snowden, Poitras also kept all the film's footage on encrypted drives and in the closing credits of her film, *Citizenfour*, Poitras added an acknowledgment of the free software projects that made the film possible, including the anonymity software Tor, the Tor-based operating system Tails, the anonymous whistle-blowing platform SecureDrop, GPG encryption, Off-The-Record (OTR) encrypted instant messaging, hard disk encryption software TrueCrypt, and GNU Linux, without which, Poitras argues, neither her reporting on the Snowden leaks nor her film itself would have been possible (Greenberg, 2014). However, as research demonstrates, most journalists worldwide don't make use of digital tools to stay safe online, although to a certain extent they have an awareness of digital threats. One of the main reasons for this is that journalism schools don't include digital security training in their curricula. A study by Citizen Lab (Oliver, 2018) suggested that most journalism schools do not do enough security training to prepare the next generation of reporters to protect themselves, their sources, and their colleagues online. Only half of the 32 schools across the US and Canada that responded to the survey offer digital security training, and less than a quarter make that training mandatory. The needs of journalists in relation to acquiring knowledge about digital security are mostly met through training programs provided by journalism organizations (Pew Research Center, 2015; Henrichsen, Betz, & Lisosky, 2015; Bytes for All, 2012). But, these kinds of events may sometimes be seen as illegal by governments in countries such as Turkey. In July 2017, the head of Amnesty International Turkey was arrested along with activists and trainers during a "digital security workshop" on Büyükada, one of the Princes' Islands off Istanbul, and were imprisoned for a period of three months, accused of being members of and aiding an "armed terrorist organization" (Shaheen, 2017).

4. Past research

Significant research has appeared in recent years on the digital security threats faced by journalists working in different regions of the world and their awareness of these threats. The research conducted by the Pew Research Center in association with Columbia University's Tow Center for Digital Journalism with 671 members of Investigative Reporters and Editors, Inc. revealed that about two-thirds of the investigative journalists surveyed believe the U.S. government has probably collected data on their phone calls, emails or online communications, and 80% believe that being a journalist increases the likelihood that their data will be collected. Concerns about surveillance and hacking have led many of these journalists to alter their behavior in the past year. Nearly half said they have to some degree changed the way they store or share sensitive documents, and one-third of the participants echoed these comments in relation to how they communicate with other reporters, editors or producers. In addition, among the 454 respondents who identify themselves as reporters, 38% said that in the past year they had again to some degree changed the way they communicate with sources (Pew Research Center, 2015).

Other research conducted by Freedom House and the International Center for Journalists with 102 journalists and bloggers in Mexico showed that nearly 70% have been threatened or have suffered attacks because of their work. In addition, almost all (96%) said they know of colleagues who have been attacked. Respondents to the survey also said they view cyber-espionage and email-account hacking as the most serious digital risks they face. And while nearly all have access to and rely on the Internet, social networks, mobile phones and blogging platforms for their work, they also admitted that they have little or no competence in using digital security tools (Sierra, 2013).

In December 2011, the Pakistan-based ICT and human rights organization Bytes for All conducted research to provide a snapshot of the level of awareness and use of digital security strategies by the media community in Pakistan. According to the findings, three-quarters of the 52 journalists and bloggers surveyed had personally experienced a security issue due to their work. However, most of the respondents were unaware of the security risks they face in their online activities, such as email interception and data theft. Nor were respondents aware of the widely available strategies and tools that could protect them in the digital space, including the use of secure email services, data encryption, or IP blocking services that help conceal sensitive online activities. The research also revealed that 90.4% of respondents have never received any training in how to ensure their digital security (Bytes for All, 2012).

Another piece of research was conducted in 2015 by the Center for International Media Assistance (Ramos, 2016) to measure how journalists around the world take advantage of technology to enhance their security. A total of 154 journalists responded from North America, Latin America, Western and Eastern Europe, the Middle East, Central and Southeast Asia, and Africa. The research found that most journalists do not employ digital tools in their general security and safety procedures, whether physical or digital; about 60% of respondents reported not using these tools in any situation. The regional differences in usage also reflected the level of assimilation of technology in journalism. The study showed that journalists in North America and Europe are more likely to use digital tools for security, while journalists in Africa are the least likely to.

Too little research has been undertaken by journalists on the subject of digital safety in Turkey. In their study, consisting of 22 in-depth interviews with representatives of alternative media initiatives and citizen journalists, Ataman and Çoban found that phones had been wiretapped with a view to supporting accusations filed against journalists in Turkey; it is also suspected that police have sometimes successfully tried to infiltrate journalists' online communication channels and mobile applications. News-collective staff stated that they take extra precautions when they use their phones, e-mail, or messaging applications. The study showed that despite well-intentioned efforts of citizen journalists, they lack awareness and technical knowledge about digital security and are generally ignorant about the best practices in protecting themselves against digital surveillance. They use conventional stashing methods to conceal their archives or delete visuals that may cause legal problems, and format their hard disks to prevent their archives from being seized. According to the study, news collectives have a better understanding of digital security and offer training sessions on this subject to the citizen journalists who have collaborated with them. Despite the training they receive, citizen journalists are reluctant to use digital security measures unless they are compelled by the collectives they work with (Ataman & Çoban, 2018).

5. Methodology

The main research question of the study is to what extent journalists in Turkey are aware of digital security and what measures they take against digital security threats. Four secondary research questions are also employed in the study:

- Which security threats do Turkish journalists face?
- To what extent do Turkish journalists use digital technology?
- Which digital security tools do Turkish journalists use?
- What are the digital security training experiences and needs of these Turkish journalists?

In order "to collect information from a large number of people with the ability to represent a particular population" (Berger, 2000), a survey was undertaken in order to answer the research questions. Data were collected with a structured questionnaire, which was created by examining questionnaires previously employed in the related literature. Since journalists in Turkey widely use closed social networks like WhatsApp, Facebook and e-mail groups to communicate and collaborate with each other, the snowball technique was used to reach the target population. Starting with the initial journalists from mainstream and alternative media, the questionnaire was distributed through channels such as e-mail, online discussion groups, social networks, messaging platforms and the mailing lists of journalists; a total of 54 journalists participated in the survey between 15 September 2017 and 23 October 2017. In relation to the fourth research question, an additional content analysis was conducted on open-ended responses to determine the digital security training needs of journalists.

The main limitation of the study was the low number of journalists who participated in the survey. Although the questionnaire had been distributed through many channels and the call for participation in the survey reached many journalists, the number of participants remained low. Thus, the results of this survey are not a statistical representation of the general state of digital security for journalists in Turkey, but they do offer quantitative evidence as to their digital security awareness and practices.

6. Findings

6.1 Overview

About half (28) of the respondents were woman journalists, and the median value of the age range was 25-39, representing 38 respondents. More than half (33) of the respondents had been working as journalists for nine years or less. A significant majority (42) stated that the Internet was their main working area in the media, and over two-thirds said they were working as staff journalists, followed by about one-third as freelancers and only 5 as citizen journalists or bloggers. In terms of the topics covered on a regular basis, politics and human rights were foremost, with rates in excess of two-thirds, followed by crime and war.

6.2 Security of journalists

Research findings show that physical detention and job insecurity are the most common threats Turkish journalists face. Although the respondents benefit from digital tools, they are also exposed to digital security threats.

When asked whether their journalistic activities included meetings with sensitive contacts or informants, three-quarters of the participants responded that they did. Only half of journalists stated that their activities included meetings with individuals or organizations that might be a source of interest to the authorities, gangs or criminals. When asked to rank three challenges facing journalists today, all the journalists identified being arrested or detained as their chief concern. Second was the risk of being dismissed, demoted or reprimanded at work (26) and the third was being physically attacked (24) (cf. Figure 1).

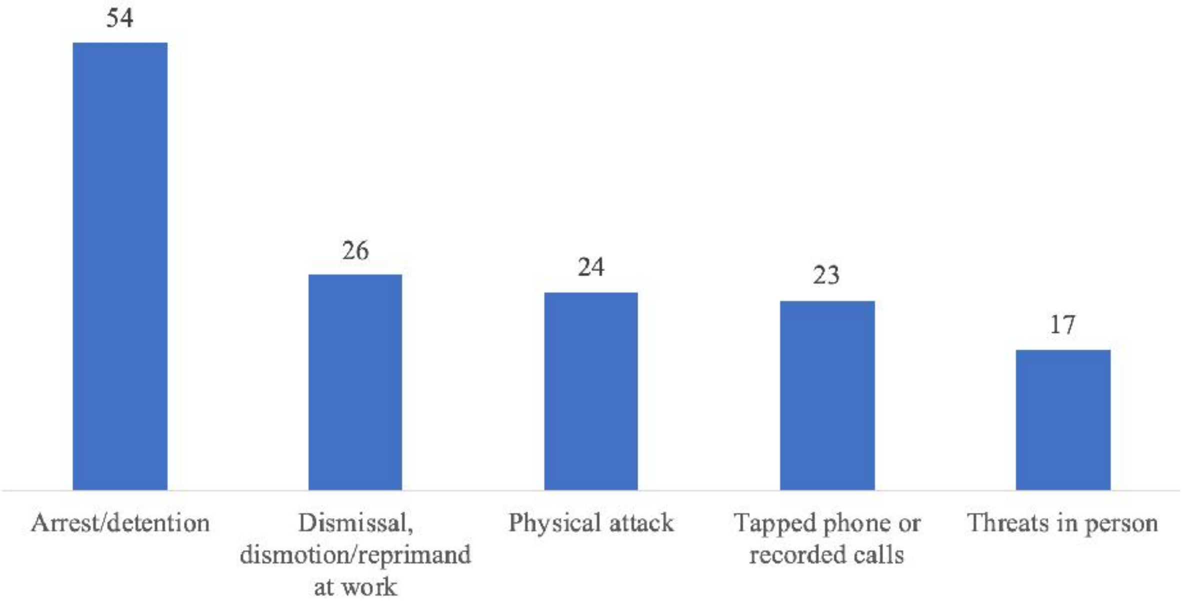


Figure 1: Top three threats Turkish journalists might face

Almost all respondents said that their work as a journalist had caused them some form of security concern. Personal safety was a concern for almost all respondents, while 33 cited information security, and nearly one-half thought the safety of colleagues was another important concern (cf. Figure 2).

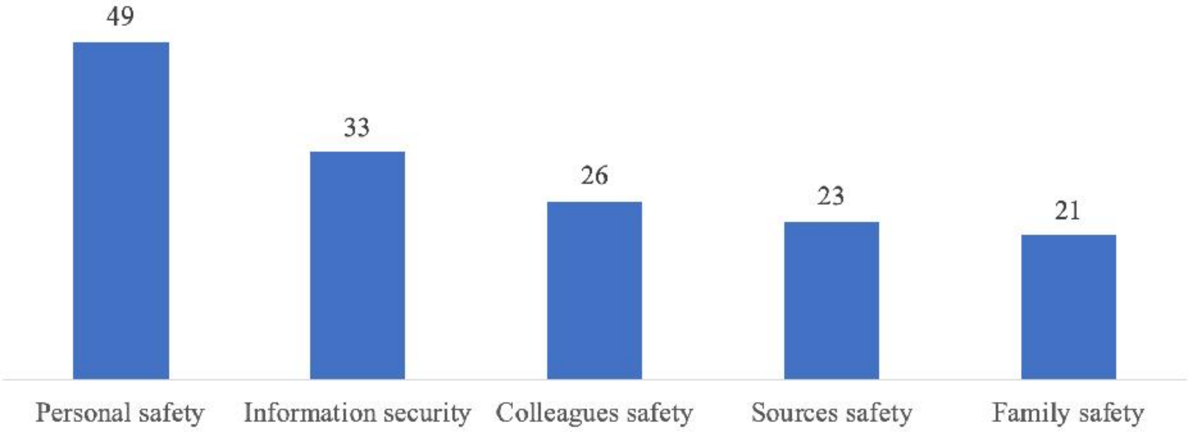


Figure 2: Main security concerns

When asked whether the journalists had experienced any negative consequences due to their journalistic activities in the last 18 months, 39 respondents said yes. According to the responses, personal threats were the most common negative consequence of being a journalist in Turkey, followed by wire-tapping, physical attacks, online disinformation campaigns, arrest and cyber-attacks (cf. Figure 3).

Two-thirds of those surveyed said that for today’s journalists, the benefits of digital communication such as email and cellphones outweigh the risks. Eighteen respondents said the risks outweigh the benefits. Concerns about surveillance and hacking were not regarded as sufficient to deter many journalists from pursuing a story or a source. Fourteen respondents said that such concerns had kept them from pursuing a story, and 17 said that as a result they had not reached out to a particular source in the past 18 months. On the other hand, these concerns had led many of the journalists to alter their behavior in the past 18 months. Nearly two-thirds said that to some degree they had changed the way they store or share sensitive documents, one half said that they had changed the way they communicate with sources, and almost half said they had to one degree or another changed the way they use the Internet to do research (cf. Figure 4).

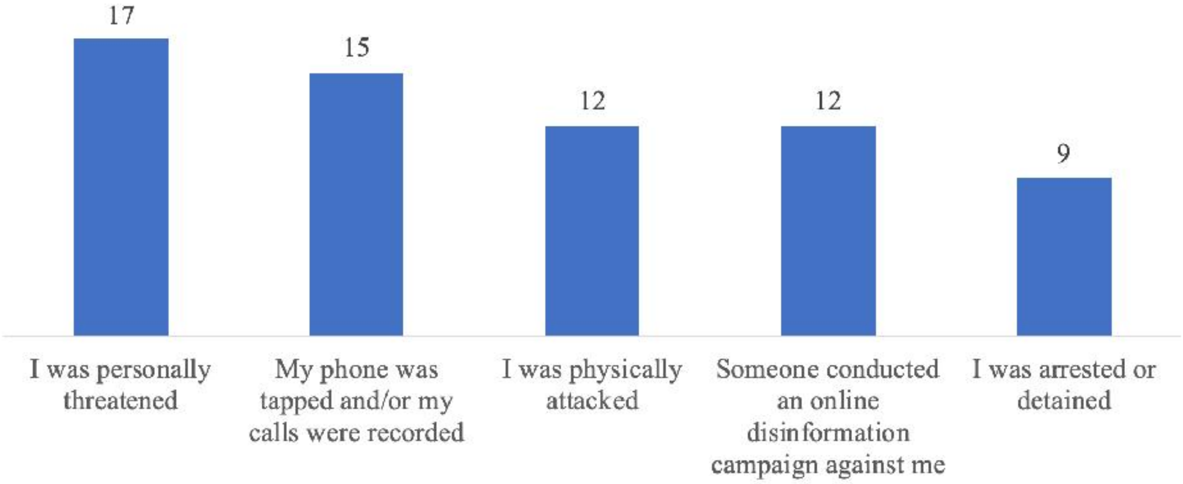


Figure 3: Negative consequences resulting from journalistic activities in the last 18 months

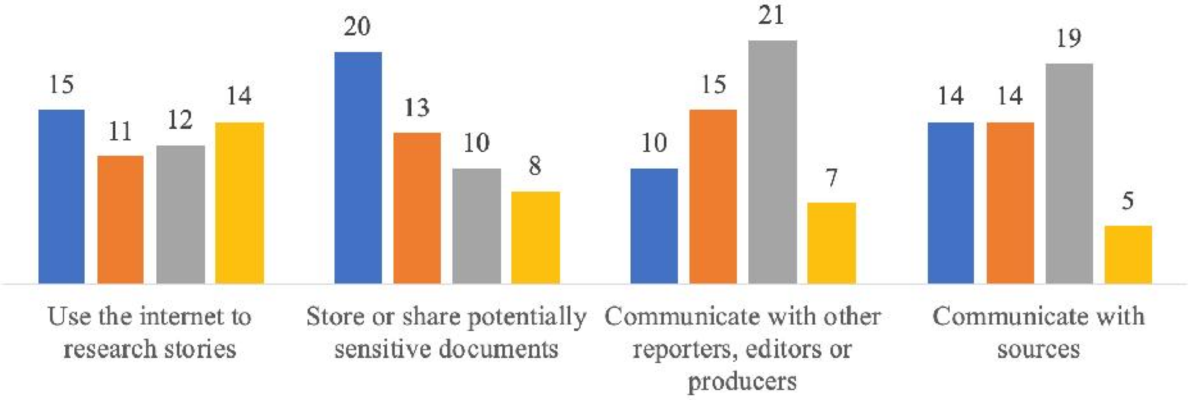


Figure 4: Changes in the way journalists conduct their work

Almost all the surveyed journalists believe the government has probably collected data about their phone calls, e-mails or online communications; and all respondents believe that being a journalist increases the likelihood that their data will be collected by governments. To protect their sources' identities, nearly two-thirds of the respondents stated that they prefer to meet them in person instead of communicating via phone or e-mails. This measure was followed by the use of encryption while communicating with sources through e-mail or messaging applications (11).

6.3 Digital technology usage

The study revealed that the journalists who participated in the survey use digital technologies to a great extent. Based on survey results, respondents seemed to rely on mobile technology to gather and report news and information. Nearly nine of ten participants said they used mobile phones, and three of four said they used laptops for their journalistic work. The use of social networks and e-mails was also common among journalists, and over half of the respondents used websites & search engines, audio & video recording devices and desktop computers when researching, distributing, or writing a story (cf. Figure 5).

A large majority of the respondents (49) said that they use the web for writing stories. Nearly eight in ten participants use e-mail to some extent to obtain and share information. More than half of the respondents stated that they often use e-mail in their journalistic work for researching and distributing stories as well as liaising with media outlets. While *Gmail* is the most commonly used e-mail service provider with 46 respondents, nearly half of the survey participants use their corporate e-mail accounts. In terms of e-mail security, only half of the respondents were aware of secure e-mail services.

In researching or writing a story, respondents reported that Twitter and Facebook were their two most used social media platforms. Twitter was the most popular social networking website, with 44 respondents using it to a moderate or heavy extent, followed by Facebook with 33 and then YouTube with 26. In distributing stories, respondents again stated that they mostly used Twitter (43) and Facebook (36), but only one in four journalists used YouTube to share stories.

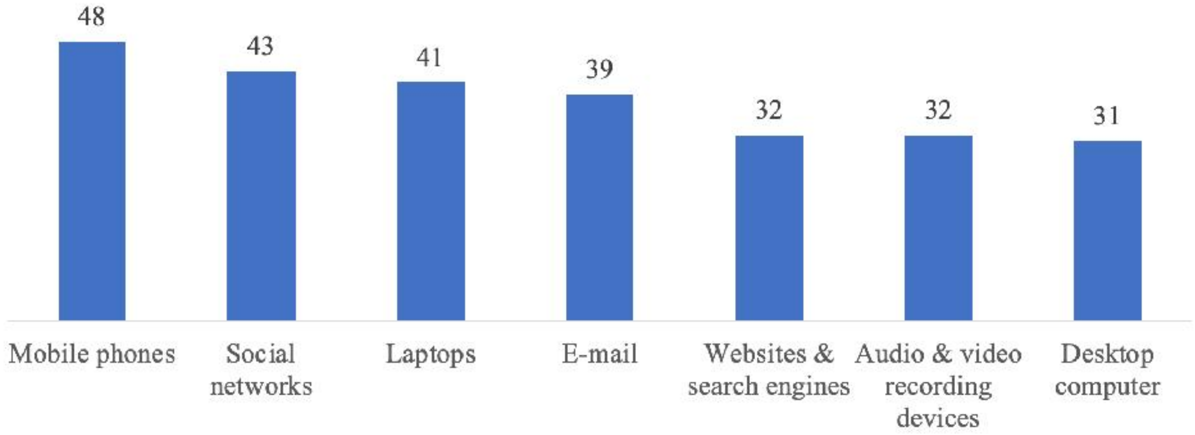


Figure 5: Technologies and tools used when researching, distributing, or writing a story

6.4 Digital security

As regards the respondents' digital security practices, the findings show that they have a basic awareness about hiding their identities when going online, probably because of the government's pressure on the press and its control of the Internet. Although password and anti-virus protection tools are widely used by journalists, only a few are aware of digital security strategies and more advanced digital security tools.

Participants were asked whether they used any of several possible digital security techniques on their own computers, tablets, or mobile phones, as well as on devices provided by their employers. The results showed that with respect to their own devices, the respondents use privacy-enhancing search engines, privacy-related browser plug-ins and software, which allows them to browse the web anonymously, slightly more than devices provided by their employers (cf. Figure 6).

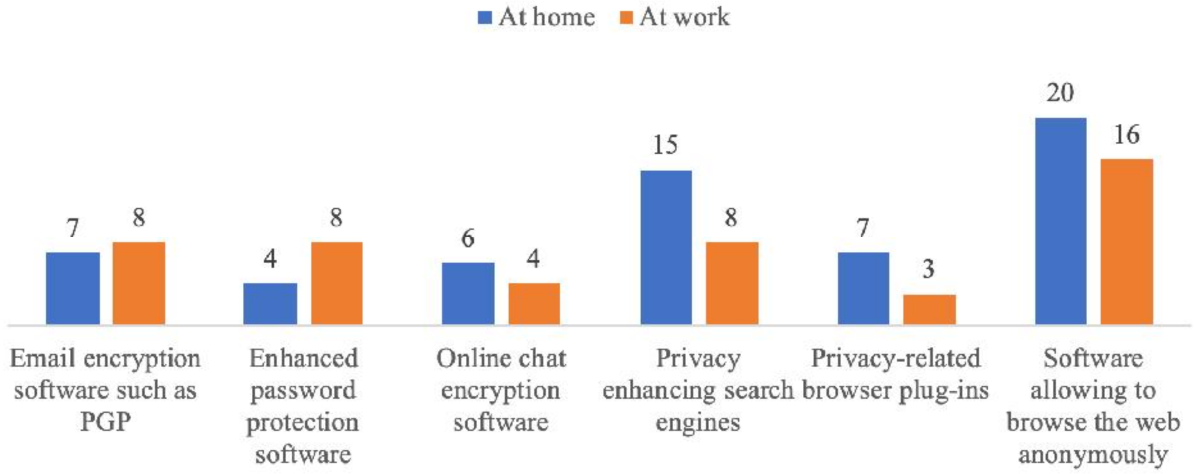


Figure 6: Use of digital security-related tools at home and at work

Almost seven in ten respondents said that they don't click on any web links or attachments contained in an email or social media message, if the sender is unknown. On the other hand, nearly eight in ten journalists stated that they would generally do so, if the sender was known to them (cf. Figure 7).

Survey participants were asked which features are most important to them in selecting an e-mail service. The largest group of respondents (28) replied that "ease of use" is the most important feature for them in an e-mail service. Only one in three journalists considered "security" the most important feature for them to have in an e-mail service. In terms of selecting a blogging or micro-blogging service such as Twitter, most respondents rated either "ease of use" or "popularity" as the most important feature. Only one in five respondents said the security features of a particular blogging or micro-blogging portal were their first consideration in choosing (cf. Figures 8 and 9).

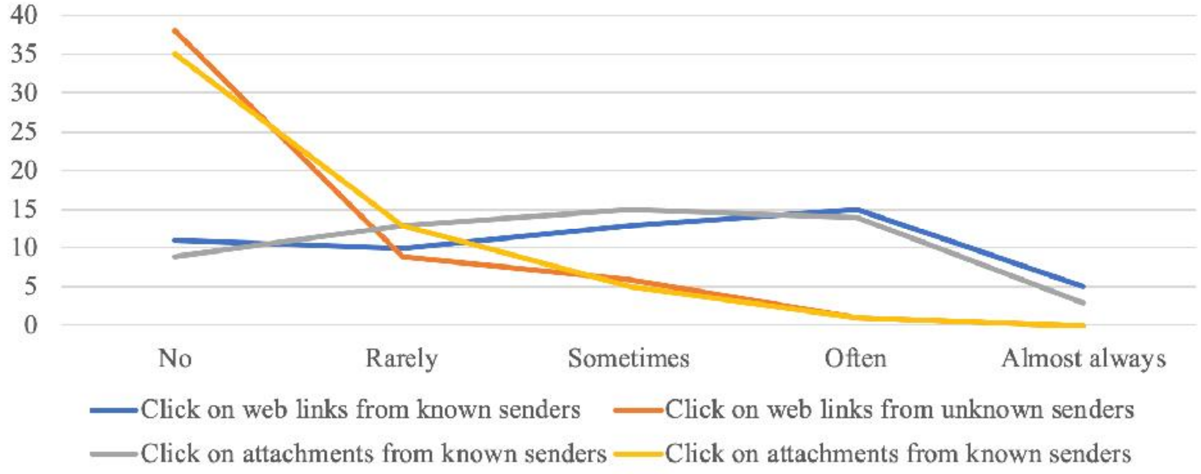


Figure 7: Clicks on web links and attachments

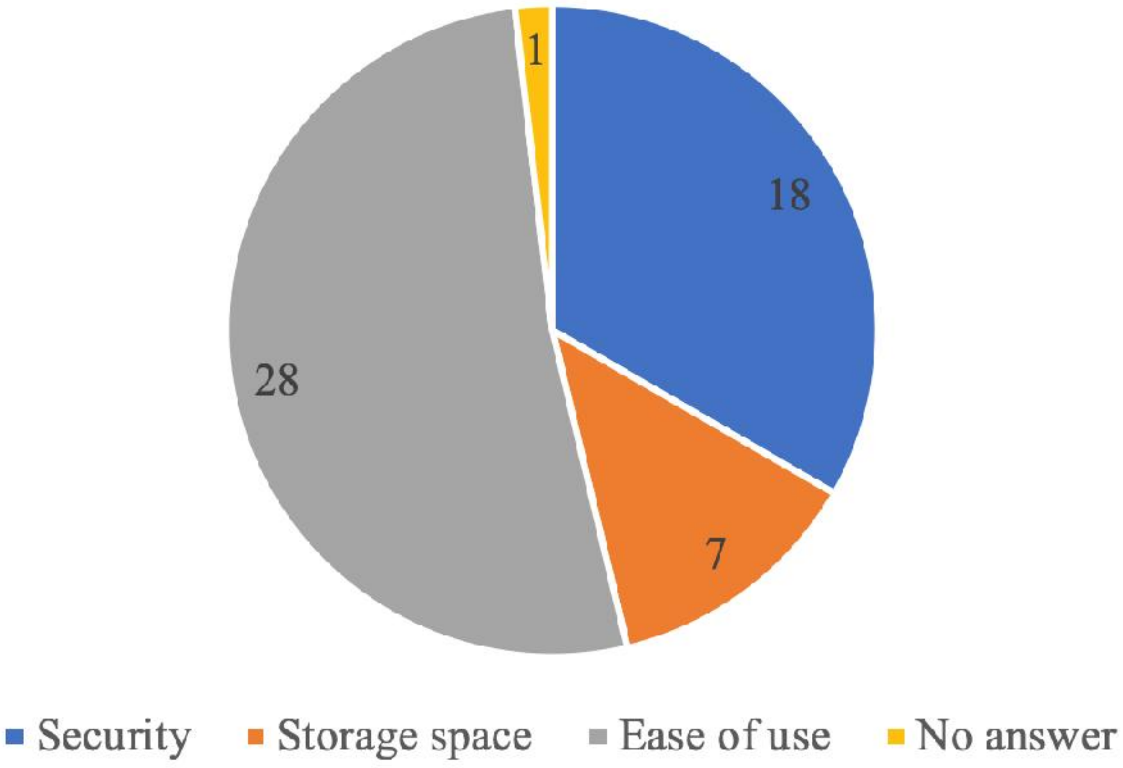


Figure 8: Features which determined the selection of an e-mail service

In terms of knowledge about the digital security of journalists, almost one in ten respondents is somewhat familiar with digital threat modeling, and only one third of them were aware of strategies and tools intended to keep them safe online. Those respondents who said they were aware of digital security tools for their online communications mainly had heard of basic strategies such as using strong passwords, anti-virus software, VPNs and two-factor authentication. Respondents were also asked which strategies they used in their day-to-day life to protect their online communication. The largest number of respondents reported using strong passwords and VPNs to protect themselves online, followed by anti-virus software, two-factor authentication and firewall protection (cf. Figure 10).

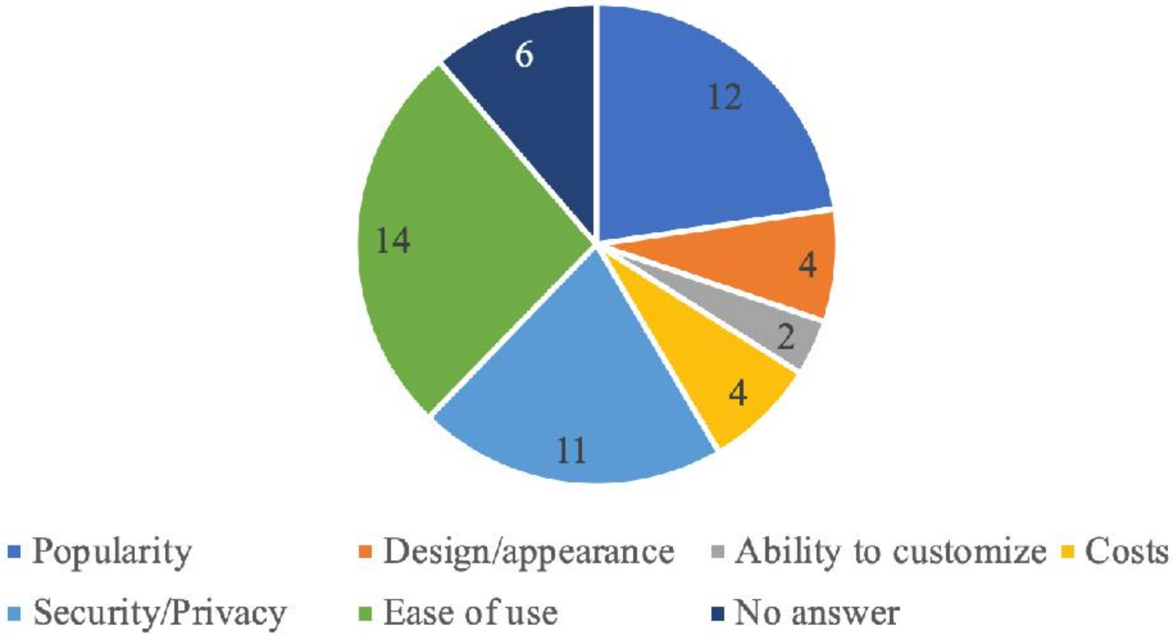


Figure 9: Features which determined the selection of a blogging/micro-blogging service

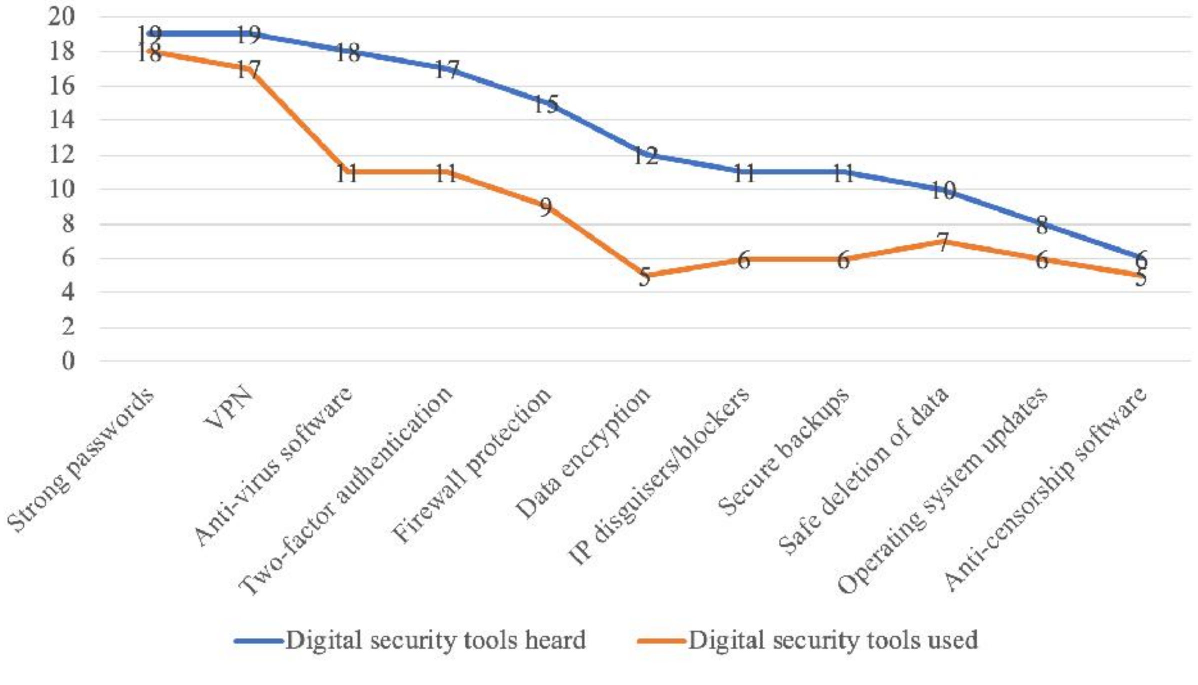
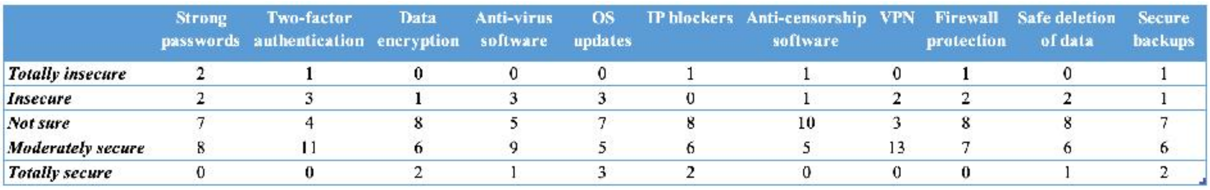


Figure 10: Digital security tools

Survey participants rated several digital security techniques to indicate how secure they thought each was. Respondents believed that VPNs, two-factor authentication and anti-virus software were somewhat secure tools to safeguard against online threats, but most said they did not know about the level of security offered by tools such as data encryption, IP blocking, anti-censorship tools, or safe data deletion (cf. Figure 11).

The participants were asked about the range of practices they apply to protect their privacy in digital media and how these practices had changed in the past 18 months. The most commonly used technique was clearing the browser history, followed by turning off the geo-location feature of mobile devices, applications and social media platforms; using different passwords for different online accounts and utilizing the enhanced privacy settings on social media platforms were also cited. Most respondents who reported using these approaches said they had done so for more than 18 months. Disabling the cookies of Internet browsers was the measure least often employed, and nearly three of ten respondents had started to use different passwords for their different online accounts in the last 18 months (cf. Figure 12).



	Strong passwords	Two-factor authentication	Data encryption	Anti-virus software	OS updates	IP blockers	Anti-censorship software	VPN	Firewall protection	Safe deletion of data	Secure backups
Totally insecure	2	1	0	0	0	1	1	0	1	0	1
Insecure	2	3	1	3	3	0	1	2	2	2	1
Not sure	7	4	8	5	7	8	10	3	8	8	7
Moderately secure	8	11	6	9	5	6	5	13	7	6	6
Totally secure	0	0	2	1	3	2	0	0	0	1	2

Figure 11: Digital security perception

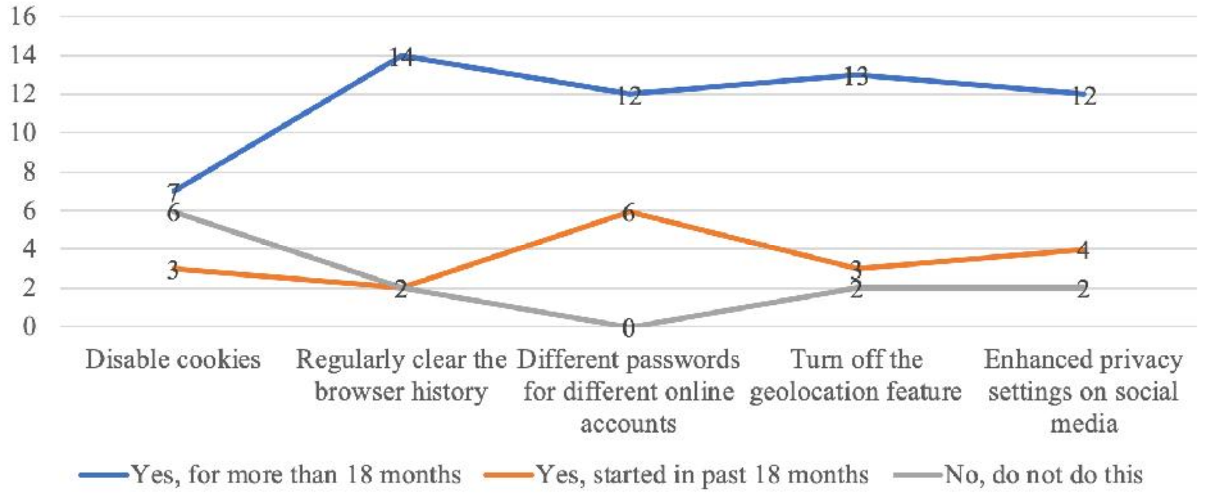


Figure 12: Digital privacy protection

6.5 Training

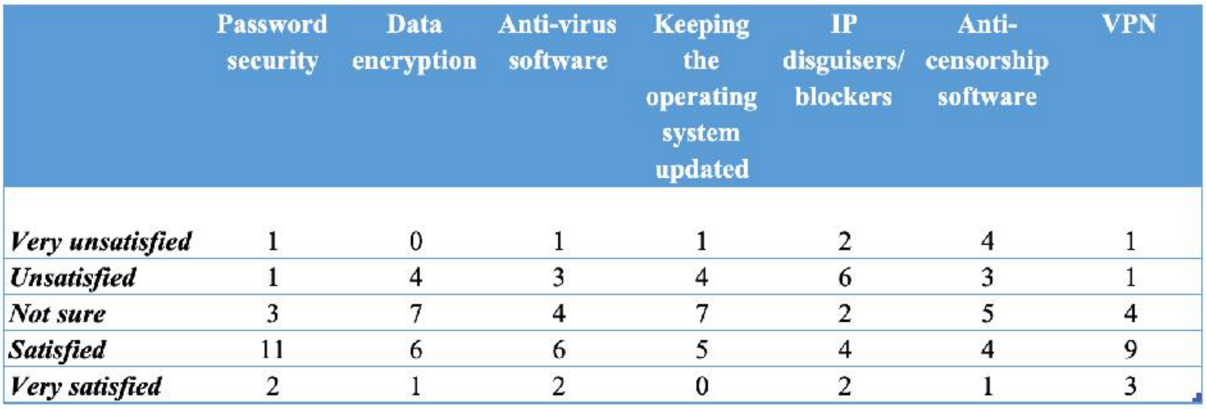
It's clear that the respondents lack the necessary knowledge about online security. Since Turkish journalism schools almost never offer courses on digital security, vocational trainings are their only sources from which to gain knowledge of this issue, and only a small share of the participants had received this kind of instruction, as the findings show.

Almost one in three journalists had had training on how to protect themselves and their sources either in the physical or digital worlds. The most common source of training for this group was a journalism conference, seminar or webinar. Nearly two-thirds said they had learned about physical safety for journalists from this type of training, and almost three of four respondents said they had received digital security training from journalism conferences, seminars or webinars. With respect to the issue of physical safety, the next most common source of relevant information was either news organizations journalists currently worked for or ones they had worked for in the past; this was also the case with digital security training, with four in ten respondents.

Participants who attended digital security training were asked how satisfied they were with courses teaching specific digital security-related topics. The respondents said they were somewhat satisfied with the course teaching password security (three-fourths) and VPN usage (two-thirds). But a majority of the journalists were either not sure or somewhat dissatisfied with topics such as data encryption, keeping the operating system updated, IP blockers and anti-censorship software usage. Almost one in three respondents said password security and data encryption were the most important topics covered in digital security training, followed by one in four respondents, who were not sure which topic was the most important (cf. Figure 13).

The journalists were also asked to rate their overall knowledge of secure digital practices. Fewer than half of respondents rated their digital security knowledge as good, and almost four in ten respondents rated their knowledge as poor or only fair (cf. Figure 14).

Finally, participants were asked to describe training needs in terms of digital security for their geographic area. Among those who commented (33), one in three respondents said that they needed "a lot of training" on digital security, without naming any specific topic, need or problem. Almost six in ten respondents who stated their specific needs in relation to digital security training said that they needed training in relation to how to protect their data on their devices or in the cloud, followed by how to protect privacy on the Internet for one-fifth of the respondents.



	Password security	Data encryption	Anti-virus software	Keeping the operating system updated	IP disguisers/ blockers	Anti-censorship software	VPN
Very unsatisfied	1	0	1	1	2	4	1
Unsatisfied	1	4	3	4	6	3	1
Not sure	3	7	4	7	2	5	4
Satisfied	11	6	6	5	4	4	9
Very satisfied	2	1	2	0	2	1	3

Figure 13: Digital security training satisfaction

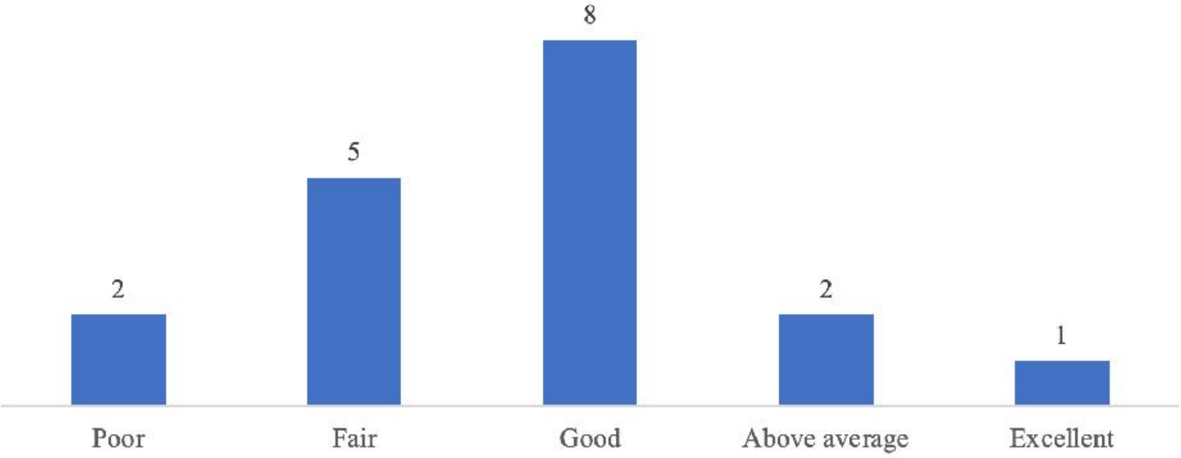


Figure 14: Overall digital security knowledge

7. Discussion and conclusions

Although discussions on the physical safety of journalists were limited to conflict areas of the world, digital security issues were of interest to all the journalists surveyed, irrespective of where they worked. However, the professional development levels of journalists depend on several factors, including economic, political and cultural ones, so that region-specific studies are critical in relation to digital security awareness and practices. Thus, this study can be understood as an initial situational assessment of the present state of the security issue in Turkey.

A vast majority of the respondents were young persons who have worked as journalists for only a relatively short period of time, with their main area of work online media. They cover difficult issues in the complex political arena of Turkey and often have to engage with security conscious and politically sensitive contacts and informants. Since all of them ranked being arrested or detained as their chief concern and believed the government had collected data in relation to their communications, safety may be seen as a key concern for journalists in Turkey during the course of their work. The figures show that this concern is not without merit, as journalists have had difficulties in relation to a number of security-related issues, ranging from personal threats to physical and digital attacks. In this sense, these findings seem consistent with the present situation in relation to journalists' working conditions, as set out at the beginning of this study. The fact that almost all the journalists saw arrest and detention as a possible consequence of their work or experienced security concerns because of their work would appear to indicate that in Turkey journalism is a profession burdened with a degree of risk. As such, within Turkey, the issue extends beyond the question of the level of safety awareness among journalists and can be regarded as also encompassing questions in relation to democracy and freedom of information.

Another important fact revealed by the study is that the journalists who participated in the survey rely heavily on digital technology and often use it in doing research, or distributing or writing stories. They were seen to use digital technology in their journalistic work to a large extent, both on mobile and stationary devices, particularly with regard to e-mail and social media usage, where security issues are most prevalent. However, when compared to the findings of the Pew Research Center's research on investigative journalists and digital security (2015), it is interesting that two in three respondents thought that for today's journalists the benefits of digital communication outweigh the risks: this figure was almost 97 percent among US journalists. The reason for the journalists' skepticism about the benefits of digital communication may be largely attributable to their lack of awareness of digital security tools which make digital communication safer for journalists. According to the findings, only a small number of participants used digital security tools to protect themselves and their sources against digital surveillance.

This low level of usage may be clearly seen in the findings. Although the respondents had a general level of awareness of the phishing attack risks posed by web links, as well as social media messages and email attachments from unknown sources, security was underrated by them when selecting e-mail or blogging services. Only one in ten respondents knew what digital-threat modeling meant, and only one in three respondents said they were aware of digital security tools for their online communications. Furthermore, it was clear that the extent of their knowledge in relation to the use of digital security tools didn't extend beyond strong passwords and VPN usage, and most respondents lacked any understanding of the level of security offered by the more complex tools and techniques available.

This situation is not exclusive to Turkey, however, with a lack of knowledge and best practice also evident in Mexico, Pakistan and South Asia. While nearly all Mexican journalists have access to and rely on the Internet, social networks, mobile phones and blogging platforms for their work, they have little or no command of digital security tools such as encryption, the use of VPNs, anonymous Internet navigation and secure file removal (Sierra, 2013). Although most Pakistani journalists and bloggers are aware of basic strategies to safeguard their online interactions, they are unaware of more sophisticated digital security tools (Bytes for All, 2012). On a broader scale, the situation is even worse in South Asia. One of every five South Asian journalists does not use secure passwords and shares passwords with colleagues. Nearly one-third of journalists in South Asia do not lock their phones despite their containing large amounts of sensitive data. One-third of South Asian journalists never encrypt emails. Nearly half of the journalists indicated they are unaware of or do not use tools to clean or hide their browsing history. For more than one-third of journalists in South Asia, digital security violations are the biggest threat, yet more than two-thirds of journalists lack any knowledge of digital security (International Federation of Journalists, 2016). However, as research shows (Pew Research Center, 2015), US journalists are particularly conscious about using digital security tools.

As previous research cited in this study also reveals, the most important means of raising the level of journalists' awareness of digital risks and of equipping them with state-of-the-art techniques with regard to digital security is to organize more training programs. The respondents' safety training experiences show why Turkish journalists have a low level of awareness of digital security, as only one in three of the journalists had taken any safety training to protect themselves and their sources either in the physical or digital worlds. As noted in previous research (Bytes for All, 2012; Pew Research Center, 2015; and Sierra, 2013) on digital security among journalists, this is a common problem globally, irrespective of locally prevailing conditions. The need for digital security training is also reflected in the respondents' answers, something which is positive in terms of their awareness of their low level of knowledge in relation to digital security. As stated by the respondents, training such as this is usually organized in Turkey by media and journalistic initiatives in the form of conferences, seminars or webinars. The problem here is that the sphere of influence of these programs is limited to journalists who have privileged access to them, which is why strong consideration should be given to including digital security as part of the curriculum in all journalism schools.

In conclusion, it is clear that journalists in Turkey are not only under online surveillance by international intelligence agencies, as the Snowden case demonstrates, but are also subject to government control through its monitoring of online channels. However, although this gives rise to difficult and unsafe working conditions, this study reveals that journalists in Turkey don't rely on digital self-defense tools as much as might be expected. As such, based on the findings of this research, relevant training programs by journalism organizations and the inclusion of digital security in journalism-school curricula would appear advisable.

References

Akser, M., & Baybars-Hawks, B. (2012). Media and Democracy in Turkey: Toward a Model of Neoliberal Media Autocracy. Middle East Journal of Culture and Communication, 5(3), 302-321.

Ataman, B., & Çoban, B. (2017). How Safe Is It? Being an activist citizen journalist in Turkey. In U. Carlsson, & R. Pöyhtäri (Eds.), The Assault on Journalism (pp. 279-288). Göteborg: NORDICOM.

Ataman, B., & Çoban, B. (2018). Counter-surveillance and alternative new media in Turkey. Information, Communication & Society, 21(7), 1014-1029.

Beiser, E. (2017, 12 13). Record number of journalists jailed as Turkey, China, Egypt pay scant price for repression. Retrieved 07 09, 2018, from Committee to Protect Journalists: https://cpj.org/reports/2017/12/journalists-prison-jail-record-number-turkey-china-egypt.php

Berger, A. A. (2000). Media and Communication Research Methods. Thousand Oaks: Sage.

Bytes for All. (2012). Digital Security and Journalists: A SnapShot of Awareness and Practice in Pakistan. Internews Center for Innovation & Learning.

Corke, S., Finkel, A., Kramer, D. J., Robbins, C. A., & Schenkkan, N. (2014). Democracy in Crisis: Corruption, Media, and Power in Turkey. Washington D.C.: Freedom House.

Çalışkan, B. (2010). Yeni İletişim Ortamlarında Gözetim: Üniversite Çalışanlarının Gözetim Algıları. Yeni İletişim Ortamları ve Etkileşim Uluslararası Konferansı Bildiri Kitabı. İstanbul: Marmara Üniversitesi İletişim Fakültesi.

Deibert, R., & Rohozinski, R. (2010). Control and Subversion in Russion Cyberspace. In R. Deibert, J. Palfrey, R. Rohozinski, & J. Zittrain (Eds.), Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace (pp. 15-34). Cambridge & London: MIT Press.

Deuze, M. (1999). Journalism and the Web: An Analysis of Skills and Standards in an Online Environment. Gazette, 61(5), 373-390.

Dolgun, U. (2008). Şeffaf Hapishane Yahut Gözetim Toplumu: Küreselleşen Dünyada Gözetim, Toplumsal Denetim ve İktidar İlişkileri. İstanbul: Ötüken Neşriyat.

European Federation of Journalists. (2018, 05). Monitoring jailed journalists in Turkey. Retrieved 07 09, 2018, from European Federation of Journalists: http://europeanjournalists.org/turkey-journalists-in-jail/

Fenton, N. (2009). New Media: Old News: Journalism and Democracy in the Digital Age. (N. Fenton, Ed.) London: SAGE.

Fenton, N. (2010). News in the Digital Age. In S. Allan (Ed.), The Routledge Companion to News and Journalism (pp. 557-567). Oxon: Routledge.

Filibeli, T. E., & İnceoğlu, Y. G. (2018). From political economy of the media to press freedom: obstacles to the implementation of peace journalism in Turkey. Conflict & Communication Online, 17(1), 1-11.

Freedom House. (2018). Democracy in Crisis: Freedom in the World 2018. Washington D.C.: Freedom House.

Greenberg, A. (2014, 10 15). Laura Poitras on the crypto tools that made her Snowden film possible. Retrieved 07 26, 2018, from Wired: https://www.wired.com/2014/10/laura-poitras-crypto-tools-made-snowden-film-possible/

Greenwald, G. (2013, 06 06). NSA collecting phone records of millions of Verizon customers daily. Retrieved 03 20, 2018, from The Guardian: https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

Greenwald, G. (2013, 06 07). NSA Prism program taps in to user data of Apple, Google and others. Retrieved 03 20, 2018, from The Guardian: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Henrichsen, J. R., Betz, M., & Lisosky, J. M. (2015). Building digital safety for journalism: a survey of selected issues. Paris: UNESCO.

International Federation of Journalists. (2016). Safer, Smarter Journalism: Survey on Digital Security in South Asia'a Media. Brussels: International Federation of Journalists.

Lyon, D. (1994). The Electronic Eye: The Rise of Surveillance Society. Minneapolis: University of Minnesota Press.

Lyon, D. (2015). Surveillance After Snowden. Cambridge: Polity.

Media and Law Studies Association. (2018, 07 09). List of Imprisoned Journalists and Media Workers. Retrieved 07 09, 2018, from Media and Law Studies Association: https://docs.google.com/spreadsheets/d/1tGjR-e-xqoyqpKECskQauMXMPPoMD1IZL4wHG2rd1Is/edit#gid=1377181219

Miller, L. C. (1998). Power Journalism: Computer Assisted Reporting. Fort Worth, TX: Harcourt Brace.

Newman, N., Fletcher, R., Kalogeropoulos, A., Levy, D. A., & Nielsen, R. K. (2018). Reuters Institute Digital News Report 2018. Oxford: Reuters Institute for the Study of Journalism.

Oliver, J. (2018, 01 08). Journalism schools still behind on cybersecurity training, new survey finds. Retrieved 08 09, 2018, from Columbia Journalism Review: https://www.cjr.org/innovations/journalism-schools-behind-cybersecurity.php

Pew Research Center. (2015). Investigative Journalists and Digital Security. Pew Research Center.

Poitras, L., Rosenbach, M., Schmid, F., & Stark, H. (2013, 06 29). NSA Spied on European Union Offices. Retrieved 03 20, 2018, from Der Spiegel: http://www.spiegel.de/international/europe/nsa-spied-on-european-union-offices-a-908590.html

Ramos, J. G. (2016). Journalist Security in the Digital World: A Survey. Are We Using the Right Tools? Center for International Media Assistance.

Reddick, R., & King, E. (1997). The Online Journalist: Using the Internet and other Electronic Resources. Fort Worth, TX: Harcourt Brace.

Reitman, J. (2013, 12 04). Snowden and Greenwald: The Men Who Leaked the Secrets. Retrieved 07 26, 2018, from Rolling Stone: https://www.rollingstone.com/culture/culture-news/snowden-and-greenwald-the-men-who-leaked-the-secrets-104970/

Shaheen, K. (2017, 10 25). Turkish judge bails eight human rights activists. Retrieved 07 12, 2018, from The Guardian: https://www.theguardian.com/world/2017/oct/25/turkish-judge-bails-eight-amnesty-human-rights-activists

Sierra, J. L. (2013). Digital and Mobile Security for Mexican Journalists and Bloggers. Freedom House & International Center for Journalists.

Singer, J. (1998). Online Journalists: Foundation for Research into their Changing Roles. Journal of Computer Mediated Communication, 4(1).

Singer, J. (2001). The Metro Wide Web: Changes in Newspapers Gatekeeping Role Online. Journalism and Mass Communication Quarterly, 78(1), 65-80.

Singer, J. (2003). Who Are These Guys? The online challenge to the notion of journalistic professionalism. Journalism: Theory, Practice and Criticism, 4(2), 139-168.

The Citizen Lab. (2013, 10 21). Monitoring Information Controls During the Bali IGF. Retrieved 07 16, 2018, from The Citizen Lab: https://citizenlab.ca/2013/10/monitoring-information-controls-bali-igf/

Turkish Statistical Institute. (2017, 08). Hanehalkı Bilişim Teknolojileri Kullanım Araştırması 2017. Retrieved 08 07, 2018, from Turkish Statistical Institute: http://www.tuik.gov.tr/HbPrint.do?id=24862

Villareal, M. G. (2017). The Protection of Citizen Journalists during Armed Conflicts: A legal approach. In U. Carlsson, & R. Pöyhtäri (Eds.), PöyhtäriThe Assault on Journalism (pp. 267-278). Göteborg: Nordicom.

Wagstaff, J. (2014). Journalists, media under attack from hackers: Google researchers. Retrieved 03 27, 2017, from http://www.reuters.com/article/us-media-cybercrime-idUSBREA2R0EU20140328

Walker, M. (2014). Privacy vs. Security: Smart Dust and Human Extinction. In R. Luppicini (Ed.), Evolving Issues Surrounding Technoethics and Society in the Digital Age (pp. 245-257). Hershey: IGI Global.

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

Yeşil, B., & Sözeri, E. K. (2017). Online Surveillance in Turkey: Legislation, Technology and Citizen Involvement. Surveillance & Society, 15(3/4), 543-549.

Yeşil, B., Sözeri, E. K., & Khazraee, E. (2017). Turkey's Internet Policy after the Coup Attempt: The Emergence of a Distributed Network of Online Suppression and Surveillance. Philadelphia: Internet Policy Observatory.

The author:

Behlül Çalışkan, born in 1982, received a Master's Degree at Marmara University based on his research into user interactions in online newspapers. In 2016, he completed his PhD in journalism at the same university with a dissertation entitled "The Impact of Information Leaks on Journalism in a Networked Society". In his academic works, he has mostly focused on theoretical and empirical studies on media, communication and culture in Turkey. His research has concentrated on topics such as new media, digital journalism and information leaks.
eMail: behlulcaliskan@gmail.com