Journalism Research
2022, Vol 5 (3) p. 234-252
ISSN 2569-152X
DOI: 10.1453/2569-152X-32022-12693-en

HERBERT VON HALEM VERLAG

Research Paper

Sahar Khamis and Khalid Al-Jaber

Counter digital revolution, disinformation, and journalistic constraints in Arab media

Abstract: **The spread of social media platforms ushered the beginning of an unprecedented communication era, which is borderless, immediate, widespread, and defies restrictions and censorship. Digital technology aided the spread of democracy and freedom of expression and helped to overthrow some Arab regimes in 2011. At that time, it was believed that these platforms paved the way for democracy by allowing citizens to easily circumvent governmental censorship, and by facilitating communication, networking, and organization among activists, thus weakening authoritarian regimes. These assumptions were overly optimistic, as the detours in democratization and political reform in the Arab region over a decade later illustrate. This article tackles the exploitation of new media, and the laws and regulations governing them, by Arab authoritarian regimes to crack down on opponents, activists, and journalists, oftentimes under the mantle of fighting disinformation, using a plethora of techniques. It also illustrates how disinformation could spread rapidly through governmentally orchestrated campaigns via new communication tools, causing serious political consequences and high risks to activists and journalists, while aiding counter revolutions. The constraining implications of these complex phenomena on Arab journalism will be explored, especially in the aftermath of the COVID-19 pandemic.**

1. Fake news: A new term for an old phenomenon

Nowadays, *fake news* has become a common term describing false or misleading information which serves someone's political or economic interests, at the expense of the truth. However, governments' reliance on propaganda and fake news to undermine, stigmatize, or exclude their opponents is not a new

phenomenon. Misinformation and disinformation have always been used to influence public opinion, in line with the ideas and goals of the misleading rulers. The aim was always to change perceptions, distort views, influence minds, and manipulate emotions to create doubts, confusion, and brainwashing around serious issues of key importance.

American historian Robert Darnton of Harvard University alerts us that, »the concoction of alternative facts is hardly rare, and the equivalent of today's poisonous, bite-size texts and tweets can be found in most periods of history, going back to the ancients« (DRANTON 2017). He cites a very ancient example from the Byzantine era, pointing to the anecdotes of the 6th-century Byzantine historian Procopius, which are considered among the first examples of media misinformation. These secret proto-blogs were full of »doubtful information« on the scandals of one of the rulers, with the intention of smearing his reputation (DARNTON 2017).

Likewise, Olivier Thibaut reminds us that, »In capital letters and with an exclamation mark, ›FAKE NEWS!‹ may have been popularized by Donald Trump in hundreds of his tweets but the concept has existed for centuries« (THIBAUT 2018). He cites François Bernard Huyghe, a research fellow at the Institute for International and Strategic Affairs, who mentioned that media disinformation which spread during the Cold War was characterized by the »deliberate spreading of false information to influence opinion and weaken an enemy,« especially in the Western camp (THIBAUT 2018). One of the most notable examples was a Soviet intelligence propaganda campaign which began in 1983 by publishing an article in an Indian newspaper claiming that HIV was a biological weapon developed in U.S. military laboratories (GRIMES 2017). A more recent example of these disinformation battles, albeit coming from the West this time, is the claim that the COVID-19 virus may have been deliberately manufactured inside a Chinese lab in Wuhan, and later on leaked from this lab (RUWITCH 2021).

An infamous example of politicized and misleading information in the Arab world was the coverage of the June 1967 war in the radio station *Sawt Al Arab* (The Voice of the Arabs). Egyptian radio broadcaster Ahmed Saeed was given orders by the Egyptian government to project a false victory of the Egyptian forces in the war with Israel, which later proved to be incorrect. While he falsely reported the shooting down of dozens of Israeli planes and the destruction of hundreds of pieces of Israeli tanks, the war ended with Israel's occupation of more Palestinian land, the Sinai Peninsula in Egypt, and the Golan Heights in Syria (BOWEN 2017). Following this military defeat, Ahmed Saeed submitted his resignation and confessed before his death that the content of his broadcast was dictated by top state officials.

Today, the challenge of spreading misinformation and disinformation continues, albeit in different forms, at a much faster pace, and with stronger impact, thanks to the communication revolution and new digital technologies. This

impacted the authenticity, credibility, and seriousness of journalistic coverage in some cases, as some media outlets, in the absence of serious reporting and professional journalistic standards, fall victim to governmental pressure to spread deceptive propaganda, misinformation, and disinformation to serve the regime's agenda (KHAMIS/EL-IBIARY 2022).

2. Social media and global disinformation

More than ever before, social media, especially Facebook and Twitter, are facing multiple accusations of becoming platforms for spreading misinformation and disinformation, thus contributing to undermining democracy around the world, through serving politicians' agendas and helping them stir up social divisions, tarnish the image of minorities, and smear rival groups. This increases the threat of social media shifting from useful informational tools to serve the public to dangerous social control tools which are manipulated by politicians in both democratic and authoritarian regimes, although the risk is always higher under authoritarian governments (BANJO 2019).

The presidential elections in the United States in 2016 and in Brazil in 2018 provided evidence that social media could be ideal tools for spreading rumors and disinformation, resulting in increased polarization and dangerous fragmentation. After Facebook's confirmation that Russian entities funded promotional messages through its network during the U.S. presidential election in 2016 to support Donald Trump (CNN 2019), Twitter also confirmed that it had been targeted by similar campaigns, despite both platforms continued claims to support democracy.

Both platforms bowed to pressure and agreed to cooperate with Congress in investigating possible Russian interference in Donald Trump's election. Although the Kremlin has repeatedly denied such accusations, Facebook admitted that mysterious Russian companies and institutions have deceived them and published thousands of ads on their pages that interfered with the U.S. presidential election of 2016 in which Republican nominee Donald Trump won (SHANE/GOEL 2017). Later on, Twitter did the same (SWAINE 2018).

When the American public first heard about Russian meddling in the 2016 presidential elections, many simply shrugged it off as unbelievable and dismissed it as unrealistic. However, over time, more Americans, especially democrats, liberals, and independents, started to realize the inconvenient truth regarding the role of social media platforms in influencing the 2016 election's results (SHANE/GOEL 2017; SWAINE 2018).

According to a University of Oxford study which surveyed 28 countries, many authoritarian governments, including most Arab countries, use the services of

large numbers of technologically savvy employees to create content which can influence the public opinion of their people, both inside their countries and abroad, while also shaping international public opinion about these countries. The study concluded that »every authoritarian regime has social media campaigns targeting their own populations« (BRADSHAW/HOWARD 2017). The study revealed that fabricated news, which is oftentimes more exciting than verified facts, is spreading more quickly via the internet, due to the speed of widely spreading large amounts of content online, regardless of the accuracy of the shared information (BRADSHAW/HOWARD 2017).

Another report by Freedom House (2017) found that the elections in 18 countries were impacted by misinformation and disinformation, which have been propagated through online campaigns. The report revealed the efforts exerted by these governments to influence online rhetoric and public opinion, both at home and abroad. Additionally, the report, which examined freedom to use the internet in 65 countries and covered about 87 percent of the world's internet users, also discussed how 30 governments were involved in using social media to stifle dissent. It indicated that for the seventh consecutive year, worldwide freedom indicators dropped, as governments stepped up their efforts to influence the internet users' online discussions, actions, and interactions (FREEDOM HOUSE 2017).

In the face of this surging wave of media disinformation, large media organizations, which often partner with high-tech companies and social media platforms, are starting to strengthen their monitoring, fact-checking, and other investigative activities to support fact-based journalism. However, these efforts remain limited in the face of the tide of social media influence, and its far reaching implications, coupled with the significant exploitation of these platforms by governments and various other entities to serve their agendas.

3. Social media and the counter revolution: From liberation to repression

When the Arab Spring uprisings erupted in 2011, the high hopes for political reform and a smooth transition to democratization (LYNCH 2012; 2016) were coupled with equally high expectations attached to the democratizing potentials of new media, which were believed to pave the way for the revolutionary transitions, widen the margin of freedom of expression, and act as catalysts and amplifiers for political change (EL TANTAWY/WIEST 2011).

Authoritarian governments in most of the Arab world were not prepared for the new tide of freedom of expression which was made possible through social media platforms at that time, as well as the various organizational and networking opportunities they made possible for activists. For decades, many of these

governments invested in controlling and manipulating mainstream media, through a plethora of direct and indirect techniques and mechanisms (SAKR 2013; SEIB 2007). However, they lagged behind the young activists in the Arab region when it came to jumping on the technological bandwagon.

Over a decade since the eruption of these uprisings, however, we are witnessing an entirely different reality in the Arab region, with the detours and backlashes in the so-called post-Arab Spring countries. These range from sectarian strife and statelessness in Libya and a brutal civil war in Syria to a crushed uprising in Bahrain, a return to military dictatorship in Egypt, and a devastating war in Yemen. Even the only country which was perceived as the sole success story, namely Tunisia, suffered from democratic setbacks recently.

These undesirable outcomes encouraged governments in both Arab Spring and non-Arab Spring countries to engage in relentless efforts to keep up with the new wave of »cyberactivism« (HOWARD 2011) to build their digital capacities, control the mediated narratives, and counter dissent, albeit through different techniques and for different reasons. The governments of Arab Spring countries, which experienced these unfortunate outcomes, felt a dire need to control the mediated narratives to avoid the eruption of new waves of public dissent and revolt. The governments of non-Arab Spring countries engaged in similar practices to prevent the eruption of uprisings in the first place and to avoid facing similar outcomes.

Some of these governments' efforts included creating »electronic armies« using automated accounts which authoritarian regimes deployed like riot police over the internet. One good example is the »Syrian Electronic Army,« which the Syrian regime effectively utilized to trace its opponents online, in an effort to troll, hack, sabotage, and block their digital activities. Interestingly, this army of online hackers has been praised by Syria's dictator, Bashar Al Assad, for its patriotism (KHAMIS/GOLD/VAUGHN 2013).

These digitally repressive efforts signaled a shift from the optimistic, or even utopian, phase of »techno-euphoria« to a new phase characterized by the harsh reality of »digital authoritarianism,« which has been steadily on the rise in the Arab World in recent years (JONES 2022; KHAMIS 2020a).

In this new post-Arab Spring phase of »digital authoritarianism,« thousands of accounts on Twitter and Facebook turned out to be propaganda horns for governments. Some belong to influencers who appear to have joined their authoritarian government's propaganda efforts either willingly or under duress. Others were previously unknown but received thousands of followers and the Twitter verification mark in record time. For each of these influencers, there are hundreds of smaller accounts which seem to be managed by different groups, serving as infantry soldiers in a well-coordinated online army.

In 2019, large tech companies admitted to cracking down on fake accounts that sought to target or silence the regimes' critics and regional rivals. In August 2019, Facebook admitted to dismantling an orchestrated online campaign associated with the government of Saudi Arabia. In total, Facebook proceeded to suspend roughly 350 accounts that had spent over $100,000 in order to reach over 1.4 million individual followers via advertisements. While the government of Saudi Arabia officially denied any involvement in the operation, a representative from Facebook stated: »For this operation, our investigators were able to confirm that the individuals behind this are associated with the government of Saudi Arabia… Anytime we have a link between an information operation and a government, that's significant and people should be aware« (STUBBS 2019).

In a separate incident, occurring around the same time, Facebook also admitted suspending 350 fake accounts associated with the governments of Egypt and the United Arab Emirates, but fell short of accusing these governments of being behind the account operations. These accounts mostly targeted these countries' regional rival Qatar, during the Gulf blockade at that time, and they also engaged in spreading misinformation and disinformation around different issues (STUBBS 2019).

Twitter also announced the cancellation of 5,929 accounts associated with a Saudi company believed to be tracking dissidents online (STONE 2019). Twitter later clarified that these accounts were only a random sample of the 88,000 accounts the company had flagged as possibly being used to spread Saudi propaganda online (MILLER 2019).

According to Human Rights Watch, the economically affluent and technologically savvy governments of the Gulf Cooperation Council (GCC) countries have used surveillance technologies purchased from »Western and Israeli companies« to track the activities of some of their citizens online (HUMAN RIGHTS WATCH 2016). The report noted that these governments used a »spy program,« based on evidence provided by the Citizen Lab research group in Toronto. This program, which is designed by the infamous Israeli spyware company NSO, allows »access to emails, text messages, call histories, contact lists, files, and potentially passwords, and can allow authorities to turn on a phone or laptop's camera and microphone to take pictures, or record video and conversations without the owner's knowledge« (HUMAN RIGHTS WATCH 2016). The danger here is that »[t]hese companies apply techniques as sophisticated, or perhaps more sophisticated, than U.S. intelligence agencies,« according to Sasha Romanosky, a policy researcher at the RAND Corporation (ROMANOSKY 2017). According to the Citizen Lab, about 175 people have been targeted by espionage programs developed by NSO since 2016, including human rights activists and dissidents (ZILBER 2018).

In 2016, Citizen Lab reported that it discovered a campaign of spyware attacks by a sophisticated operator against Emirati journalists, activists and dissidents

(MARCZAK/SCOTT-RAILTON 2016). The State of Bahrain is at the top of the list of authoritarian countries that buy spying devices from the State of Israel and use them to spy on its citizens according to an investigative article published by the Israeli newspaper *Haaretz* (SHEZAF/JACOBSON 2018). Another article in *Haaretz* revealed that the Israeli spyware group NSO has struck a deal with Saudi officials to sell them a $55 million cell phone hacking program called Pegasus 3, just a few months before the Saudi Crown Prince MbS launched a crackdown campaign on his opponents at home (HAREL/LEVINSON/KUBOVICH 2018).

One of the most high-profile cases of cyber-surveillance in the Gulf region is that of the young Saudi women's rights activist Loujain Al-Hathloul, who was imprisoned by the Saudi government in 2018. According to some reports, the arrest of Al-Hathloul came after collaboration between Saudi authorities and the UAE's Project DREAD, a cyber-surveillance unit established with the help of American ex-intelligence community operatives (HASAN 2019).

Citizen Lab scanned the internet for servers linked to the Israeli spyware program, Pegasus, and found evidence of usage in 45 countries worldwide, including 17 Middle Eastern countries. The Citizen Lab report identified what appears to be a significant expansion of Pegasus use in the GCC. Overall, at least six operators have been identified with significant operations in the GCC, two of which appear to be mostly focused on the UAE, one focused mostly on Bahrain, and another focused on Saudi Arabia (MARCZAK et al. 2018).

A heated controversy around the social media messaging app ToTok, not to be confused with TikTok, illustrated the Israeli-Emirati collaboration that has facilitated the proliferation of surveillance technologies in the UAE. Originally marketed as a free video, voice, and messaging app within the UAE, further evidence suggested that the app's original intention was to spy on conversations by those using the service. Unbeknownst to customers, the app was continually monitoring users' location and communications and could even use the microphone and camera to listen-in on conversations (*The Guardian* 2019). A deeper investigation revealed that the messaging app was actually developed by Israeli ex-intelligence officials who went on to work for DarkMatter, an Abu Dhabi-based cybersecurity company (HAARETZ 2019). In the days following the story's breaking, the app became unavailable for download on the Apple App Store and Google Play Store, although the company's leadership said that the unavailability was temporary and related to a »technical issue« (BBC 2019). Most importantly, the UAE government denied that the app was intended for use as a spy tool (*The Times of Israel* 2019), and the creator of the app denied having any affiliation with any government.

In a belated step intended to avoid ethical and legal consequences, Twitter removed fake and shady accounts in 2019, which were mostly concentrated in Egypt, Saudi Arabia, and the United Arab Emirates, for spreading misleading

information on political and military conflicts in the Middle East (NPR 2019). Twitter also suspended 4,258 »fake UAE« accounts, which were suspected of promoting false news about the Yemen war, where Saudi Arabia has been leading a military coalition against Iran-backed Houthis since 2015 (NEWS 1 2019).

One of the Arab governments which has been widely known for tracing its opponents online is Saudi Arabia. An infamous incident which came to be known as the »Twitter spy scandal« surfaced when two former Twitter employees were charged by the Justice Department in the United States with spying on behalf of the government of Saudi Arabia (NAKASHIMA/BENSINGER 2019). While at Twitter, they were able to browse the records of thousands of Twitter users in order to identify the opponents and critics of the kingdom. Some of the accounts which have been traced by these two spies belonged to activists who have been tweeting using aliases and pseudonyms to protect their identities, ensure their personal safety, and avoid state retaliation. A third person was also accused of acting as the liaison between some Saudi officials and the two former Twitter employees facilitating this unlawful data breach (BBC 2019).

The significance of this story is that associates of an Arab Gulf state were able to successfully exploit their positions as Twitter employees to access large databases and obtain personal information belonging to some government critics. The danger here is that social media which is supposed to act as a safe venue for Saudi citizens, as well as citizens from other Arab states, to come together to discuss issues they otherwise have no place or space to discuss, became an arena for Saudi authorities to trace its opponents, with the intention of curtailing critical voices (BLOOMBERG 2019). Through such actions on the part of authoritarian regimes, including unmasking the identities of those who hide behind anonymous accounts, social media is becoming an increasingly insecure and unsafe place for the critics of Arab regimes, as more of these governments strive to collect information on their dissidents and opponents online, with the intention of targeting them and silencing them (KHAMIS 2019).

The shocking facts revealed in this scandal raise serious questions regarding the dual role of social media as a double-edged sword, namely as tools for liberation and repression, simultaneously (BRUMFIELD 2019). They also raise red flags around issues of data governance, internet freedom, and foreign governments' exploitation of social media's vast databases. Additionally, the complex context through which this scandal came to fruition, through a mixture of illegal activities, including bribery, corruption, and exploitation, draws some interesting, yet troubling, parallels to other incidents (KHAMIS 2019).

For example, given that the »Twitter spy scandal« exposes the danger of a foreign power exploiting American social media platforms to identify critics and suppress their voices, a parallel could be drawn with the Russian interference in the 2016 presidential elections in the United States, despite the different context,

aims, and scope, since both incidents involved foreign governments and took place online through mastering cyberspace tactics and techniques, including hacking (CNN 2019).

There are also some parallels between the Saudi Twitter scandal and the data breach scandal involving Facebook and Cambridge Analytica, in which the personal data and private information of a large number of Facebook users were leaked (*South China Morning Post* 2018). Both incidents raised the alarm regarding the dangers of invasion of privacy and the threats to online data security, shaking confidence in social media platforms and shattering their credibility in the eyes of many users.

Most importantly, at least one individual named in the Twitter scandal's court documents appeared to be an associate of Saudi officials whom the CIA has concluded with a high degree of confidence likely ordered the assassination of famous journalist Jamal Khashoggi in 2018 (HARRIS/MILLER/DAWSEY 2018).

The New York Times published an article indicating that Saudi Arabia had deployed an »electronic army« to target journalist Jamal Khashoggi, who was horrifically killed inside the Saudi consulate in Istanbul, and other critics of the Saudi regime on Twitter, in addition to using the services of the recruited spies inside Twitter. The article indicated that Khashoggi's online attackers were part of a broad effort by Crown Prince Mohammed bin Salman (MbS) and his close advisers to silence critics inside and outside the kingdom. Hundreds of people worked in an »electronic committee« based in the capital Riyadh to turn public opinion against dissidents (BENNER et al. 2018).

Moreover, one of the 6,000 Twitter accounts which were hacked on behalf of the Saudi government (MORRIS 2018) belonged to the prominent Saudi dissident and regime critic, Omar Abdulaziz, a young blogger living in self-exile in Canada, who developed a close friendship with the late Jamal Khashoggi and announced his commitment to continue the journey which was started by his late friend to champion the cause of reform in his home country (KHAMIS/FOWLER 2020).

The infamous case of journalist Jamal Khashoggi's gruesome murder also has its origins in Saudi cyber-surveillance efforts. According to Saudi critic and prominent blogger Omar Abdulaziz, his communications with his late friend Khashoggi which involved any criticism of the Saudi regime were monitored by the Saudi regime, without his prior knowledge (BRAGA 2018). Therefore, Abdulaziz sued NSO, the infamous Israeli spyware company which allegedly sold this spyware capability to the Saudis (*The Times of Israel* 2018).

Another case involved the prolific Saudi Twitter activist Ghanem Almasarir, who is believed to have been hacked by the Saudis using the same Israeli technology. In both cases, users were sent suspicious text messages with links that when clicked on would allow the spy software to infiltrate their devices and to access their mobile phones' cameras and microphones (SILVERSTEIN 2019).

Such incidents are a stark reminder that in the post-Arab Spring phase, Arab regimes' critics, whether they are activists, opponents, or truth-seeking journalists, are not safe from governmental surveillance, tracing, trolling, hacking, and, ultimately, retaliation, even when they seek to protect their personal safety through self-exile in the diaspora (KHAMIS/FOWLER 2020).

4. The COVID-19 era and the battle over the truth

The counter digital revolution in the Arab region exacerbated amid the COVID-19 pandemic, as various Arab regimes started deploying new tools and using innovative mechanisms to ensure that the official, state-orchestrated narrative around the pandemic dominates all media platforms, without being challenged in different journalistic sources. The surge in people's desire to seek information about the pandemic was alarming to many authoritarian governments in the region, for whom any window for gaining access to non-state controlled information was instantly perceived as a threat which needed to be eliminated (KHAMIS 2020b).

Arab governments' struggle to control, and define, the official narrative around the COVID-19 pandemic, including statistics about infections and death rates, according to their own interests and agendas, resulted in a dual outcome. On one hand, it increased the reliance on manipulated, state-controlled official media outlets, as their main communication tools. On the other hand, their desire to ensure »maximum narrative control« resulted in cracking down on both local and international media outlets and journalists, who dared to challenge the officially crafted narrative (*Middle East Eye Correspondent* 2020). This new phase of »weaponized censorship« led to the demise of free expression, including journalistic freedom, in many Arab countries (MARZOUK 2020). For example, a number of Arab governments cracked down harshly on both local and foreign media outlets in retaliation for noncompliant COVID-19 reporting, under the pretext of spreading disinformation (KHAMIS 2020b).

Some examples included the detention of Lina Attalah, the Editor-in-Chief of the website *Mada Masr*, known as Egypt's last independent media outlet, the journalist Hassan Mahgoub, and an editor, Atef Hasballah, in the midst of a growing wave of crackdown on press freedom linked to COVID-19 reporting (MICHAELSON 2020). One infamous case was that of the late 65-year-old Egyptian journalist, Mohamed Mounir, who was believed to be »murdered by Coronavirus« (MYERS 2020) twice. One time when daring to report on it, in a manner which angered the Egyptian authorities, and another time when paying his life as a price for this reporting, after contracting the virus in a crowded Egyptian jail and dying from COVID-19-related complications a few days after his release from jail (KHAMIS 2020b). Even international reporters and foreign correspondents were

not immune to this surging wave of governmental repression. One example was the infamous case of the *Guardian* correspondent Ruth Michaelson, whose press credentials were revoked and who was expelled from Egypt, after publishing an article citing a higher number of COVID-19 cases in Egypt than officially declared by the Egyptian government (SANDERS IV 2020).

The techniques utilized by authoritarian Arab regimes ranged from closing down websites to arresting local journalists and ousting international correspondents, as well as exploiting punitive legal codes and laws, such as »cybercrime laws,« and other restrictive measures, to tighten their grip on all media outlets, under the guise of countering »disinformation.« The danger behind these new laws and regulations is that they were oftentimes broad, obscure, and vague on purpose to criminalize any reporting which falls outside the realm of state approval or which contradicts the official, governmental narrative about the pandemic. Such reporting was oftentimes criminalized as spreading »false news« online, which could be punishable by a five years' jail sentence and paying steep fines in some Arab countries, such as Egypt (ASSOCIATED PRESS 2020).

Moreover, some Arab governments effectively utilized new online surveillance tools and techniques, including digital contact tracing applications, for the purpose of monitoring COVID-19 cases and identifying the location, mobility, and social networks of those who tested positive. Such advanced digital applications are more widely used in the affluent and more technologically developed Arab Gulf countries (NAFIE 2020). Although such applications are meant to slow down the spread of the pandemic, there are numerous dangers associated with them, such as facilitating hacking activities, the use of spyware tools, and invasion of privacy practices which are deployed by Arab authoritarian regimes. While these digital tools have been sanctioned and legitimized, under the mantle of tracing the spread of the virus, they could also be utilized effectively to trace the regimes' opponents and critics, including activists and truth-revealing journalists (KHAMIS 2020b). According to the Committee to Protect Journalists (CPJ) »Covid-19 and Press Freedom« map and report, which document the types and locations of various COVID-19-related threats, many violations by Arab regimes against press freedom, including shutting down numerous websites, restricting access to them, and/or arresting journalists, were widespread throughout the region amid the pandemic (CPJ 2020).

Overall, the toolkit of repressive measures which were deployed by Arab regimes amid the pandemic included: Laws against »fake news;« jailing journalists; suspending free speech; blunt censorship; threatening and harassing journalists; denying accreditation requests; restricting freedom of movement; restricting access to information; expulsions and visa restrictions; surveillance and contact tracing; and emergency measures (JACOBSEN 2020).

5. Concluding remarks: The road ahead

As the tug-of-war between Arab regimes and those who dare to expose their wrongdoings, including truth-seeking journalists, critics, and activists, continues, it is most likely that the battle over the disseminated content via legacy media and digital media, who controls it, and how, will also continue.

The spread of propaganda and extensive misleading information on a wide scale through social media platforms leads to manipulating and deceiving public opinion, both at home and abroad, which is an important weapon in the hands of authoritarian regimes. Therefore, it is crucial to validate the news which is transmitted through these platforms to curtail such harmful effects. This is especially important in light of the increased reliance on social media as sources of information, especially among young people.

According to a Pew Research Center survey (2021), around seven-in-ten Americans are using social media to connect with one another, engage with news content, share information, and entertain themselves, with the new generation turning entirely to social media, and 61 % of those surveyed developing their political views based on Facebook's content, while only 31 % rely on legacy media, such as television. The reliance on social media also increased significantly in the Arab world in recent years. For example, 98 % of Saudi Arabia's population are internet users and 82 % rely heavily on social media for news and entertainment (*Global Media Insight* 2022). The United Arab Emirates has a staggering figure of 106 % social media usage (individual users can have more than one social media account), as of January 2022 (DATA REPORTAL 2022). Therefore, social media should be platforms where people disseminate, and receive, correct information and verified news from reliable sources, rather than disinformation and propaganda.

However, in an era in which cyberwars between governments and their opponents are constantly escalating, terrifying incidents such as the »Twitter Spy Scandal,« and many others, signal real dangers and serious threats to the lives of those who dare to speak up against repressive regimes (AKKAD 2019), including activists, critics, and journalists. The social responsibility, and credibility, of the social media industry is now in question, as such incidents certainly raise concerns about Silicon Valley's ability to protect the private information of its users, in general, and the dissidents and opponents of repressive governments, in particular. The challenges facing social media companies today include developing mechanisms to keep their data secure, not only from hackers, but also from rogue employees (*South China Morning Post* 2019). It is essential for social media giants, such as Facebook and Twitter, to come up with new policies that determine who can and cannot have access to their databases, and in what ways (TIFFANY 2019). Additionally, they must draft clear rules and regulations to ensure

the safety and protection of their data from manipulation, whether by foreign governments and other entities or by their own staff and insiders.

Since these threats and challenges are multifaceted, they require equally multifaceted strategies to combat them. One way to overcome such threats in the future is involving Silicon Valley companies in drafting and implementing effective and transparent new policies. This could restore the public's trust in the social media giants' integrity and credibility.

Another equally important issue is spreading much-needed media literacy skills among audiences, through proper education, training, and awareness campaigns. Many internet users are, unfortunately, not adept at distinguishing between fabricated content and accurate news. This poses many risks to online audiences who lack the needed awareness, ranging from falling victim to state propaganda to falling victim to the recruitment efforts of extremist or terrorist groups online, and everything in between.

It is the hope that if all of these measures, and others, are effectively implemented that some of the risks and dangers of this new phase of digital authoritarianism and counter digital revolution in the Arab region, and elsewhere, could be monitored, tackled, minimized, or even prevented, moving forward.

About the authors

Dr. Sahar Khamis is an Associate Professor in the Department of Communication and an Affiliate Professor in the Department of Women's Studies at the University of Maryland, College Park. She is an expert on Arab and Muslim media, and the former Head of the Mass Communication Department at Qatar University. Dr. Khamis holds a Ph.D. in Mass Media and Cultural Studies from the University of Manchester in England. She is the co-author of the books: *Islam Dot Com: Contemporary Islamic Discourses in Cyberspace* (Palgrave Macmillan, 2009) and *Egyptian Revolution 2.0: Political Blogging, Civic Engagement and Citizen Journalism* (Palgrave Macmillan, 2013). She is the co-editor of the book: *Arab Women's Activism and Socio-Political Transformation: Unfinished Gendered Revolutions* (Palgrave Macmillan, 2018). Contact: skhamis@umd.edu

Dr. Khalid Al-Jaber is the Director of the MENA Center in Washington D.C. and an Assistant Professor of Political Communication at the Gulf Studies Program at Qatar University. Previously, he worked at Al-Sharq Studies & Research Center and he was the Editor-in-Chief of *The Peninsula*, Qatar's leading English language daily newspaper. Al-Jaber is a scholar of Arab and Gulf Studies. His research focuses on political science, public diplomacy, international communication, and international relations. He published several academic books and contributed to several

professional journals. Dr. Al-Jaber obtained his PhD from the University of Leicester in the UK and his MA from the University of West Florida in the USA.

Translation of the German version of this article by Kerstin Trimble, with financial support by the Otto Brenner Foundation.

References

AKKAD, DANIA (2019): Twitter's Saudi Spy Network Leaves Activists Living in Fear. In: *Middle East Eye*, 18 November 2019.

ASSOCIATED PRESS (AP) (2020):Egypt arrests doctors, silences critics over virus outbreak. In: *The Washington Post*, 6 July 2020. https://www.washingtonpost.com/health/egypt-arrests-doctors-silences-critics-over-virus-outbreak/2020/07/06/65eb7984-bf50-11ea-8908-68a2b9eae9e0_story.html

BANJO, SHELLY: Facebook, Twitter and the Digital Disinformation Mess. In: *The Washington Post*, 2 October 2019. https://www.washingtonpost.com/business/facebook-twitter-and-the-digital-disinformation-mess/2019/10/01/53334c08-e4b4-11e9-b0a6-3d03721b85ef_story.html

BBC (2019): Ex-Twitter Employees Accused of Spying for Saudi Arabia. In: BBC, 7 November 2019.

BBC (2019): Google and Apple Remove Alleged UAE Spy App ToTok. In: BBC, 23 December 2019. https://www.bbc.com/news/technology-5089084

BENNER, KATIE; MAZZETTI, MARK; HUBBARD, BEN; ISAAC, MIKE (2018): Saudi's Image Makers. A Troll Army and a Twitter Insider. In: *The New York Times*, 20 October 2018. https://www.nytimes.com/2018/10/20/us/politics/saudi-image-campaign-twitter.html

BLOOMBERG (2019): Two Ex-Twitter Employees Charged With Spying for Saudi Arabia. In: *Bloomberg*, 7 November 2019.

BOWEN, JEREMY (2017): 1967 War: Six Days that Changed the Middle East. In: BBC, 5 June 2017. https://www.bbc.com/news/world-middle-east-3996046

BRADSHAW, SAMANTHA; HOWARD, PHILIP N. (2017): Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation. In: *Oxford University Research Archive.* https://ora.ox.ac.uk/objects/uuid:cef7e8d9-27bf-4ea5-9fd6-855209b3e1f6/download_file?file_format=pdf&safe_filename=Troops-Trolls-and-Troublemakers.pdf&type_of_work=Report

BRAGA, MATHEW (2018): A Quebecer spoke out against the Saudis – then learned he had spyware on his iPhone. In: *CBC News*, 1 October 2018. https://www.cbc.ca/news/science/omar-abdulaziz-spyware-saudi-arabia-nso-citizen-lab-quebec-1.4845179

BRUMFIELD, CYNTHIA (2019): Twitter Spy Scandal a Wake-Up Call For Companies to Clean up their Data Access Acts. In: *CSO*, 12 November 2019.

CNN (2019): 2016 Presidential Campaign Hacking Fast-Facts. In: *CNN,* 31 October 2019.

COMMITTEE TO PROTECT JOURNALISTS (CPJ) (2020): Covid-19 and press freedom. https://cpj.org/covid-19/

DARNTON, ROBERT (2017): The True History of Fake News. In: *The New York Review of Books*, 13 February 2017. https://www.nybooks.com/daily/2017/02/13/the-true-history-of-fake-news/

DATA REPORTAL (2022): Digital 2022: The United Arab Emirates. In: *Data Reportal*, 9 February 2022. https://datareportal.com/reports/digital-2022-united-arab-emirates

EL TANTAWY, NAHED; WIEST, JULIA B. (2011): Social media in the Egyptian revolution: Reconsidering resource mobilization theory. In: *International Journal of Communication*, 5, 1207-1224.

FREEDOM HOUSE (2017): New Report - Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy. In: *Freedom House*, 14 November 2017. https://freedomhouse.org/article/new-report-freedom-net-2017-manipulating-social-media-undermine-democracy

GLOBAL MEDIA INSIGHT (2022): Saudi Arabia Social Media Statistics 2022. In: *Global Media Insight*, 17 June 2022. https://www.globalmediainsight.com/blog/saudi-arabia-social-media-statistics/

GRIMES, DAVID ROBERT (2017): Russian fake news is not new: Soviet Aids propaganda cost countless lives. In: *The Guardian*, 14 June 2017. https://www.theguardian.com/science/blog/2017/jun/14/russian-fake-news-is-not-new-soviet-aids-propaganda-cost-countless-lives

HAARETZ (2019): Popular Messaging App Is UAE Spy Tool, Developed By Firm Employing Ex-NSA and Israeli Intel Officers. In: *Haaretz*, 23 December 2019. https://www.haaretz.com/middle-east-news/popular-app-is-uae-spy-tool-made-by-firm-employing-ex-israeli-intel-officers-1.8304528

HAREL, AMOS; LEVINSON, CHAIM; KUBOVICH, YANIV (2018): Isreali Cyber Firm Negotiated Advanced Attack Capabilities Sale with Saudis. In: *Haaretz*, 25 November 2018. https://www.haaretz.com/israel-news/.premium-israeli-company-negotiated-to-sell-advanced-cybertech-to-the-saudis-1.6680618

HARRIS, SHANE; MILLER, GREG; DAWSEY, JOSH (2018): CIA Concludes Saudi Crown Prince Ordered Jamal Khashoggi's Assassination. In: *Washington Post*, 16 November 2018.

HASAN, MEHDI (2019): Don't Forget that Saudi Arabia is Imprisoning and Torturing Women's Rights Activist Loujain Al-Hathloul. In: *The Intercept*, 24 December, 2019.

HOWARD, PHILIP N. (2011): *The digital origins of dictatorship and democracy: Information technology and political Isla*m. Oxford: Oxford University Press.

HUMAN RIGHTS WATCH (2016): Arab Gulf States: Attempts to Silence 140 Characters. In: *Human Rights Watch*, 1 November 2016. https://www.hrw.org/news/2016/11/01/arab-gulf-states-attempts-silence-140-characters

JACOBSEN, KATHERINE (2020): Amid Covid-19, the Prognosis for press freedom is dim. Here are 10 symptoms to track. In: *Committee to Protect Journalists* (CPJ). https://cpj.org/reports/2020/06/covid-19-here-are-10-press-freedom-symptoms-to-track/

JONES, MARC OWEN (2022). *Digital authoritarianism in the Middle East: Deception, disinformation and social media*. London: C Hurst & Co Publishers Ltd.

KHAMIS, SAHAR (2019): The Twitter Spy Scandal: Context, Parallels, Threats, and Responsibilities.« In: *Gulf International Forum*, 9 December 2019. https://gulfif.org/the-twitter-spy-scandal-context-parallels-threats-and-responsibilities/

KHAMIS, SAHAR (2020a): Between »digital euphoria« and »cyber-authoritarianism:« Technology's two faces. In: *Oasis. Christians and muslims in the global world*, (16) 31, 2020, pp. 94-102.

KHAMIS, SAHAR (2020b): A battle of two pandemics: Coronavirus and digital authoritarianism in the Arab World. In: SEXTON, MICHAEL; CAMPBELL, ELIZA (eds.): *Cyber War & Cyber Peace in the Middle East*. Washington, DC: Middle East Institute, pp. 145-162.

KHAMIS, SAHAR; EL-IBIARY, RASHA (2022): Egyptian women journalists' feminist voices in a shifting digitalized journalistic field. In: *Digital Journalism*. https://www.tandfonline.com/doi/full/10.1080/21670811.2022.2039738

KHAMIS, SAHAR; FOWLER, RANDALL (2020): Arab resistance in the diaspora: Comparing the Saudi dissident and the Egyptian whistleblower. In: *Journal of Arab & Muslim Media Research*, 13(1), pp. 31-49.

KHAMIS, SAHAR, GOLD, PAUL B. AND VAUGHN, KATHERINE (2013): Propaganda in Egypt and Syria's 'cyberwars': Contexts, actors, tools, and tactics. In: AUERBACH, JONATHAN; CASTRONOVO, RUSS (eds.): *The Oxford handbook to propaganda studies*. New York: Oxford University Press, pp. 418-438.

LYNCH, MARC (2012): *The Arab uprising: The unfinished revolutions of the new Middle East*. New York: Public Affairs.

LYNCH, MARC (2016): *The new Arab wars: Uprisings and anarchy in the Middle East*. New York: Public Affairs.

MARCZAK, BILL; SCOTT-RAILTON, JOHN; MCKUNE, SARAH; ABDUL RAZZAK, BAHR; DEIBERT, RON (2018): Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries. In: *Citizen Lab*, 18 September 2018. https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

MARCZAK, BILL; SCOTT-RAILTON, JOHN (2016): The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender. In: *Citizen Lab*, 24 August 2016. https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

MARZOUK, HORRIYA (2020): Weaponized censorship: The final demise of free expression in Egypt's media. In: *The New Arab*, 2 July 2020. https://english.alaraby.co.uk/english/indepth/2020/7/2/the-final-demise-of-free-expression-in-egypts-media

MICHAELSON, RUTH (2020): Egyptian editor briefly detained in Covid-19 reporting crackdown. In: *The Guardian*, 17 May 2020. https://www.theguardian.com/world/2020/may/17/egyptian-editor-held-in-covid-19-reporting-crackdown

MIDDLE EAST EYE CORRESPONDENT (2020): Fear is overcoming me: Egypt cracks down harder on media amid pandemic. In: *Middle East Eye*, 21 June 2020. https://www.middleeasteye.net/news/fear-overcoming-me-egypt-steps-crackdown-media-amid-pandemic

MILLER, MAGGIE (2019): Twitter Removes 88k Accounts Tied to Saudi Arabia. In: *TheHill*, 20 December 2019. https://thehill.com/policy/cybersecurity/475488-twitter-takes-down-88k-accounts-tied-to-saudi-arabia

MORRIS, LOVEDAY (2018): Secret Recordings Give Insight Into Saudi Attempts to Silence Critics. In: *The Washington Post*, 17 October 2018.

MYERS, ELISABETH R. (2020): Egyptian journalist Mohamed Mounir murdered by Coronavirus. In: *Inside Arabia*, 25 August 2020. https://insidearabia.com/egyptian-journalist-mohamed-mounir-murdered-by-coronavirus/?fbclid=IwARobgj32CYLOiAuVQFpgNyJD7R_QVnpx9G_GKcxLqMrOp75WdKcqFws3bog

NAFIE, MUHAMMED (2020): UAE's coronavirus tracing app-Is it compulsory and other questions answered. In: *Al Arabiya English*, 20 April 2020. https://english.alarabiya.net/en/coronavirus/2020/04/20/UAE-s-coronavirus-tracing-app-Is-it-compulsory-and-other-questions-answered

NAKASHIMA, ELLEN; BENSINGER, GREG (2019): Former Twitter Employees Charged With Spying for Saudi Arabia by Digging Into the Accounts of the Kingdom's Critics. In: *The Washington Post*, 6 November 2019.

NEWS 1 (2019): Twitter closes thousands of pro-Saudi accounts in Egypt and UAE for spreading misleading news. In: *News 1*, 20 September 2019. https://www.news1.news/sa/2019/09/twitter-closes-thousands-of-pro-saudi-accounts-in-egypt-and-uae-for-spreading-misleading-news.html

NPR (2019): Twitter Removes Thousands of Accounts For Manipulating Its Platform. *NPR*, 20 September 2019. https://www.npr.org/2019/09/20/762799187/twitter-removes-thousands-of-accounts-for-manipulating-their-platform

PEW RESEARCH CENTER (2021): Social Media Fact Sheet. https://www.pewresearch.org/internet/fact-sheet/social-media/

ROMANOSKY, SASHA (2017): Private-Sector Attribution of Cyber Attacks: A Growing Concern for the U.S. Government?« In: *Law Fare*, 21 December 2017. https://www.lawfareblog.com/private-sector-attribution-cyber-attacks-growing-concern-us-government

RUWITCH, JOHN (2021): *NPR*, 31 March 2021. https://www.npr.org/2021/03/31/983156340/theory-that-covid-came-from-a-chinese-lab-takes-on-new-life-in-wake-of-who-report

SAKR, NAOMI (2013): *Transformations in Egyptian journalism*. New York: Palgrave Macmillan.

SANDERS IV, LEWIS (2020): Egypt expels British journalist over coronavirus coverage. In: *DW*, 27 March 2020. https://www.dw.com/en/egypt-expels-british-journalist-over-coronavirus-coverage/a-52942136

SEIB, PHILIP (2007): New media and prospects for democratization. In: SEIB, P. (ed.): *New media and the new Middle East.* New York, NY: Palgrave Macmillan, pp. 1-17.

SHANE, SCOTT; GOEL, VINDU (2017): Fake Russian Facebook Accounts Bought $100,000 in Political Ads. In: *The New York Time*s, 6 September 2017. https://www.nytimes.com/2017/09/06/technology/facebook-russian-political-ads.html

SHEZAF, HAGAR; JACOBSON, JONATHAN (2018): Revealed: Israel's Cyber-spy Industry Helps World Dictators Hunt Dissidents and Gays. In: *Haaretz*, 20 October 2018. https://www.haaretz.com/israel-news/.premium.MAGAZINE-israel-s-cyber-spy-industry-aids-dictators-hunt-dissidents-and-gays-1.6573027

SILVERSTEIN, RICHARD (2019): Israeli Tech's Dirty Ops. In: *Jacobin*, 6 June 2019, https://jacobinmag.com/2019/06/whatsapp-hacking-ngo-group-israel

SOUTH CHINA MORNING POST (2018): How Cambridge Analytica Exploited Facebook Users' Data, and Why it's a Big Deal. In: *South China Morning Post*, 28 March 2018.

SOUTH CHINA MORNING POST (2019): Twitter Spy Case Shines Spotlight on Rogue Staff. In: *South China Morning Post*, 9 November 2019.

STONE, JEFF (2019): Twitter Removes Nearly 6,000 Accounts Spreading Saudi Propaganda. In: *Cyberscoop*, 20 December 2019.

STUBBS, JACK (2019): Facebook Says it Dismantles Cover Influence Campaign Tied to Saudi Government. In: *Reuters*, 1 August 2019. https://www.reuters.com/article/us-facebook-saudi/facebook-says-it-dismantles-covert-influence-campaign-tied-to-saudi-government-idUSKCN1UR50J

SWAINE, JON (2018): Twitter admits far more Russian bots posted on election than it had disclosed. In: *The Guardian*, 19 January 2018. https://www.theguardian.com/technology/2018/jan/19/twitter-admits-far-more-russian-bots-posted-on-election-than-it-had-disclosed

THE GUARDIAN (2019): Popular Chat App ToTok is Actually a Spying Tool of UAE Government – Report. In: *The Guardia*n, 23 December 2019. https://www.

theguardian.com/world/2019/dec/23/totok-popular-chat-app-spying-tool-uae-government

THE TIMES OF ISRAEL (2018): Saudi Dissident Sues Israel Spyware Firm Over Khashoggi Killing. In: *The Times of Israe*l, 3 December 2018. https://www.timesofisrael.com/saudi-dissident-sues-israeli-spyware-firm-over-khashoggi-killing/

THE TIMES OF ISRAEL (2019): UAE Denies Developing Popular Middle East App as Spy Tool. In: *The Times of Israel*, 28 December 2019. https://www.timesofisrael.com/uae-denies-developing-popular-middle-east-app-as-spy-tool/

THIBAUT, OLIVIER: Before Trump, the long history of fake news. In: *Yahoo News*,12 July 2018. https://sg.news.yahoo.com/trump-long-history-fake-news-045226919.html

TIFFANY, KAITLYN (2019): A Timeline of High-Profile Tech Apologies. In: *Vox*, 26 July 2019.

ZILBER, NERI (2018): The Rise of the Cyber-Mercenaries. In: *Foreign Policy*, 31 August 2018. https://foreignpolicy.com/2018/08/31/the-rise-of-the-cyber-mercenaries-israel-nso/