GLOBAL TRENDS ANALYSIS

Ahmed Maati

COVID-19 and digital authoritarianism: Identifying risks and countermeasures

02 2022

IMPRINT

Published by
Stiftung Entwicklung und Frieden/
Development and Peace Foundation (sef:)
Dechenstr. 2, 53115 Bonn, Germany
Bonn 2022

ISSN: 2568-8804

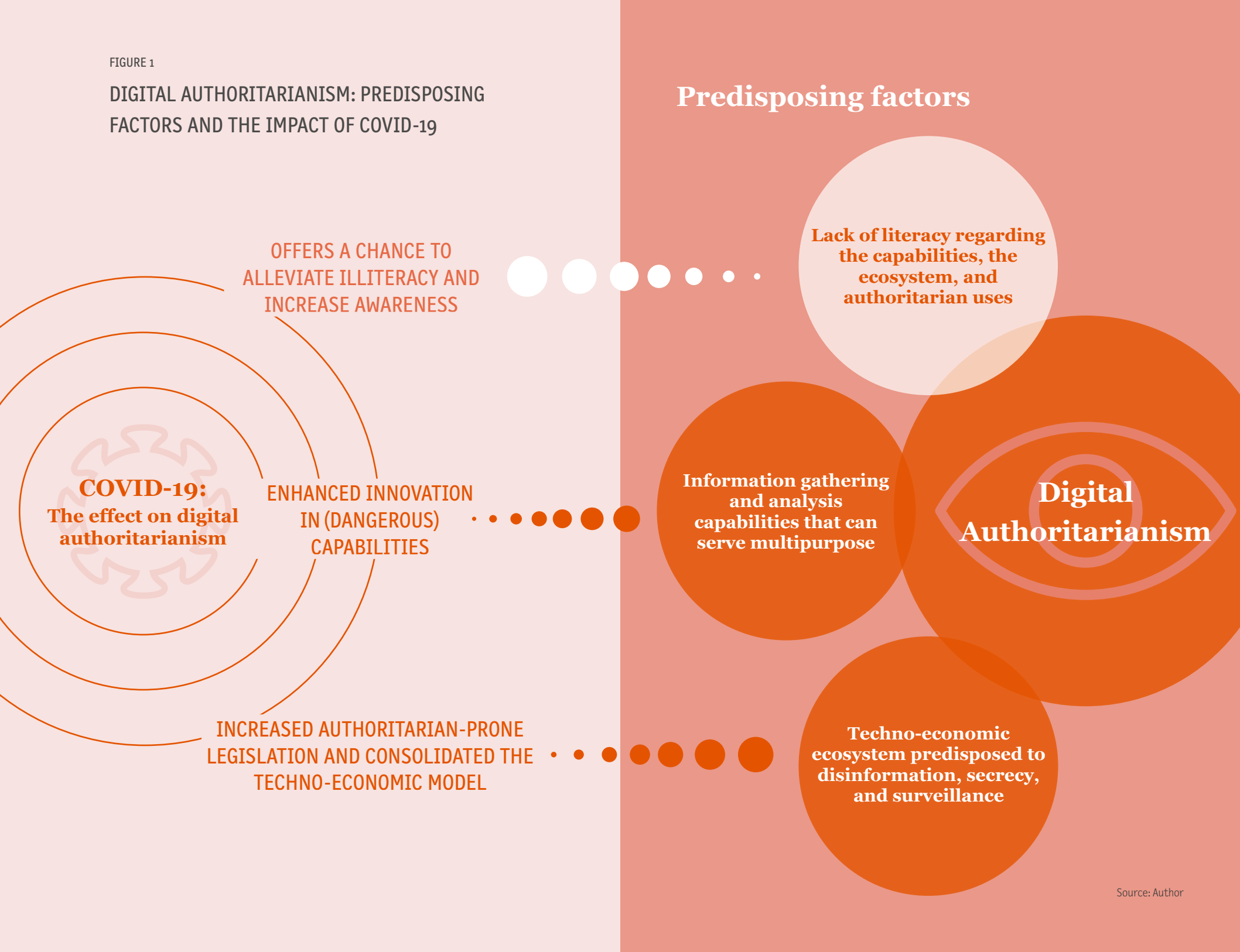
INTRODUCTION

There is no doubt that advances in digital technologies have positive effects on various aspects of life. At the same time, recent years have shown that these technologies can pose a global threat to privacy and freedom, and can equally foster repression and authoritarian tendencies, even in established democracies. Particularly in light of the COVID-19 pandemic, various scholars and rights groups have warned against the proliferating dangers of this 'digital authoritarianism'. I highlight three aspects of digital technologies that render them susceptible to authoritarianism: (i) the far-reaching capabilities of these technologies, especially in serving multiple purposes, (ii) their entrenchment in a reinforcing ecosystem, and (iii) the general lack of literacy regarding digital technologies' capabilities, ecosystem, and authoritarian usage.

While the pandemic presents dictators with a chance to consolidate and normalise authoritarian uses of digital technologies, it grants democracies an opportunity to raise awareness of digital technologies' dangerous capabilities and their authoritarian-friendly ecosystem. This can, in turn, sensitise citizens and policy-makers to take more adequate measures to counteract the authoritarian dangers of these technologies.

FIGURE 1

DIGITAL AUTHORITARIANISM: PREDISPOSING FACTORS AND THE IMPACT OF COVID-19



Source: Author

1. DIGITAL TECHNOLOGIES AND AUTHORITARIANISM

1.1 DIGITAL TECHNOLOGIES, AUTHORITARIANISM, AND AUTHORITARIAN PRACTICES

The term 'digital authoritarianism' is not unproblematic. Technically, political science considers authoritarianism to be a type of political regime – a set of rules that govern access to political power and determine the relationship of those who are in power with those who are not (Fishman 1990, p. 428). The exact definition of authoritarianism is not a subject of consensus, and the field is divided between many who consider authoritarianism the absence of democracy, and some who try to formulate a more direct definition. There is, however, more consensus on many general features of how power and politics look in authoritarian regimes. For the purpose of identifying risks and countermeasures, I focus on the general features that characterise authoritarianism, examine how digital technologies relate to these features, and then evaluate COVID-19's impact on these aspects.

Authoritarianism entails a malevolent configuration of rules – the most obvious of which is that access to power is not regulated via free and fair elections. But it goes beyond that, for free and fair elections, albeit important, are not the only constituent element of democratic regimes. Autocrats, driven by the desire to maintain political power, need to know, influence, and control the beliefs and behaviour of their subjects (Schlumberger et al. 2022). This automatically predisposes authoritarianism to large-scale violations of civil and political rights, including widespread repression, lack of accountability, and surveillance excesses.

While many of these authoritarian tendencies also characterise some actors in democracies, one important difference is that, in democracies, these ills do not constitute the logic of political rule. It is, therefore, useful to think about these tendencies in democracies as "authoritarian practices" that "sabotage accountability to people over whom a political actor exerts control, or their representatives, by means of secrecy, disinformation and disabling voice" (Glasius 2018, p. 515). Below, I discuss three characteristics of digital technologies that predispose them to enabling authoritarian practices or authoritarianism. Digital authoritarianism is, thus, the enablement of the ills discussed above as a result of digitisation or the use of digital technologies.

1.2 THREE CHARACTERISTICS THAT PREDISPOSE DIGITAL TECHNOLOGIES TO AUTHORITARIANISM

(i) Digital technologies' marvellous capabilities to gather, analyse, and predict data render them very attractive to authoritarian regimes and authoritarian actors in democracies alike. They offer (would-be) dictators the ability to obtain unprecedented information about citizens, as well as to repress and control them. Many technologies allow this to occur covertly and in secret, escaping oversight and accountability. This applies all the more since most technologies can serve multiple purposes; some can even simultaneously offer dictators the ability to surveil, repress, and control. Some widely used and commercially available capabilities already exist; others are still in the development and research stages.

In recent years, digital technologies have proved effective in gathering vast quantities of information on individuals and psychometrically using this data to influence individuals' behaviour and beliefs. By utilising users' interaction with an application that runs on Facebook, Cambridge Analytica created a large dataset on "tens of millions of users", which it used to influence their voting behaviour (Confessore 2018). Some malicious computer programs can covertly turn smartphones into live surveillance devices, hardly leaving a trace. Pegasus is a widely known example of that: in 2019, Facebook revealed that a vulnerability in the WhatsApp application had exposed 1400 phones to Pegasus (Simpson 2019). Dubbed the "impossible spyware", Pegasus operates in at least 45 countries and is almost impossible to detect (Marczak et al. 2018). If detected, it destroys the infected device after having removed any trace of itself (Lookout Security 2017). The software was also used to surveil various activists around the world (Priest et al. 2021). Artificial Intelligence (AI) has particularly revolutionised these capabilities. Algorithms can be trained not only to identify individuals in real-time but also to predict their behaviour (and sometimes to outperform it). In 2017, a Google AI was even able to predict the behaviour of a Go champion and defeat him in the complex game (BBC 2021).

More concerning capabilities exist, but the extent of their usage remains unclear. Several studies have documented the successful usage of WIFI waves in normal routers to identify the number of individuals in a room (Alam Nipu et al. 2018; Cushman et al. 2016). What is more, some were also able to identify the individuals based on their style of walking, which creates unique

identifiable disturbances in the wave signals with an accuracy of 94.5% in a room of two people and 88.9% in a room of six (Xin et al. 2016). Other research utilised radio waves to identify individuals' movements and handwriting from behind thick walls, without the need to use any extra devices inside the surveilled room (Ding et al. 2021; Guo et al. 2020). Utilising a similar technology, other researchers were able to 'hear' individuals from behind walls by analysing wave disturbances caused by lip movements (Wang et al. 2016); others identified keystrokes on keyboards with a real-life accuracy of more than 93% (Ali et al. 2015). More invasive technologies gather and analyse data by direct brain-computer interfaces. In 2017, the Defense Advanced Research Projects Agency (DARPA) granted various research funds to develop brain implants that simultaneously record the signals of one million human neurons (DARPA 2017; Miranda et al. 2015; Murphy 2017). Reliable assessments of the widespread use of these capabilities are absent; however, their sheer existence speaks to the unprecedented propensity to gather and analyse data to influence and predict individuals' behaviours and beliefs.

These capabilities can serve multiple purposes, which facilitates secrecy and lack of accountability in their illegitimate uses. They are multipurpose in a double sense: surveillance technologies, for instance, could both aid law enforcement and violate privacy rights. On another level, the algorithm underlying medical diagnostic software could be repurposed for facial recognition. In the above examples, the technologies that utilise digital implants to gather, analyse, or influence neuronal signals to achieve better prosthetic control for amputees could also be employed to surveil and control individuals' behaviours and decisions.

Government agencies can, therefore, acquire or develop digital capabilities for seemingly legitimate purposes while concealing (the potential for) malevolent uses. This is famously the case with the use of digital surveillance capabilities such as Pegasus. Both the developer – the NSO group – and governments officially claim that the software is deployed solely for law enforcement purposes (Priest/Dwoskin 2021). In practice, however, it has been used by both democracies and autocracies to surveil and repress activists and critics (Kenyon 2019). This also thwarts accountability for digital authoritarianism; not only because of secrecy, but also because responsibility is diffused between firms and governments who claim to employ technologies for legitimate purposes, and developers who might have developed the underlying technology for medical or other legitimate purposes.

The above problematics of technologies' extensive, multipurpose, and authoritarian-pronecapabilities are potentiated by (ii) an ecosystem that is geared toward privacy violation and lack of transparency and oversight. This equally authoritarian-prone ecosystem consists of techno-economic and legal levels. On the techno-economic level, profit depends on gathering large amounts of user data. This does not only apply to surveillance capitalism (Zuboff et al. 2019); the profit both digital services and the technologies underlying them generate depends on gathering and analysing large amounts of user data (Saglam 2022). Like their analog counterparts, digital services from social media to music applications profit from advertising revenues. They gather and analyse data to learn about individual preferences and consumption – for instance, music preferences to increase the time users spend on their platforms by suggesting music similar to users' preference, and attract new users, increasing their ad revenues. They can also sell data to third parties to similarly exploit it for profit. While analyses of market trends have always existed, algorithmic capacities enhance and automate them to an unprecedented extent. Algorithms themselves need to be trained on large amounts of data; the more data they generate and analyse, the better they can target users, and the more they generate profit.

This techno-economic ecosystem not only enables unprecedented surveillance and control, but also facilitates disinformation. The economic incentive to generate, gather, and analyse data, coupled with a lack of transparency regarding the (algorithmic) strategies followed to this end are, as the case of Cambridge Analytica illustrates, perfect ingredients for privacy violations and manipulation. Digitised data gathered from different sources and on different devices can also be cross-read and analysed; this triangulation of information paints an ever-accurate picture of individuals' beliefs and behaviour. Besides that, driven by the desire to maximise usage and increase user data, some social media algorithms intentionally disseminate misinformation as it has proved useful in maximising the time users spend on their platforms (Van Cleave 2021).

On the legal level, digital technologies operate in a largely under-regulated ecosystem in which many governments can legally violate citizens' privacy. This concerns both the regulation of technologies and services such as AI and social media, but also regulation against government abuses. In 2021, more than a quarter of the 169 countries examined in the Digital Society Project had legal frameworks that allowed the government to access at least "many"

FIGURE 2
Legal frameworks regulating government access to online data
Content of privacy protection by law, 2021, 169 countries
(N = 179; no data for 10 cases)

Source: Author's compilation based on Digital Society Project 2022 (http://digitalsocietyproject.org/data/).

types of personal data on the internet (Digital Society Project 2022) [see Figure 2]. A study of 38 national AI strategies reports that: "While almost all strategies highlighted the need to ensure potential harms were mitigated against … strategies largely failed to set out any specific details of *how* this should be done in practice" (Bradley et al. 2021, p. 27). Also, attempts to bring tech giants under state regulation do not usually result in greater protection for users (Shahbaz/Funk 2019, p. 11).

These are just a few examples of the legal and economic infrastructures in which digital capabilities are embedded. The capabilities of digital technologies predispose them to authoritarianism as they enable covert knowledge, manipulation, and control of individuals. The ecosystem provides the legal and economic frameworks to do so.

Finally, (iii) a general lack of awareness regarding these characteristics that predispose digital technologies to authoritarianism prevents citizens and policy-makers from taking timely countermeasures. Most authoritarian uses of digital technologies become visible to the public after having already inflicted damage. For instance, surveillance programs of the US National Security Agency (NSA) came to public attention only because of Edward Snowden's testimonies years after their initial deployment. The fiasco surrounding Cambridge Analytica occurred after it influenced two pivotal elections in the USA and Great Britain. The NSO-developed Pegasus spyware came under public scrutiny after having contributed to the repression of activists and journalists.

2. COVID-19, DIGITAL TECHNOLOGIES, AND AUTHORITARIANISM

The pandemic has, overall, potentiated aspects that predispose digital technologies to authoritarianism. It has driven the development and deployment of dangerous digital surveillance and control capabilities and facilitated investments in digital capabilities. In parallel, it provided a justification for governments to legally violate citizens' privacy, increased the amount of digitised data, and facilitated digital disinformation. As the pandemic's 'digital shadow' continues (Shahbaz/Funk 2020), we may even be on the verge of a dangerous normalisation of digital authoritarianism (Maati/Švedkauskas 2021). COVID-19's negative effects concern both democracies and dictatorships. However, as the next section shows, it also presents democracies with a unique opportunity to raise public awareness of authoritarian practices that are enabled by digital technologies and to highlight the characteristics that incline these technologies to authoritarianism.

COVID-19 has triggered many advancements in technological capabilities that serve authoritarian regimes and practices. The pandemic has been an emergency; a crisis that justified the development and use of digital surveillance and repression technologies in both democratic and authoritarian regimes (Maati/Švedkauskas 2020). Between April 2020 and 2022, 20 countries either developed or acquired AI surveillance technologies (Feldstein 2021, p. 227; 2022). 2020 witnessed the greatest one-year increase in the number of countries able to shut down at least three quarters of domestic internet access since 2011 [see Figure 3a]. The Freedom on the Net data also shows a greater global deterioration in internet freedom during the years of the pandemic, compared to previous years [see Figure 3b]. In 2021, 34 countries scored worse than in 2019, whereas only 17 scored worse between 2016 and 2018 (Freedom House 2021).

Almost all countries have utilised digital technologies for contact tracing purposes, many gathering biometric data about individuals (Shahbaz/Funk 2020, p. 14). There is no doubt that the dangers to privacy these applica-

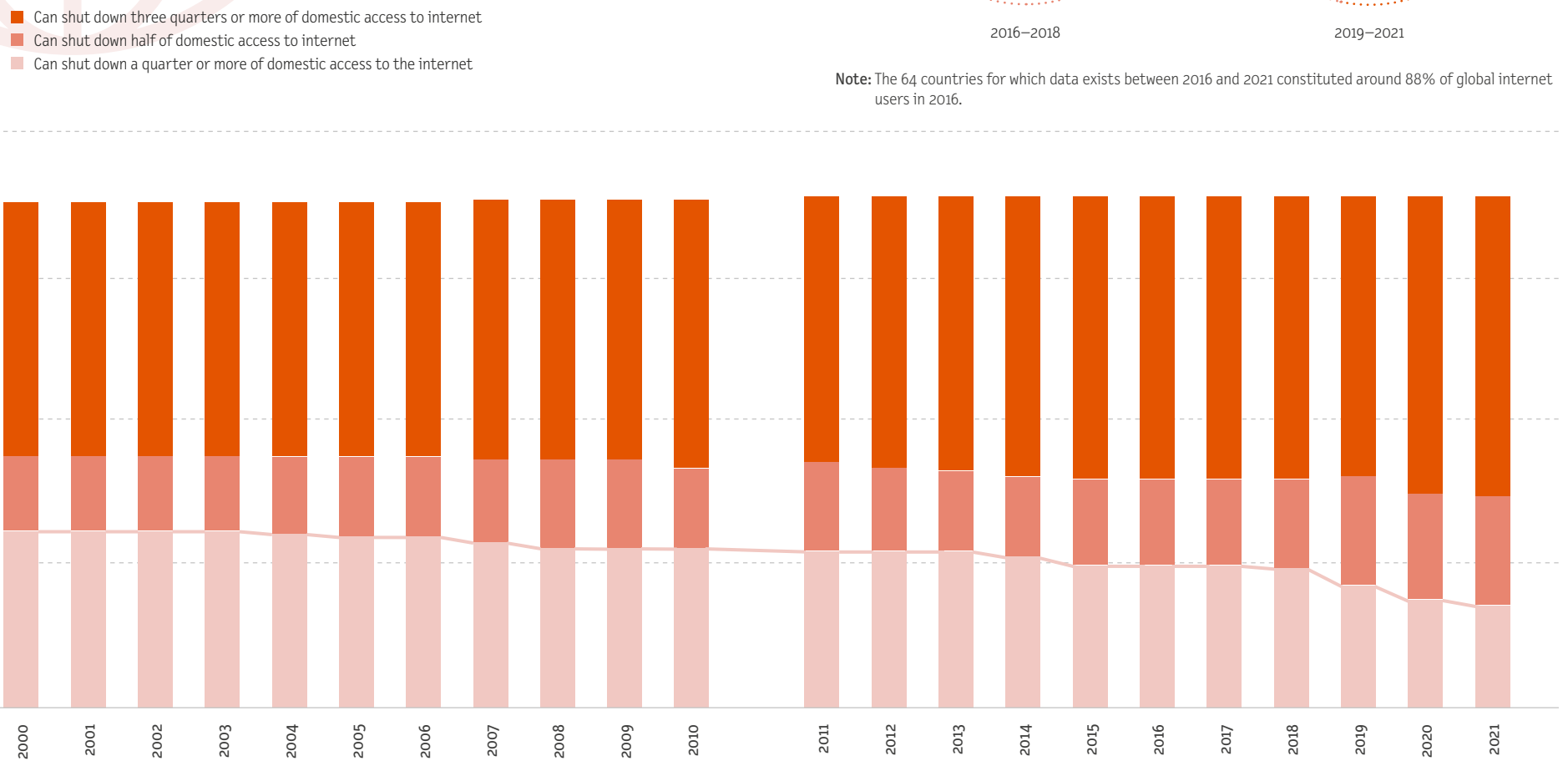
FIGURE 3

THE COVID-19 PANDEMIC POTENTIATED DANGEROUS CAPABILITIES

FIGURE 3a

Increase in government capacity to shut down the internet

Government internet shutdown capacity, 2000–2021, 179 countries

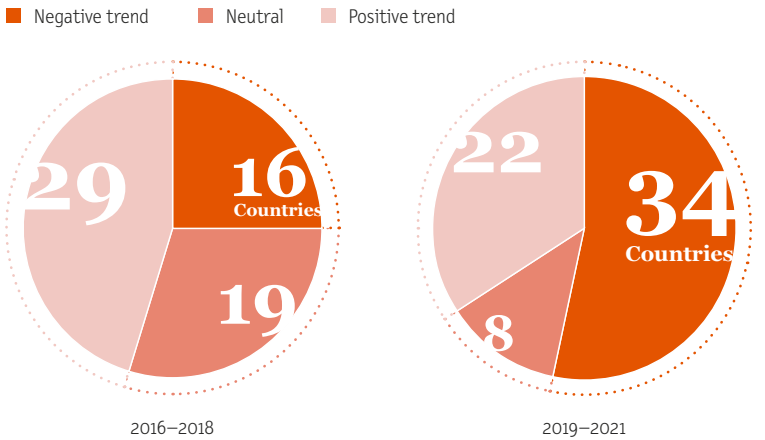


Source: Author's compilation based on Digital Society Project 2022 (http://digitalsocietyproject.org/data/).

FIGURE 3b

Online freedoms have suffered a pivotal deterioration during the pandemic

Number of countries before (2016–2018) and during (2019–2021) the pandemic, 64 countries



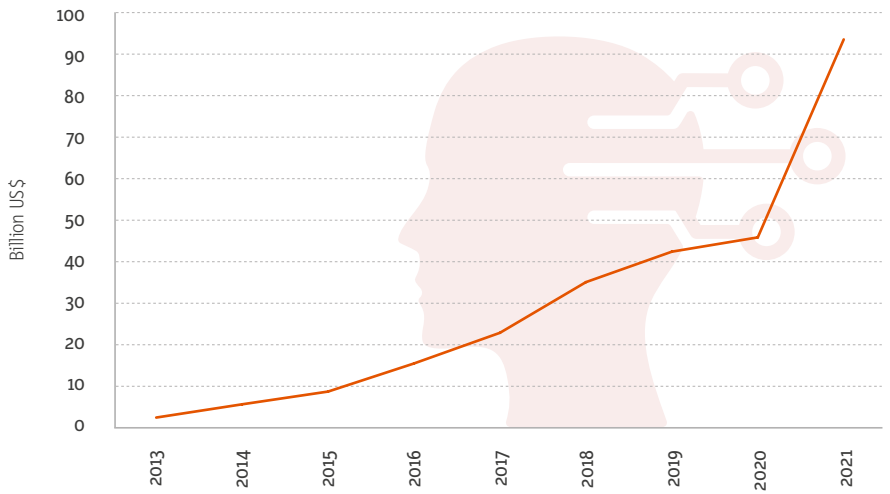
Note: The 64 countries for which data exists between 2016 and 2021 constituted around 88% of global internet users in 2016.

Source: Author's compilation based on Freedom House 2021.

tions pose are greater in authoritarian contexts, yet democracies have been far from immune to these dangers. In 2020, Amnesty International (2020) listed Norway's contact tracing application amongst the most "alarming mass surveillance tools". In India, smart cities were dedicated to live-tracking individuals to enforce quarantine orders. Under emergency regulations, Israel triangulated GPS, credit card, and cellular data to enforce quarantine and trace contacts (Halbfinger et al. 2020). Even Germany's often hailed contact tracing application operates on platforms provided by Apple and Google, raising concerns about big tech's access to user data (Norton Rose Fulbright 2021).

COVID-19 turned digital connectivity from a "convenience [to] a necessity" (Shahbaz/Funk 2020, p. 1), forcing many individuals, schools, financial institutions, and businesses to rely on digital technologies (Rodriguez Contreras 2021; Sorgner 2021). The pandemic has also accelerated digitisation

FIGURE 4
The pandemic increased investment in the development and enhancement of technological capabilities
Total investment by leading countries in AI 2013–2021



Note: The Stanford AI index investigates 29 countries that are leading the world in the fields of AI development. They include China, Germany, India, Japan, Malaysia, Russia, Singapore, South Korea, Spain, and the USA.

Source: Stanford AI Index 2022a

in the supply chain sector by three to four years (Rodriguez Contreras 2021), and some research shows that 90% of supply-chain professionals plan to invest in digitisation (Agrawal et al. 2020, p. 3). The importance of AI technologies for contact tracing, data sharing, and the development of a vaccine (Rasheed et al. 2021) doubled investments in AI research and development (Stanford AI Index 2022b) [see Figure 4].

Some of the above developments do not seem problematic, yet they carry inherent risks as the pandemic consolidates digital technologies' authoritarian-friendly ecosystem. The combination of soaring investments in the development of AI, the increasing reliance on digital services that will likely outlive the pandemic (OECD 2020a, p. 2), and the production of large volumes of digitised data increase digital technologies' susceptibility to authoritarianism and to practices of surveillance, manipulation, and disinformation. The increasing reliance on digital technologies resulted in the collection and analysis of "people's most intimate data" (OECD 2020a). It enhances algorithms and makes them better able to target and manipulate individuals. The full effects of this will likely be seen in the future as soaring investments in digital technologies, particularly AI, will surely enhance their capacity to collect and analyse data. Moreover, in the context of a public health emergency, increased online activity served as an opportunity for social media algorithms to disseminate controversial information to increase usage, leading to widespread misinformation and a dangerous "infodemic" (WHO 2022).

Moreover, COVID-19 has consolidated the unaccountable and abuse-prone legal ecosystem in which digital technologies operate. It has provided governments around the world with an opportunity to increase their legal rights to surveil and control citizens, often with the help of data collected by big tech (Anisin 2022, p. 263). The Freedom on the Net report, which examines the status of digital freedoms in 65 countries that constitute 87% of the world's internet users (Shahbaz/Funk 2020, p. 5), reported in 2020 that 30 countries have legally enhanced data-sharing with private companies (p. 19). It also documents at least 20 countries that introduced new laws or directives restricting online expression during the COVID pandemic (Shahbaz/Funk 2020, p. 10).

2.1 A HEYDAY FOR AUTHORITARIANISM AND A GLIMPSE OF HOPE IN DEMOCRACIES?

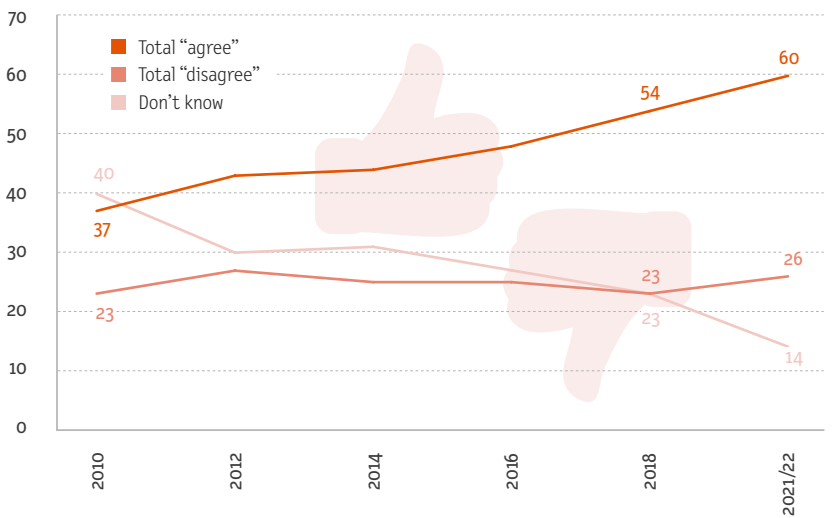
Against this background, the pandemic years have witnessed the worst setback in internet freedoms and potentiated authoritarian uses of digital technologies in both democracies and dictatorships. Nevertheless, it has presented dictatorships and democracies with different opportunities, even though it evoked some similar responses in both. It has helped dictatorships pursue the desire of surveillance and control. In democracies, while it has surely potentiated authoritarian practices, it also presents an opportunity to counter digital authoritarianism. For instance, the increasing salience of digital technologies and subsequent concerns about data privacy led both types of regimes to take measures to bring data (usage) and big tech companies under state regulation (Shahbaz/Funk 2021). While this is a chance for democracies to bring big tech companies under 'democratic' regulation, it is an opportunity for autocrats to increase their authoritarian control of data and pressure companies to serve their interests. One example is that while Germany passed a law in 2021 that mandates the government to investigate companies' behaviour that would hinder competition or prevent users from having control over their data, Russia targeted Google with its anti-monopoly law to pressure YouTube to remove regime-critical content (Shahbaz/Funk 2021, p. 20f.). The pandemic has also triggered the deployment of digital surveillance in both democracies and dictatorships. But evidence shows that while this can lead to swift normalisation of digital surveillance in dictatorships, it can raise public awareness and concern in democracies. A recent survey shows that more than 60% strongly accept the use of contact tracing applications in China, compared to less than 20% in the USA and Germany (Kostka/Habich-Sobiegalla 2020).

More importantly, some sporadic evidence invites cautious optimism that the pandemic, despite its negative effects, presents democracies with an opportunity to counter digital authoritarianism. COVID-19 could increase awareness not only of the authoritarian potential of digital capabilities, but also of the ecosystem in which they operate. It has sparked policy and academic discussions about digital surveillance, control, secrecy, and disinformation in broader societal segments. In some democracies, citizens were concerned not only about digital surveillance capabilities, but also about the lack of data and algorithmic transparency. In Ireland, the most cited reason not to use digital surveillance apps is the "fear that technology companies or the government might use the App technology for greater surveillance after the pandemic" (O'Callaghan et al. 2021, p. 863). In the United Kingdom, in-depth qualitative interviews with different segments of society show that many were worried "that their data would be accessible to others outside of government and health authorities, including 'third parties' or 'hackers'" (Williams et al. 2021, p. 380). Additionally, the pandemic has crystallised the dangers of digital capabilities to disseminate deadly disinformation and the willingness of social media platforms to allow it. For example, people were least inclined to trust the information on messaging applications and social media in French-speaking Switzerland (Liu et al. 2020, p. 153). In the EU, the

FIGURE 5
The pandemic increased public awareness of technological dangers
Standard Eurobarometer 96, Public opinion in the European Union, Winter 2021–2022

Question posed: Regardless of whether you participate in online social networks or not (social networking websites, blogs, video hosting websites), please state whether you totally agree, tend to agree, tend to disagree or totally disagree with each of the following statements:

Information on political affairs from online social networks cannot be trusted (%)



Source: European Commission 2022, p. 66.

percentage of citizens who agree that information on social media cannot be trusted continued to increase during the pandemic years (European Commission 2022, p. 65) [see Figure 5]. Similar concerns have haunted policy-makers and academics. Since the beginning of the pandemic, the Council of Europe (2020), WHO (2020), and OECD have all published various documents and guidelines to protect users' privacy while using digital technologies to fight the global pandemic (OECD 2020b). Scholarly articles from diverse fields of study have also debated the dangers of digital authoritarianism in light of the pandemic and how to respond to them.

3. SO WHAT SHOULD WE DO?

The increased salience of digital dangers during the pandemic is an opportunity for actors in democracies to reduce and counter these dangers of digital technologies. The previous sections highlighted various elements that render digital technologies susceptible to authoritarian practices in a manner accessible to a non-technical audience. The three characteristics identified above help translate COVID's effects on digital authoritarianism into categories relatable to the public and policy-makers. This may enable different actors in democracies to go beyond immediate concerns of surveillance and privacy and engage with the characteristics that make digital technologies susceptible to authoritarian use. The remaining paragraphs discuss the responsibilities of policy-makers, civil society, academics, and citizens and offer recommendations for further action, which are presented in more detail in Table 1.

Civil society actors in democracies and academics should, therefore, seize the chance to increase awareness of digital capabilities, their authoritarian uses, and the underlying characteristics that predispose them to authoritarianism (the ecosystem). COVID-19 is an opportunity to highlight these issues to the public and to policy-makers in democracies. The dangers of digital technologies might have seemed distant to the average user or policy-maker in the pre-COVID era. But now, the dangers of digital technologies do not only come from Russia or China; rather, it is increasingly obvious that at least some dangers are inherent in how these technologies operate and their extensive capabilities.

Academics have done a tremendous job researching technological dangers in light of COVID-19; they should also seize the opportunity to communicate these dangers to the public in an accessible manner. We tend to immerse ourselves in technical details and indulge in scientific jargon. While to some extent, this is necessary for scientific progress, scholars need to better orient their work to the non-scientific audience without jeopardising methodological or analytical rigour. Privacy and freedom concerns in light of COVID-19 offer a universal common ground to do so. Academics should, therefore, address the public more, while working on their communication skills for a non-academic audience.

Policy-makers in some democracies have taken steps to bring data under state control (see section 3.2). It is, however, paramount that such a push towards data sovereignty is accompanied by strict 'democratic' control against state abuses of data. The increased public salience of digital technologies' dangers during COVID offers policy-makers a window of opportunity to pressure Big Tech to be more transparent on how their algorithms gather and process data. Finally, democratic policy-makers should start discussions on how to regulate not only the uses of AI technologies, but also how these technologies are researched and the kind of data they are trained on.

Citizens are the engine of democracies and can do at least two things: The first is to collectively pressure policy-makers towards better regulation of digital technologies. This should not be confined to regulating end products or deployment but should extend to further regulating the underlying techno-economic infrastructure. In particular, citizens should fight against all legislation that grants governments more access to personal data. They should also demand full transparency for the collection and use of their data both by the government and by big tech companies; this includes transparency regarding how the algorithms that automate the data collection and analysis process operate. This has proven effective in some democracies like Germany during the pandemic as public pressure motivated the government to rely on an open-source contact tracing application. Finally, citizens should engage policy-makers in discussions to protect the data collected during public health crises from being combined and integrated with other pre-existing digital data.

The second is to adjust (online) behaviour to attenuate these dangers. Specifically, where applicable, citizens should commit to reading and navigating privacy 'cookie' notifications on websites to control the collection and handling of their data. A wide array of free software is also available to

TABLE 1

COVID-19 RAISED THE SALIENCE OF THE ELEMENTS THAT MAKE DIGITAL TECHNOLOGIES PRONE TO AUTHORITARIANISM

How can democracies seize the chance?

Civil Society

TURN SALIENCE INTO LITERACY BY

Educating citizens and policy-makers about the underlying characteristics (ecosystem) that facilitate digital authoritarianism

Starting with specific examples that became salient during COVID-19 pandemic (contact tracing applications, biometric data-gathering, etc.)

Gradually including less salient issues (social media or online shopping algorithms, etc.)

Helping citizens with software and hardware choices to secure their data

Adhering to balanced and objective accounts: Highlight the dangers without demonising technology or overlooking advantages.
The goal is to capitalise on the advantages and minimise the risks

Policy-makers

REGULATIONS TO

Bring data under democratic state control (data sovereignty)

Push Big Tech toward more transparency about how algorithms gather and process data

Insert safeguards at the research and development (not only deployment) levels of digital technologies and AI

Citizens

COLLECTIVE PRESSURE ON LOCAL REPRESENTATIVES AND POLICY-MAKERS TO

Strictly limit access to user data

Demand full transparency on how companies gather and process data – including transparency on how algorithms work

Regulate digital technologies throughout their lifecycle: Research, development, and deployment

ADJUST INDIVIDUAL BEHAVIOUR TO MINIMISE RISKS

Carefully read privacy policies and cookie notifications. Only accept conditions/cookies you find reasonable

Check companies' track record of data protection before using their services or buying their digital products

Regularly flush cookies and tracking files

Use security and anti-tracking software on all digital devices

Academics

ADDRESS PUBLIC MORE AND USE ACCESSIBLE NON-TECHNICAL LANGUAGE TO

Spread knowledge about the characteristics and dangers of digital authoritarianism as well as its relevance to everyday life in democracies

Aid civil society in raising balanced awareness of the advantages and dangers of digital technologies

Help governments and policy-makers identify threats and counter dangers

Aid citizens to adjust (online) behaviour to minimise risks

clear online tracking data from digital devices. We should also 'cautiously' rely on trusted sources that evaluate companies' commitment to protecting user information (e.g. https://rankingdigitalrights.org) when using services or buying devices. Finally, security, encryption, and anti-tracking software should be installed and used on all digital devices (https://netalert.me offers easy explanations of different threats and tools to counter them).

While COVID-19 potentiated digital authoritarianism globally, it is up to democracies to create opportunities in times of crisis. Raising awareness is a necessary first step to counter digital authoritarianism.

REFERENCES

AGRAWAL, MAYANK/ELOOT, KAREL/MANCINI, MATTEO/PATEL, ALPESH 2020: Industry 4.0: Reimagining Manufacturing Operations after COVID-19 (McKinsey & Company), n.p. (https://www.mckinsey.com/business-functions/operations/our-insights/industry-40-reimagining-manufacturing-operations-after-covid-19, 26.10.2022).

ALAM NIPU, NAIFUL/TALKUDER, SOUVIK/SOUVIK TALUKDER/ISLAM, SAIFUL/CHAKRABARTY, AMITABHA 2018: Human Identification Using WIFI Signal, in: Joint 7th International Conference on Informatics, Electronics & Vision (ICIEV) and 2nd International Conference on Imaging, Vision & Pattern Recognition (IcIVPR), pp. 300-304.

ALI, KAMRAN/LIU, ALEX X./WANG, WEI/SHAHZAD, MUHAMMAD 2015: Keystroke Recognition Using WiFi Signals, in: Proceedings of the 21st Annual International Conference on Mobile Computing and Networking, MobiCom '15, New York: Association for Computing Machinery, pp. 90-102.

AMNESTY INTERNATIONAL 2020: Bahrain, Kuwait and Norway Contact Tracing Apps a Danger for Privacy, n.p. (https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/, 24.08.2022).

ANISIN, ALEXEI 2022: Pandemic Surveillance Capitalism: Authoritarian Liberalism or Democratic Backsliding?, in: Journal of Political Power, Vol. 15/2, pp. 262-278.

BBC 2021: Google AI Defeats Human Go Champion, London (https://www.bbc.com/news/technology-40042581, 01.09.2022).

BRADLEY, CHARLES/WINGFIELD, RICHARD/METZGER, MEGAN 2021: National Artificial Intelligence Strategies and Human Rights: A Review (Global Partners Digital), n.p. (https://www.gp-digital.org/wp-content/uploads/2021/05/NAS-and-human-rights_2nd_ed.pdf, 12.10.2022).

CONFESSORE, NICHOLAS 2018: Cambridge Analytica and Facebook: The Scandal and the Fallout So Far (The New York Times), New York City (https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html, 01.09.2022).

COUNCIL OF EUROPE 2020: Contact Tracing Apps, Strasbourg (https://www.coe.int/en/web/data-protection/contact-tracing-apps, 30.08.2022).

CUSHMAN, ISAAC/RAWAT, DANDA B./BHIMRAJ, ABHISHEK/FRASER, MALIK 2016: Experimental Approach for Seeing through Walls Using Wi-Fi Enabled Software Defined Radio Technology, in: Digital Communications and Networks, Vol. 2/4, pp. 245-255.

DARPA (Defense Advanced Research Projects Agency) 2017: Towards a High-Resolution, Implantable Neural Interface, Arlington (https://www.darpa.mil/news-events/2017-07-10, 03.08.2022).

DIGITAL SOCIETY PROJECT 2022: DSM Data V4, n.p. (http://digitalsocietyproject.org/data/, 12.10.2022).

DING, DIAN/YANG, LANQING/CHEN, YI-CHAO/XUE, GUANGTAO 2021: VibWriter: Handwriting Recognition System Based on Vibration Signal, in: 18th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), pp. 1-9.

EUROPEAN COMMISSION 2022: Media Use in the European Union, Brussels (Standard Eurobarometer 96, Winter 2021-2022) (https://data.europa.eu/doi/10.2775/911712 0811.2022).

FELDSTEIN, STEVEN 2021: The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance, Oxford: Oxford University Press.

FISHMAN, ROBERT M. 1990: Rethinking State and Regime: Southern Europe's Transition to Democracy, in: World Politics, Vol. 42/3, pp. 422-440.

FREEDOM HOUSE 2021: All Score Data, 2011-2021 (Freedom House), n.p. (https://freedomhouse.org/report/freedom-net, 12.10.2022).

GLASIUS, MARLIES 2018: What Authoritarianism Is... and Is Not: A Practice Perspective, in: International Affairs, Vol. 94/3, pp. 515-533.

GUO, ZHENGXIN/XIAO, FU/SHENG, BIYUN/FEI, HUAN/YU, SHU 2020: WiReader: Adaptive Air Handwriting Recognition Based on Commercial WiFi Signal, in: IEEE Internet of Things Journal, Vol. 7/10, pp. 10483-10494.

HALBFINGER, DAVID M./KERSHNER, ISABEL/BERGMAN, RONEN 2020: To Track Coronavirus, Israel Moves to Tap Secret Trove of Cellphone Data (The New York Times), New York City (https://www.nytimes.com/2020/03/16/world/middleeast/israel-coronavirus-cellphone-tracking.html, 12.10.2022).

KENYON, MILES 2019: Dubious Denials & Scripted Spin: Spyware Company NSO Group Goes on 60 Minutes (The Citizen Lab), Toronto (https://citizenlab.ca/2019/04/dubious-denials-scripted-spin-spyware-company-nso-group-goes-on-60-minutes, 11.10.2022).

KOSTKA, GENIA/HABICH-SOBIEGALLA, SABRINA 2020: In Times of Crisis: Public Perceptions Towards COVID-19 Contact Tracing Apps in China, Germany and the US, Berlin (https://papers.ssrn.com/abstract=3693783, 26.08.2022).

LIU, ZHAN/SHAN, JIALU/DELALOYE, MATTHIEU/PIGUET, JEAN-GABRIEL/GLASSEY BALET, NICOLE 2020: The Role of Public Trust and Media in Managing the Dissemination of COVID-19-Related News in Switzerland, in: Journalism and Media, Vol. 1/1, pp. 145-158.

LOOKOUT SECURITY 2017: Pegasus for Android: Technical Analysis and Findings of Chrysaor (Security report), n.p. (https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-android-technical-analysis.pdf, 11.10.2022).

MAATI, AHMED/ŠVEDKAUSKAS, ŽILVINAS 2020: Framing the Pandemic and the Rise of the Digital Surveillance State, in: Mezinárodní vztahy, Vol. 55/4, pp. 48-71.

MAATI, AHMED/ŠVEDKAUSKAS, ŽILVINAS 2021: Long-Term Prescription? Digital Surveillance Is Here to Stay, in: Mezinárodní vztahy, Vol. 56/4, pp. 105-118.

MARCZAK, BILL/SCOTT-RAILTON, JOHN/MCKUNE, SARAH/RAZZAK, BAHR A./DEIBERT, RON 2018: HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries (The Citizen Lab), Toronto (https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/, 01.07.2019).

MIRANDA, ROBBIN A. ET AL. 2015: DARPA-Funded Efforts in the Development of Novel Brain-Computer Interface Technologies, in: Journal of Neuroscience Methods, Vol. 244, pp. 52-67.

MURPHY, MARGI 2017: The Government Wants to Put 'Telepathy' Chips in Our Brains (New York Post), New York City (https://nypost.com/2017/07/12/the-government-wants-to-put-telepathy-chips-in-our-brains, 03.08.2022).

NORTON ROSE FULBRIGHT 2021: Contact Tracing Apps: A New World for Data Privacy, n.p. (https://www.nortonrosefulbright.com/en-de/knowledge/publications/d7a9a296/contact-tracing-apps-a-new-world-for-data-privacy, 24.08.2022).

O'CALLAGHAN, MICHAEL E. ET AL. 2021: A National Survey of Attitudes to COVID-19 Digital Contact Tracing in the Republic of Ireland, in: Irish Journal of Medical Science, Vol. 190/3, pp. 863-887.

OECD (Organisation for Economic Co-operation and Development) 2020a: Digital Transformation in the Age of COVID-19: Building Resilience and Bridging Divides. (Digital Economy Outlook 2020 Supplement), Paris (https://www.oecd.org/digital/digital-economy-outlook-covid.pdf, 12.10.2022).

OECD (Organisation for Economic Co-operation and Development) 2020b: Tracking and Tracing COVID: Protecting Privacy and Data While Using Apps and Biometrics, Paris (https://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protect-ing-privacy-and-data-while-using-apps-and-biometrics-8f394636/, 30.08.2022).

PRIEST, DANA/DWOSKIN, ELIZABETH 2021: Chief of WhatsApp, Which Sued NSO over Alleged Hacking of Its Product, Disputes Firm's Denials on Scope of, Involvement in Spyware Operations (The Washington Post), Washington, DC (https://www.washingtonpost.com/investigations/2021/07/24/whatsapp-pegasus-spyware/, 01.09.2022).

PRIEST, DANA/TIMBERG, CRAIG/MEKHENNET, SOUAD 2021: Private Israeli Spyware Used to Hack Cellphones of Journalists, Activists Worldwide (The Washington Post), Washington, DC (https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/, 01.09.2022).

RASHEED, JAWAD ET AL. 2021: COVID-19 in the Age of Artificial Intelligence: A Comprehensive Review, in: Interdisciplinary Sciences: Computational Life Sciences, Vol. 13/2, pp. 153-175.

RODRIGUEZ CONTRERAS, RICARDO 2021: COVID-19 and Digitalisation (Eurofound), n.p. (https://www.eurofound.europa.eu/data/digitalisation/research-digests/covid-19-and-digitalisation, 12.08.2022).

SAGLAM, KORAY 2022: The Digital Blender: Conceptualizing the Political Economic Nexus of Digital Technologies and Authoritarian Practices, in: Globalizations, Vol. 19/7, first online.

SCHLUMBERGER, OLIVER/EDEL, MIRJAM/MAATI, AHMED/SAGLAM, KORAY 2022: How Authoritarianism Transforms: A Framework to Study Digital Dictatorship. Unpublished Manuscript (under review).

SHAHBAZ, ADRIAN/FUNK, ALLIE 2019: Freedom on the Net 2019: The Crisis on Social Media. Washington, DC: Freedom House.

SHAHBAZ, ADRIAN/FUNK, ALLIE 2020: Freedom on the Net 2020: The Pandemic's Digital Shadow. Washington, DC: Freedom House.

SHAHBAZ, ADRIAN/FUNK, ALLIE 2021: Freedom on the Net 2021: The Global Drive to Control Big Tech. Washington, DC: Freedom House.

SIMPSON, KAITLYN 2019: Flaw in WhatsApp Exploited to Target Human Rights Lawyer, Finds Citizen Lab (The Varsity), Toronto (https://thevarsity.ca/2019/06/26/flaw-in-whatsapp-exploited-to-target-human-rights-lawyer-finds-citizen-lab/, 25.09.2019).

SORGNER, ALINA 2021: The COVID-19 Crisis and Digital Transformation: What Impacts on Gender Equality?, n.p. (https://www.unido.org/stories/covid-19-crisis-and-digital-transformation-what-impacts-gender-equality, 12.08.2022).

STANFORD AI INDEX 2022a: Global AI Vibrancy Tool (Stanford Institute for Human-Centered Artificial Intelligence), Stanford (https://aiindex.stanford.edu/vibrancy/, 06.09.2022).

STANFORD AI INDEX 2022b: The AI Index Report - Artificial Intelligence Index (Stanford Institute for Human-Centered Artificial Intelligence), Stanford (https://aiindex.stanford.edu/report/, 06.09.2022).

VAN CLEAVE, KRIS 2021: Facebook Whistleblower: Internal Documents Detail How Misinformation Spreads to Users (CBS News), Washington, DC (https://www.cbsnews.com/news/facebook-whistleblower-frances-haugen-documents-misinformation-spread/, 24.08.2022).

WANG, GUANHUA/ZOU, YONGPAN/ZHOU, ZIMU/WU, KAISHUN/NI, LIONEL M. 2016: We Can Hear You with Wi-Fi!, in: IEEE Transactions on Mobile Computing, Vol. 15/11, pp. 2907-2920.

WHO (World Health Organization) 2020: Ethical Considerations to Guide the Use of Digital Proximity Tracking Technologies for COVID-19 Contact Tracing: Interim Guidance, Geneva (https://apps.who.int/iris/bitstream/handle/10665/332200/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1-eng.pdf, 12.10.2022).

WHO (World Health Organization) 2022: Infodemic, Geneva (https://www.who.int/health-topics/infodemic, 01.09.2022).

WILLIAMS, SIMON N./ARMITAGE, CHRISTOPHER J./TAMPE, TOVA/DIENES, KIMBERLY 2021: Public Attitudes towards COVID-19 Contact Tracing Apps: A UK-Based Focus Group Study, in: Health Expectations: An International Journal of Public Participation in Health Care and Health Policy, Vol. 24/2, pp. 377-385.

XIN, TONG/GUO, BIN/WANG, ZHU/LI, MINGYANG/YU, ZHIWEN 2016: FreeSense: Indoor Human Identification with WiFi Signals, Xi'an (http://arxiv.org/abs/1608.03430, 06.09.2022).

ZUBOFF, SHOSHANA/MÖLLERS, NORMA/WOOD, DAVID MURAKAMI/LYON, DAVID 2019: Surveillance Capitalism: An Interview with Shoshana Zuboff, in: Surveillance & Society, Vol. 17/1-2, pp.257-266.

THE AUTHOR

AHMED MAATI
Postdoctoral Researcher at the Hochschule für Politik, Technical University of Munich

Institut für Entwicklung und Frieden (INEF),
Universität Duisburg-Essen, Duisburg

sef: Stiftung Entwicklung und Frieden
Development and Peace Foundation

INEF

GLOBAL TRENDS. ANALYSIS

examines current and future challenges in a globalised world against the background of long-term political trends. It deals with questions of particular political relevance to future developments at a regional or global level. GLOBAL TRENDS. ANALYSIS covers a great variety of issues in the fields of global governance, peace and security, sustainable development, world economy and finance, environment and natural resources. It stands out by offering perspectives from different world regions.