The Unfreedom Monitor

A Methodology for Tracking Digital Authoritarianism Around the World

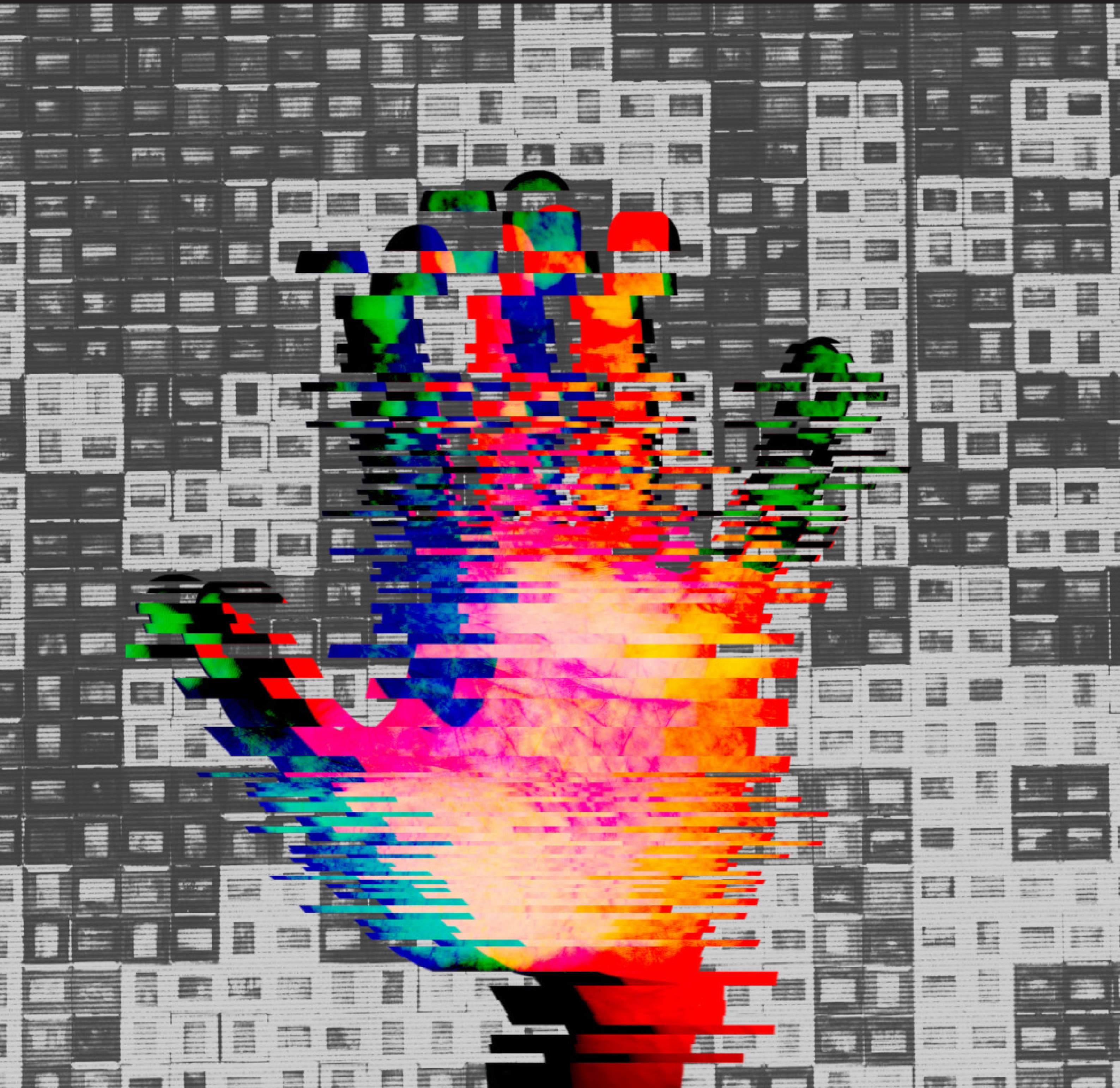


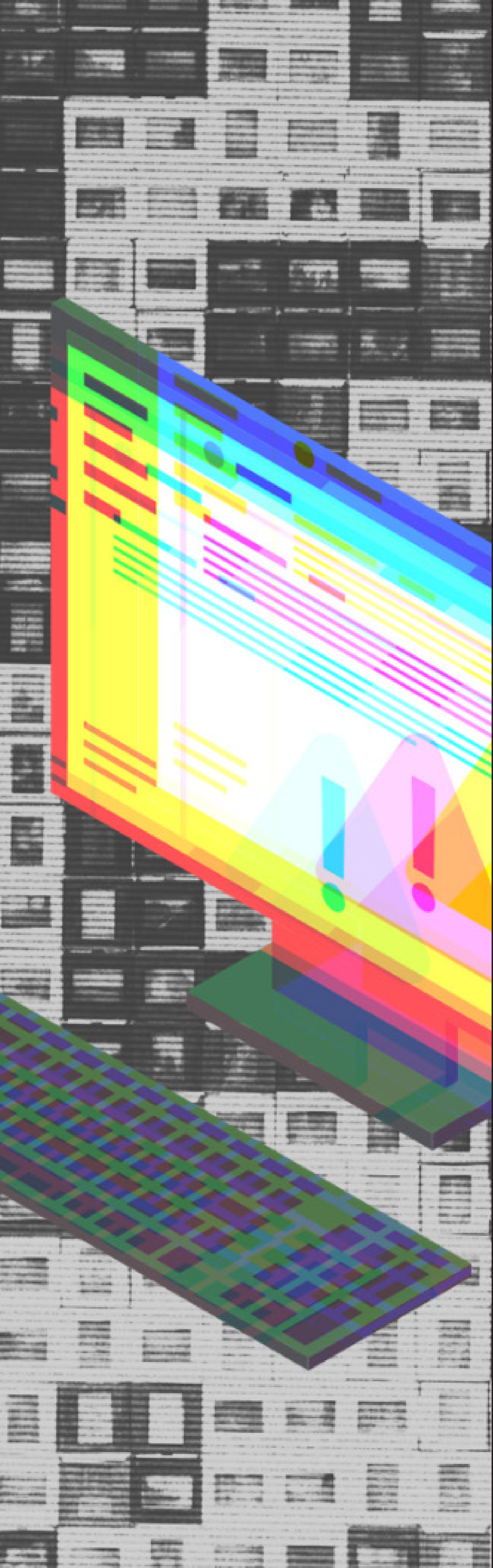
Table of Contents

Acknowledgements

This report is the collective work of 20 people spread across multiple countries and working in time zones spanning more than half of the world. Desk research was supported by colloquia and research assistance from the Global Voices community. In the interests of security, the names of all the team members have been withheld in this report. For citation purposes, the report can be attributed to the "Advox Team". Any errors or omissions should also be addressed to the general Advox team at **advox@globalvoices.org**. Funding for this project was provided by the Deutsche Welle Academy (DW) which in turn received funding from the Federal Republic of Germany through the BMZ.

© Advox

Stichting Global Voices
Kingsfordweg 151
1043GR Amsterdam
The Netherlands
https://globalvoices.org



Executive Summary

1

Digital communications technologies have been a powerful tool in the advancement of democratic governance, but in recent years there is concern that they are being used to undermine democracy as well. The Unfreedom Monitor, part of Global Voices' Advox project, aims to study and report on this growing phenomenon. This briefing document provides an overview of key developments in digital authoritarianism in a sample of 10 countries, while explaining the theoretical framework and methodology behind the project. The document also provides a basis for expanding this research to other countries so we can deepen our understanding of digital authoritarianism globally as well as its crucial implications for the future.

"Digital authoritarianism" describes the use of technology to advance repressive political interests. It is not purely confined to authoritarian regimes. Democratic states have also used and sold advanced technology to track and/or surveil citizens, spread mis/disinformation and disempower citizens' civic and political participation. Nor is it only states that perpetrate digital authoritarianism. In fact, corporations located in democratic countries are key suppliers of the technology that is used. The growth of digital authoritarianism highlights an important paradox: the internet, seen in its early days as a utopian project that promoted civic and political participation, can also be used as a tool to quash the same behaviour that it can help foster. By understanding authoritarianism as a process rather than an event, and by focusing on political choices that exacerbate this process, we can deepen our understanding of how technology impacts human rights. This is especially relevant in the context of the COVID-19 pandemic and how technology that was built to stem the spread of the virus also provided considerable surveillance power to the state.

For this report, a sample of 11 countries was chosen to reflect a range of factors: government type, approach to human rights (including rankings in indexes), and corporate relations. These countries are: Brazil, Ecuador, Egypt, India, Morocco, Myanmar, Russia, Sudan, Tanzania, Turkey and Zimbabwe. This desk research supplements a qualitative study of a dataset consisting of media items exploring issues, events, actors, media frames and responses to identify trends and patterns of digital authoritarianism. Researchers also worked within four cross-cutting themes concerning digital authoritarianism to develop an approach that can be used across contexts.The four cross-cutting themes of digital authoritarianism are: data governance, speech, access, information, explained further below:

1. **Data governance** is a major cross cutting theme that concerns practices like surveillance and data privacy. In fact, surveillance is the practice of digital authoritarianism most likely to emerge in countries regardless of whether they are considered a democratic or autocratic state, and many surveillance companies are based in economically-advanced countries that would be considered democratic. Many of the countries in this study have been linked to purchases of malware and other cyber-surveillance weapons, such as NSO Group's Pegasus software. Contract tracing apps for COVID-19 (such as India's Arogya Setu), national registration and systems, and the use of facial recognition and AI-powered CCTV.

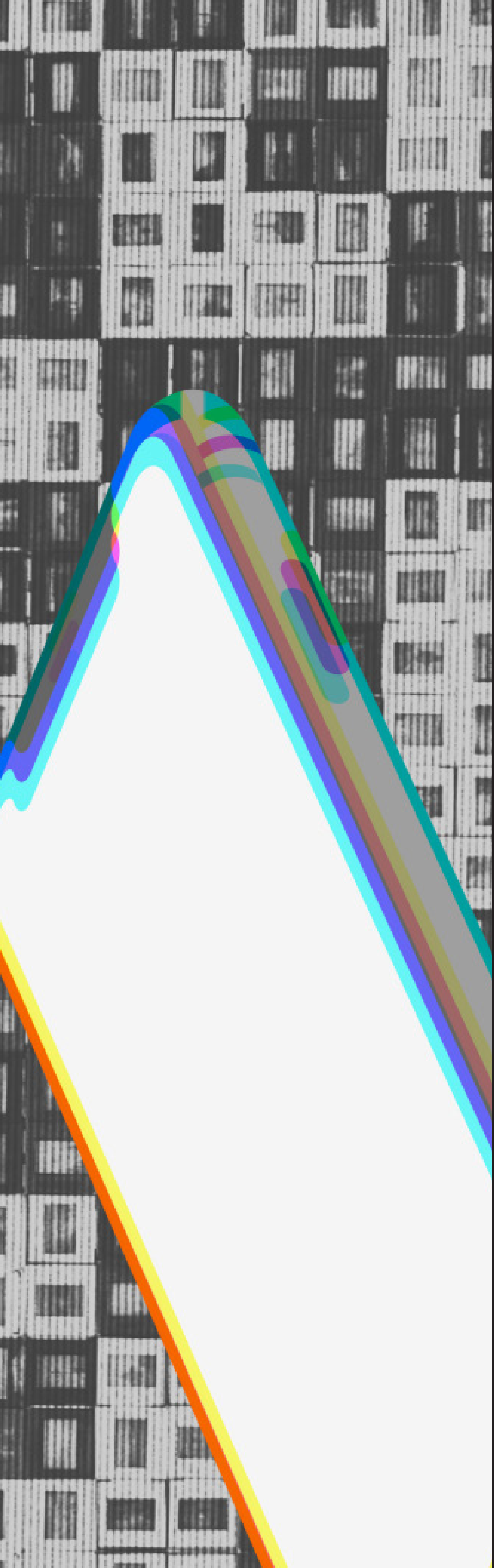
2. Constraining freedom of expression and curbing **speech** is an important aspect of digital authoritarianism. In countries like Ecuador, Morocco, Russia and Turkey, media laws have placed heavy penalties on freedom of expression, especially in the

online sphere. With the changing landscape of information-sharing, many of them don't apply to just journalists but also netizens, including social media influencers. In Egypt, for example, 500 websites have been blocked since 2017, and social media policing is widespread. Moroccans have been prosecuted for the content of their Facebook posts under the country's harsh media laws.

3. If users do not have **access** to the internet, their ability to engage in civic and political discourse is drastically reduced. Governments have done exactly that during times of upheaval or strong dissent (eg., the Myanmar coup, during citizen protests in India and in the run-up to elections in Tanzania). This stifles the free flow of information and is very costly.

4. States and government-affiliated bodies have also been identified as controlling the flow of **information**, by perpetrating large-scale disinformation campaigns as a way of promoting digital authoritarianism. In Brazil, Jair Bolsanaro is linked to a government-funded 'digital militia' that has spread false news about COVID-related topics. Influencers have been paid to spread unverified information. In India, PM Modi and his BJP party have long used their social media presence to promote their brand, with BJP-linked accounts trolling religious and political minorities.

In conclusion, this report finds that digital authoritarianism is not confined to authoritarian states. Rather, it is a culture — of increasing executive power, legislation and global capital flows — that allows the state to interfere in citizens' lives and to stifle or frustrate civic engagement. There is no single predictive factor, but digital authoritarianism is closely related to the contraction of press freedom. Moreover, it is a transnational process, and the availability of technology in one part of the world will eventually have political consequences in another. By providing examples and context to this phenomenon, this report highlights factors that point to the potential emergence of digital authoritarianism, as well as the urgency of need to prevent its unchecked spread.



Introduction

2

The Unfreedom Monitor is a project to analyse, document, and report on the growing phenomenon of the use of digital communications technology to advance authoritarian governance. The initial phase of the project tracks and documents key developments in digital authoritarianism in selected countries. This briefing note captures the theoretical and methodological rationale for the project.

Authoritarian and dictatorial regimes have a complicated relationship with media and communications technologies, using them to advance their goals, messaging and propaganda while restricting access for others in order to shape and warp reality, conceal abuses, and maintain power. This dynamic has continued with the growth of the internet and related digital technologies. While a dominant narrative about the internet has been its potential for liberation, it is increasingly used by authoritarian-minded governments as a tool for deception, propaganda and control.

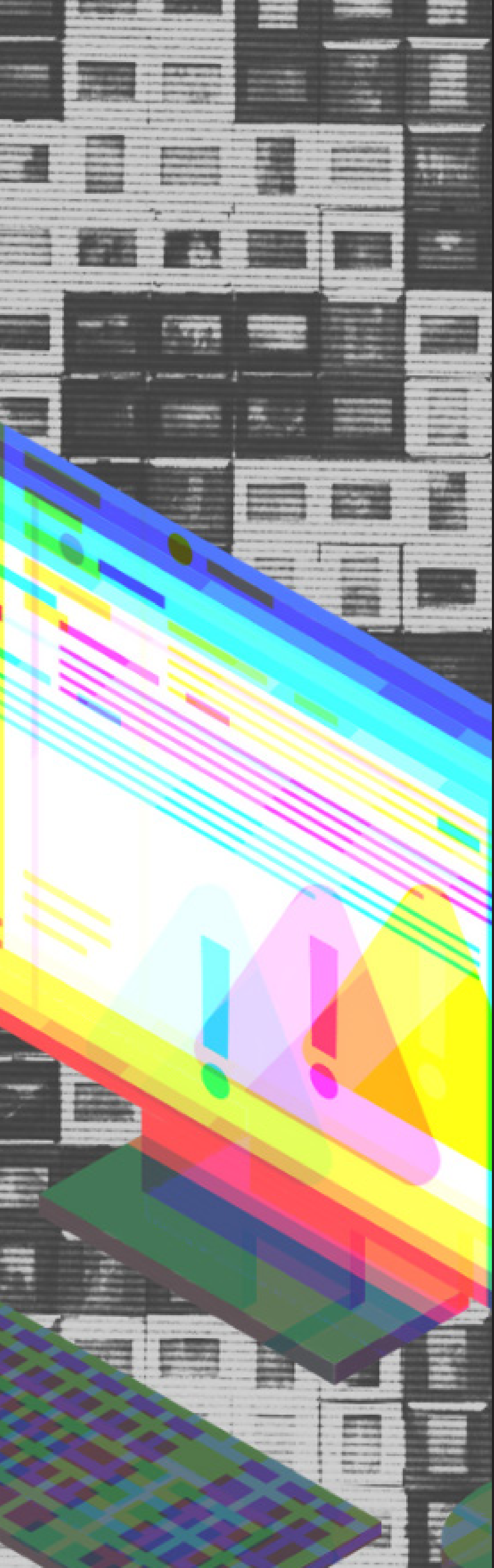
In 2010 Global Voices' co-founder Rebecca MacKinnon coined the term "networked authoritarianism" to define China's complicated manipulation of the internet in the maintenance of its power (Mackinnon 32). The Chinese government had allowed for the semblance of "authoritarian deliberation" on issues that furthered the regime's ends, while at the same time using the technology as a means of surveillance and control. The government severely restricted information, deliberation, and activism with the potential to threaten its hold on power. Global Voices has been tracking and documenting this phenomenon in China and many other states, primarily through our Advox project, since 2007 (Advox).

In the intervening decade, what is now known as digital authoritarianism has become evident in both authoritarian regimes and increasingly in democratic states. States, governments and political parties, often in collaboration with corporations, harness the power of an internet dominated by advertising technology that tracks and segments users for commercial gain. Technological advances, including exponentially powerful machine learning, facial recognition, and the use of artificial intelligence for "predictive" analysis, combined with the ubiquity of CCTV cameras, communications mobility, and embedding of sensory intelligence in consumer goods create pervasive surveillance. These technologies are often used not just to sell products, but as a tool for population control, to distort information and to disempower people in civic and political arenas. The use of technology is also increasingly a major component of international conflict and competition, including corporate and state intelligence-gathering and cyber attacks in both peace and war.

Beginning in 2009, Global Voices launched a documentation project to track threats to online expression and civics, and to call attention to the many ways state power is being used to control and harm citizens' attempts to exercise their fundamental liberties. Named Threatened Voices, the project over eight years documented nearly a 1000 cases of individuals targeted for their online activities (Global Voices). We built a prototype method and platform to help document and analyse the information about threats to online expression, even as these threats morphed from threats to individuals to threats to systems, affecting entire populations and targeting millions. We found that states became more sophisticated in their ability to detect, repress and target organising, expression and activism. Increasingly, states also combined targeted denial of information services with powerful surveillance and the ability to "flood the zone" with false and misleading information, using automated technologies and the networked power of supporters. These forces are converging in ways that both enforce the power of existing authoritarian powers and threaten the stability of long-standing democracies.

A more recent Global Voices project running since mid-2019 is the Civic Media Observatory, which offers a method for fine-grained analysis of complex media ecosystems (Global Voices). The Observatory supports careful research and reporting into information systems, giving insight into a key element in authoritarian efforts to confuse, mislead and deceive people. The Observatory has since run more than a dozen investigations, including in-depth, transnational research into infodemics related to COVID-19 and Chinese soft power in Belt & Road Initiative countries.

With the Unfreedom Monitor, Advox and Global Voices aim to combine these methodologies with in-depth country research, to provide a roadmap for possible research into other countries, thereby deepening our collective understanding of the motivation, dynamics and possible future directions of digital authoritarianism globally. This report provides a theoretical and analytical framework for understanding this work.



3

Understanding Digital Authoritarianism

A common definition of digital authoritarianism is "the use of digital information technology by authoritarian regimes to surveil, repress and manipulate domestic and foreign populations" (Feldstein). Practices that fall under the umbrella of digital authoritarianism include: surveillance, censorship, social manipulation and harassment, cyber attacks, internet shutdowns and targeted persecution against online users (Feldstein). By extension, social manipulation includes the use of coordinated inauthentic behaviour, as well as misinformation and disinformation campaigns. Artificial Intelligence is also implicated in programmes like smart cities, facial recognition, and smart policing initiatives (Feldstein). Digital authoritarianism or networked authoritarianism as defined by MacKinnon also manifests across a variety of platforms including traditional and digital media, journalism institutions, social media and interpersonal communication networks (mobile phones and messaging platforms (Chan 66). "Networked authoritarianism" places specific emphasis on the role of media and information outlets to create the conditions that enable authoritarian practices including mobilisation and misinformation (Chan 66). Thus, curtailing freedom of expression targeting media outlets, and fostering false narratives are also key practices that enable digital authoritarianism.

In contemporary political science, the concept of authoritarianism is loaded with normative considerations about certain types of government in certain regions of the world. The tendency has been to label countries outside the Western neoliberal order as authoritarian. However, contemporary events show that authoritarian tendencies can befall any system of government and it is a matter of scholarly integrity to broaden the discourse on authoritarianism to look at various types of government around the world. Significantly, there is also a pattern of companies based in nominally democratic countries building and exporting technologies that enable authoritarianism in other parts of the world, which also contributes to a global context of authoritarianism. These same technologies are being used in democratic states as tools for governance, in forms that strike many observers as undemocratic or unethical. Hintz and Milan for example, focus their analysis on what they call "surveillance culture" in the West, in which surveillance is normalised and institutionalised in Western governments as part of legitimate state practice (4). Indeed, China, often described by Western scholars as a leading exponent of digital authoritarianism, is not strictly speaking a leading exporter of hacking technology, even while it may deliberately provide technology vulnerable to hacking to other countries.

The early days of global internet access were characterised with high levels of utopianism about the political disruption the internet might trigger, specifically focusing on how it might help individuals to self-organise outside of state control. The idea of reconstituting the body politic to suit the individual as opposed to groups organised around political identities was a major part of the attraction of moving political discourses online.

In recent years this optimism has cooled as governments work to maintain a significant capacity to influence political behaviour online. Similarly, private capital is increasingly misusing the concept of digital freedom to enable exploitation and manipulation of ordinary people. There is a real tension over what to do about digital authoritarianism. On one hand, many states, advocacy organisations and citizens continue to support an internet that is open for individuals to seek out and participate in political expression. On the other hand, there is a growing concern that without meaningful regulation, billions of people are vulnerable to exploitation and manipulation when information systems are shaped primarily in the interests of profit.

In addition, maintaining open internet spaces when malevolent state-sponsored actors actively export disinformation as a geopolitical strategy is a challenge. Paradoxically, democracies that have long-standing history for building and maintaining open, free spaces for expression are now considering regulations that restrict both types of individual expression and some foreign information providers, on the grounds that they systematically spread falsehoods and propaganda. It is a practical response that recognises that the nature of the government - whether it is authoritarian or not - affects the approach to regulation.

What then does regulation that benefits people look like and where does it begin? Understanding digital authoritarianism is critical to answering this question properly, particularly in the context of a global pandemic. It becomes crucial to distinguish between practices that represent a social contract of the digital age that justly constrains the rights of some internet users only insofar as it enables the rights of others, and practices that are designed to extend the power of the state, curb freedoms and expand oppression. It becomes important to identify trends and patterns that begin the descent to authoritarianism before they take root. It also becomes important to identify the correct balance of power between citizens, corporations and their governments, and particularly structures that protect individuals and their communities first.

> “*It becomes crucial to distinguish between practices that represent a social contract of the digital age that justly constrains the rights of some internet users only insofar as it enables the rights of others, and practices that are designed to extend the power of the state, curb freedoms and expand oppression.*”

DEFINING AUTHORITARIANISM

A good place to begin the conversation on digital authoritarianism is by defining authoritarianism more broadly. Authoritarianism is connected to centralised power structures, a lack of accountability of a state to its citizens and repression of political dissidence (Hintz and Milan). It is insufficient to focus on the source of the authoritarianism rather than its outcomes, and to argue that authoritarian impulses in marginally democratic countries are a product of different forces than authoritarianism in liberal democracies (Hintz and Milan). Surveillance and disinformation, for example, are a part of political behaviour in the United States, United Kingdom and many European countries but these countries are rarely labelled authoritarian, because governments are widely viewed as having legitimate access to power as a result of free and fair electoral systems. Laws such as the Patriot Act in the United States enable widespread surveillance of individuals and specific groups but they do not generally lead to the US being labelled authoritarian.

> “*...authoritarianism refers to practices that shift power away from citizens and towards centralised authority regardless of the character of that authority*”

Rather, it can be insightful to focus equally on the ability of citizens to push back against overreaches of power as the threshold to say whether or not a regime is authoritarian: can citizens dissent? Understanding authoritarianism is about understanding balance, and overall, authoritarianism refers to practices that shift power away from citizens and towards centralised authority regardless of the character of that authority (military or civilian, monarchy or elective, working class or elitist etc.).

Even so, this labelling might be counterproductive in the long run because it assumes that authoritarianism is an event rather than a drawn-out process of decline in civic space. Dragu and Lupu argue that to properly measure the impact of technology on human rights, it is important to zoom out from moments of active repression to political choices made in advance designed to create an oppressive context (Dragu and Lupu, 991). They argue that to accurately measure the impact of technology on human rights, we have to measure the interplay between the actions of the state and the reactions of the opposition or dissenters, rather than one or the other. They use the concept of "preventive repression" to refer to a set of activities that governments use to reduce the risk of dissent, including identifying, monitoring and tracking potential regime opponents in order to neutralise them (Dragu and Lupu, 993).

For this reason the Unfreedom Monitor not only looks at practices of reprisals against human rights activists and dissenters, but more broadly at uses of technology that create an enabling environment for authoritarianism, including surveillance and abuse of legislative processes. It is not enough to observe that authoritarian regimes might be opposed to the internet. Indeed, several authoritarian regimes invest significantly in technology as a way of expanding their influence over politics domestically and internationally (Dragu and Lupu, 1010). Government action and opposition reaction occur in a single ecosystem and the observatory method allows us to track both what governments do and what societies do in response to those efforts.

Using their quantitative analysis, Dragu and Lupu broadly find that technological innovation increases opportunities for oppression. They find that internet freedom is generally on the decline around the world, that many governments are introducing restrictions on freedom of speech and online discourse, and that the use of digital technologies enhances the capacity of states for preventative repression. They also find that decision-making or selective permission is a key part of the metrics important to measuring authoritarianism. Significantly, Dragu and Lupu also argue that technology creates the possibility for non-physical authoritarian actions (Dragu and Lupu, 1010). Whereas in previous eras, governments would frequently employ force against dissent, in the present day, governments frequently resort to non-physical tactics enabled by technology, even as media and activists continue to focus their attention on the use of force. A decline in the number of physical integrity violations of human rights therefore may not be an indicator of an improving rights context, but perhaps of a shift in tactics from authoritarian regimes.

Dragu and Lupu argue that technology lowers the cost of curbing dissent because it allows practices historically designed to chill public discourse to happen with fewer inputs (996).Often the same technology that enables dissenters to organise and mobilise can be used to stifle their dissent, as when governments use social media monitoring tools to police protest movements and charge them with offences committed during such events.

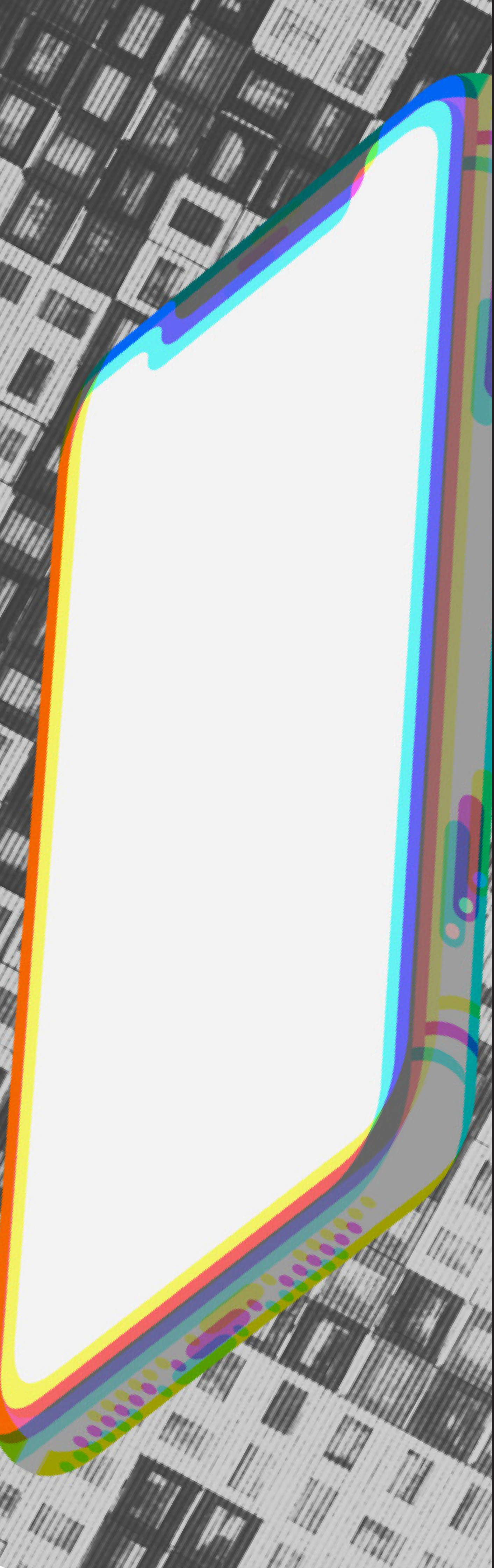
They also find that authoritarian governments' decisions on creating a permissible environment for technology hinges on the extent to which it enables their authoritarianism (995). Strategic applications of technology increase the capacity of states to create an enabling environment for the suppression of human rights. Moreover, as technology has played a key role in political mobilisations all over the world, governments are keen to stay ahead of dissenters and opponents. This creates an incentive to invest in cutting-edge technologies designed to constrain human rights.

Yet, liberal democracies are also implicated in some of the practices that limit political pluralism. Fuchs argues that digital technology empowers dangerous right-wing authoritarian movements in the same way that nationalist movements in the early 21st century relied on individual uninformed charisma and spectacles to influence public discourse (Fuchs). Similarly, the market logic of private media may open opportunities for authoritarian leaders, as the competition for views and for clicks may create incentives for the purchasing of influence or the advancement of fascist talking points in order to attract financing (Chan 65). The implication is that it is ahistorical and incomplete to think about digital authoritarianism as a distinct historical development simply because it uses novel technologies to advance historical practices.

The COVID-19 pandemic has brought renewed interest in digital authoritarianism. Legislation designed to address the pandemic has strayed dangerously near to authoritarian practice in numerous countries. The use of systemic surveillance, the creation of large data sets, mandatory digital identity and digital health records are all systems that require careful governance and boundary setting, and are rife for abuse by governments seeking to maintain or increase power. These measures may remain as tools of governance long after the immediate crisis ends (Nabben et al.). Some governments, such as Singapore, have used COVID-19 surveillance measures to expand the capacity of the surveillance state. In China, the government expanded city-wide lockdown measures to the digital arena, including using location monitoring on sites like WeChat and Alipay to constrain access based on a health rating risk (Nabben et al.). Hungary went to the extreme of criminalising criticisms of the government's response to the pandemic, while in Bulgaria the government expanded its ability to track mobile phone users (Nabben et al.). In the United States, the government has partnered with private corporations to collect and analyse data with little public accountability over what the data will be used for once the emergency passes (Nabben et al.). Many of these surveillance regimes do not have privacy built into their logics and therefore create vulnerability for citizens. Over the long term, the value of these surveillance capacities and their impact on the pandemic beyond the initial stages remains to be seen. COVID-19 has regardless become a global disease and some of the countries with elaborate surveillance systems are still struggling with it.

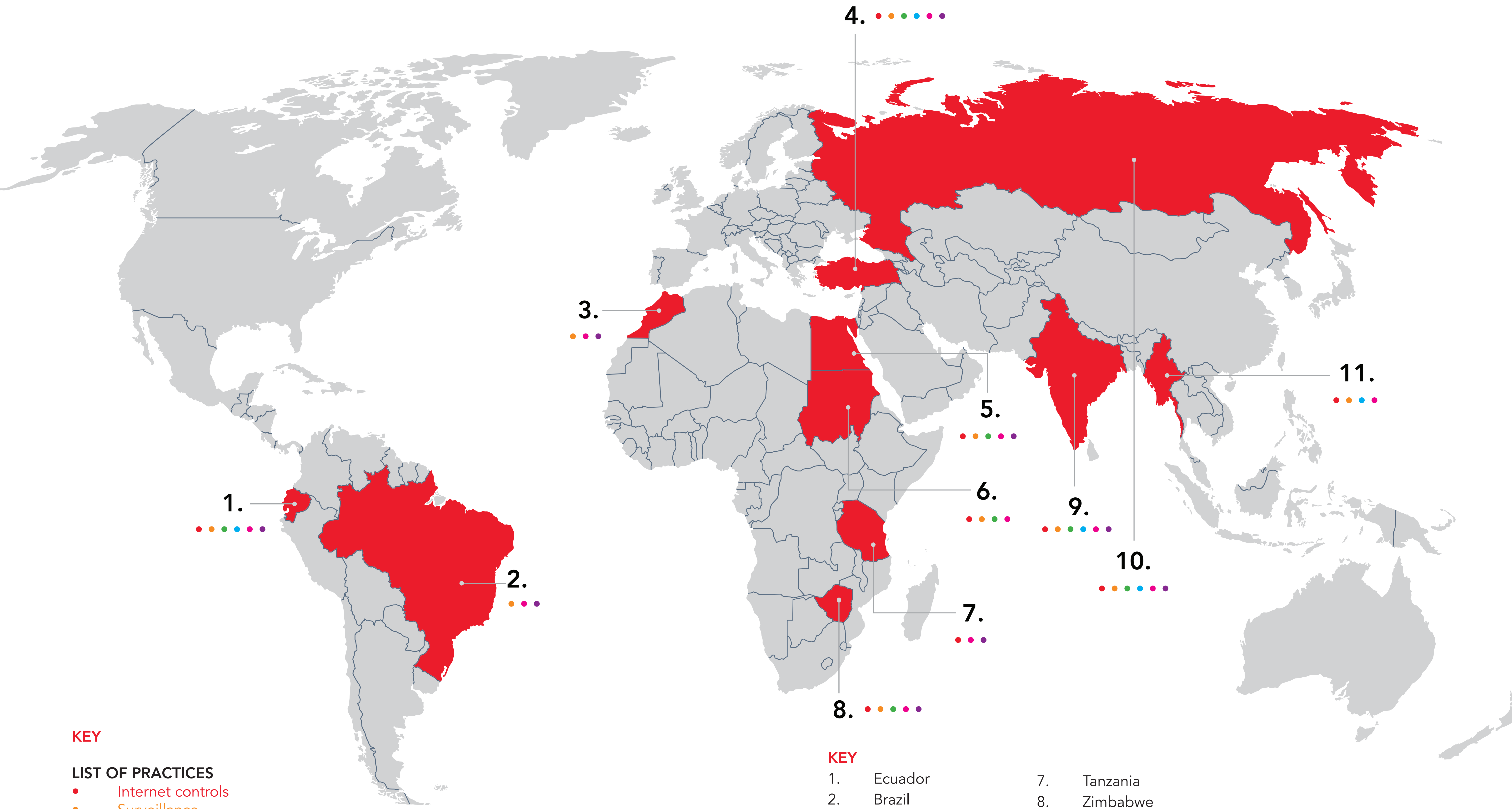
Moreover, the COVID-19 pandemic is also demonstrating that the origins of digital authoritarianism cannot solely be focused on the role of the state. The libertarian side of the internet has also fallen prey to coordinated disinformation efforts, proliferation of bots and transnational influence campaigns (Nabben et al.). As more communication has shifted online in light of the pandemic, hacking, malware attacks and video bombing of virtual communications has also increased significantly (Nabben et al.). Health records collected for managing the pandemic have also been hacked. This is a specific vulnerability for countries that have not anonymised their data by default (Nabben et al.). Only a small number of nations such as Taiwan have used the pandemic as an opportunity to decrease the space for digital authoritarianism by making public, statewide commitments to foregrounding privacy as the default standard in the new technologies that are built.

Therefore, a major goal for the Unfreedom Monitor is to expand our notions of what constitutes digital authoritarianism and to move beyond the type of government or its relationship to the Western neoliberal state to think more critically about the dynamics of power between the citizen, the internet, and the public sphere. The Unfreedom Monitor is premised as a global monitor that looks at various types of governments specifically to understand the contexts in which digital authoritarianism is enabled or normalised. The research will also unite cross-cutting themes across various regions to overturn normative presumptions about digital authoritarianism as a regionally specific practice, and instead aim for a diagnostic method that can be deployed across political contexts to help observers and analysts anticipate the emergence of authoritarian practices and to respond to them properly.



Methodology

4



KEY

LIST OF PRACTICES

- ● Internet controls
- ● Surveillance
- ● Information manipulation
- ● Technology controls
- ● Freedom restrictions
- ● Systems attacks

KEY

1.	Ecuador	7.	Tanzania
2.	Brazil	8.	Zimbabwe
3.	Morocco	9.	India
4.	Turkey	10.	Russia
5.	Egypt	11.	Myanmar
6.	Sudan		

The country selection for the Unfreedom Monitor is premised on identifying a sample of countries that reflect a variety of types of government, corporate relations and approaches to human rights. This is summarised in the matrix below:

Country and Style of government	CPJ Press Freedom Rankings 2020 (Out of 180)	Freedom House Ranking	Key Political characteristics	Digital Authoritarian practices
Brazil *Democratic, autocratic tendencies from a democratically-elected president*	111	Free, 74	Misinformation and disinformation;	• Influence campaign • Misinformation • Disinformation • Coordinated Inauthentic Behaviour • Information ecosystem shaping • Device based surveillance • Freedom of restriction • Freedom of the media • Hacking
Ecuador *Democratic with unstable transitions*	96	Partly Free, 67	Frequent changes of government, arrests and detentions of journalists	• Public digital surveillance • Online tracking • Surveillance • Intimidation of journalists • Hacking
Egypt *Military regime, coup d'etat, protests, ongoing international conflicts*	166	Not free, 18	Arrests and intimidation of opposition, journalists and critics; international conflicts	• Internet access restrictions • Social media access restrictions • Internet Shutdowns • ISP controls • Public digital surveillance • Physical surveillance • Informants • Online tracking • Influence campaign • Information ecosystem shaping • Misinformation and disinformation • Arrests and intimidation of journalists • Restricted freedoms of privacy, data, expression, movement and media • Hacking

Country and Style of government	CPJ Press Freedom Rankings 2020 (Out of 180)	Freedom House Ranking	Key Political characteristics	Digital Authoritarian practices
India *Democratic elections, dominant party, religious factionalism*	142	Partly Free, 67 (Kashmir, Not free, 27)	Gross inequality, digital ID system deepens exclusion; mis/disinformation related to minority groups	• Internet access restrictions • Internet shutdowns media access restrictions • Social media restrictions • Social media shutdowns, bandwidth throttling • Extended internet and social media shutdowns • Public digital surveillance • Physical surveillance • Coordinated Inauthentic behaviour • Information ecosystem shaping • Arrests and intimidations of journalists • Judicial intimidation • Restricted freedoms of privacy, data and media • Hacking
Morocco *Monarchy, strong military presence in public life; judicial interference.*	136	Partly Free, 37	Arrests and intimidation of journalists, Pegasus linked to government officials	• Public digital surveillance • Informants, Information ecosystem shaping • Intimidation of journalists,disinformation • Judicial intimidation • Restricted freedom of privacy, expression and media • Hacking
Myanmar *Military regime, Coup d'etat, ongoing domestic conflicts*	140	Not Free, 28	Refugee and IDP identities point of contention; targeted violence against ethnic minorities; reprisals for political protesters	• Internet access restrictions • Internet shutdown • Social media access restrictions • Bandwidth throttling • Punitive internet taxes • ISP control • Public digital surveillance • Internet of things • Physical surveillance • Informants • Online tracking • Device based surveillance • Tech service and platform blocking • Arrests and intimidation of journalists • Restricted freedom of privacy, data, expression, media and movement

Country and Style of government	CPJ Press Freedom Rankings 2020 (Out of 180)	Freedom House Ranking	Key Political characteristics	Digital Authoritarian practices
Russia *Centralised executive, uncompetitive elections*	150	Not free, 20	Compromised elections, intimidation of journalists and members of the opposition; repression of gender and sexual minorities; Conflict; harsh penalties for citizens protesting the invasion of Ukraine and independent journalists covering it, including in the digital sphere.	• Internet access restrictions • Social media access restrictions • ISP controls • Public digital surveillance • Online tracking • Disinformation • Misinformation • Influence campaign • Coordinated inauthentic behaviour • Information ecosystem shaping activities • Device based surveillance • Network interference • Platform blocking • Restricted freedom of privacy, data, expression, movement and media • Judicial intimidation
Sudan *Military regime/ hybrid following military coup, transition process, large demonstrations against the government*	159	Not Free, 17	Politically ambiguous situation, internet shutdowns	• Internet access restrictions • Internet shutdowns • Social media access restrictions • Social media shutdowns • Bandwidth throttling • Public digital surveillance • Physical surveillance • Online tracking • Influence campaign • Coordinated inauthentic behaviour • Restricted freedoms of privacy, expression and media
Tanzania *Democratic election, dominant party, centralised executive*	124	Partly Free, 34	Constrained freedom of expression	• Internet access restrictions • Internet shutdowns • Social media access restrictions • Social media shutdowns • Bandwidth throttling • Punitive internet taxes • ISP controls • Arrests and intimidation of journalists • Restricted freedoms of privacy, data, expression and media • Hacking

Country and Style of government	CPJ Press Freedom Rankings 2020 (Out of 180)	Freedom House Ranking	Key Political characteristics	Digital Authoritarian practices
Turkey *Long-serving autocrat, questionable electoral process, significant conflict zone, major presence of refugees from regional conflict, economic deterioration*	153	Not Free, 32	Failed military coup in 2016 that triggered a wave of arrests of journalists, academics, rights defenders	• Arrests and intimidation of journalists and human rights activists • Judicial intimidation • Internet access restrictions • Internet shutdown • Social media access restrictions • Social media shutdown • Bandwidth throttling • Punitive internet taxes • ISP controls • Surveillance • Public digital surveillance • Internet of things • Physical surveillance • Informants • Online tracking • Information manipulation • Influence campaign • Disinformation • Misinformation • Coordinated inauthentic behaviour • Information ecosystem shaping (creating propaganda outlets, e.g.) • Import restrictions • Device-based surveillance • Network interference • Privacy • Data • Expression • Movement • Media • Hacking

Country and Style of government	CPJ Press Freedom Rankings 2020 (Out of 180)	Freedom House Ranking	Key Political characteristics	Digital Authoritarian practices
Zimbabwe *Independence party controls the public sphere, deteriorating economic conditions*	130	Not Free, 28	Contested elections, threatening and intimidation of political opponents.	• Internet shutdown • Social media access restrictions • Social media shutdown • Bandwidth throttling • Punitive internet taxes • ISP controls • Public digital surveillance • Internet of things • Physical surveillance • Informants • Online tracking • Information manipulation • Influence campaign • Misinformation and disinformation • Coordinated inauthentic behaviour • Information ecosystem shaping (creating propaganda outlets, e.g.) • Device-based surveillance • Network interference • Violations of freedoms of: - Privacy - Data - Expression - Movement - Media

The Unfreedom Monitor combines the methodology used in Global Voices' previous work on media observatories with an in-depth analysis of the contextual issues around digital authoritarianism. The Observatory approach is primarily qualitative and looks beyond socio-technical causes to consider power analysis, offer a way to discuss effects, and to emphasise what works as well as what's negative. It is a framework that can be consistently applied across a range of contexts, in order to identify and contextualise both positive and disruptive developments, to explain the forces and motives underlying them, as well as the narrative framing devices that often require local knowledge to interpret and weigh. This method allows us to compare, draw lessons, and consolidate learning about the trends, systems and rules that influence what we know, and how we know it.

The observatory includes datasets of media items, structured analysis of context and subtext, and a civic impact score that rates media items for positive or negative impact on civic discourse. We use Airtable, a relational database, for documentation and collaborative work. The Unfreedom Monitor shifts the focus of the research to identifying and giving context to instances of digital authoritarianism. For a matrix of countries, technologies, and regulatory approaches, we will ask:

- What are the dominant and influential narratives?
- What is the evidence to support the claims underpinning these framings, and how will we document them?
- What are the actual harms, threats, and impacts of the use of technology to augment repression?
- What are potential solutions for technology interventions, policy advocacy, and information and awareness?
- What narratives more accurately reflect what is happening?

The findings of the observatory are presented separately as a dataset on the Advox website, and as part of the analysis presented in the individual country reports.

The key research question for the Unfreedom Monitor is: "What are the key motives for, methods of, and responses to, digital authoritarianism in selected national contexts?" This is further broken down into the following subquestions:

1. **Motives**
   a. What are the contexts that inspire authoritarians to clamp down on digital spaces?
   b. What are the immediate triggers of an expansion in digital authoritarianism?
   c. How do regional and international organisations affect how governments behave in relation to digital authoritarianism?

2. **Methods**
   a. What are the key technologies used in advancing digital authoritarianism?
   b. What are the key mechanisms — legal, economic etc. — through which these technologies are acquired and deployed?
   c. What role does money play in the choice of technologies?

3. **Responses**
   a. How do the citizens of the countries under investigation respond to the expansion of digital authoritarianism?
   b. How do other governments in the region and the international community respond to the expansion of digital authoritarianism?

With this information, the Unfreedom Monitor captures the key challenges of digital authoritarianism around the world, crafting a global perspective on the social and policy challenges that arise when the internet becomes the next frontier in the battle for meaningful democracy.

1. COUNTRY PROFILES

a. Brazil

Brazil is a representative democracy under a federal presidential constitutional republic system. The current president, Jair Bolsonaro, is a far-right politician who has been in politics for over 30 years and was selected in 2018 after contesting against the Workers' Party. Though Brazil is still a democracy, experts and campaigners say the country's democracy is in its most fragile state since the end of the military dictatorship, 37 years ago (Zanini). Bolsonaro's administration has the highest number of military personnel working within the Executive Branch since Brazil's democratic transition. The president and his allies have, on more than one occasion, made public remarks doubting the legitimacy of the electronic vote, verbally attacking Supreme Court justices, and raising the possibility of military intervention if the election does not roll out as he desires (Lellis; Della Coletta).

2013 was a watershed year for Brazil, triggering many of the country's current challenges. Demonstrations erupted around the country in June of that year, with protests initially directed towards an increase in public transportation fares (Winter). The movement soon incorporated other grievances, such as police violence, low public spending on health and education, elevated spending on mega sports events (in a window of two years, Brazil hosted both the World Cup and the Olympic Games), and government corruption. While the public transportation fare increase was reversed, many other grievances were unsolved, deepening people's dissatisfaction with representative politics. With a very diffuse agenda and no clear leadership in the protests, the movement was appropriated by both leftist and right-wing groups (Odilla).

The right-wing groups co-opted the momentum and staged protests focused on claims of government corruption, the World Cup investments, and a generalised dissatisfaction towards the Workers' Party. In 2015, demonstrations shifted to focus more strictly on Dilma Rousseff's administration, culminating in her eventual impeachment in August 2016 in what is today broadly considered a coup ("Manifestantes"). The Car Wash investigation targeting politicians associated with the Workers' Party continued over seven years, arresting and condemning over 100 people, including notable politicians like former president Luiz Inácio Lula da Silva. In fact, the June 2013 demonstrations triggered both Rousseff's impeachment and Lula's arrest (in 2018), empowering right-wing groups who had rallied around these demands. Soon, actors calling for military intervention and defence of Brazil's military dictatorship — once peripheral to the demonstrations— took centerstage. Significantly, buoyed by skillful use of social media, these groups found a supposedly anti-establishment candidate in Bolsonaro personification of these grievances and a belief that he could "clean the mess" left by Workers' Party governments.

By 2018, Brazil's political figures had broken into three clear groups: a pro-Bolsonaro group, a pro-Lula group, and a neither-nor group that failed to see itself represented in either of the two leading candidates. Bolsonaro was elected in the second round with 55% of valid votes (Reverdosa and Charner). He elevated many regional candidates with similar ideas, and represented a shift in Congress' composition, with new conservative actors allied to the president taking seats (Della Coletta and Benites).

Bolsonaro's popularity plummeted during the coronavirus pandemic ("Popularidade") during which he and his allies downplayed the severity of the virus, adopting a denialist stance towards lockdown and isolation measures, and acting to hinder Brazil's access to vaccines. Nonetheless, the president has been able to conserve a share of his electorate, part of which is very radicalised, echoing anti-democratic rhetoric against the Supreme Court, leftist politicians, journalists, and activists.

> *"...there is a group formed by government aides that act from within the presidential headquarters, which is responsible for producing misinformation and attacks against opposition figures"*

Social media remains a key element of Bolsonaro's strategy. Currently, this strategy plays out in two ways: use of official government channels to promote the administration and the president, which violates the Constitution; and funding bloggers, YouTubers, and WhatsApp and Telegram groups affiliated with allies. A Folha de S. Paulo report revealed that his campaign used mass messaging on WhatsApp, a practice now ruled illegal by the Supreme Court (Campos). During the pandemic, the government paid Instagram influencers to promote the use of hydroxychloroquine and other treatments that have no efficacy in treating COVID-19 (Martins and Fleck). Reports and ongoing investigations (Falcao and Vivas) also indicate that there is a group formed by government aides that act from within the presidential headquarters, which is responsible for producing misinformation and attacks against opposition figures ("Servidores"). This group, popularly called 'Hate Cabinet', has been deemed a "digital militia" by the Federal Police (Camporez et al.). In January, this group met with representatives for DarkMatter, a spyware developed by former Israeli army programmers.

Bolsonaro has also attacked journalists, a central hallmark of his political style ("Em novo meses"). Women journalists are frequent targets of attacks, with nearly 70% of them initiated by authorities, including Bolsonaro (Bergamo). In addition to attacks and scapegoating by the president himself, journalists have increasingly been attacked and harassed by civilians. The president has also limited journalists' access to his declarations by blocking some of them on social media (Martins).

b. Ecuador

From 1997 to 2007, Ecuador experienced a period of acute political instability. Over 10 years, the country had seven presidents. During that period, the country also ushered in a new constitution (1998); signed a peace treaty with Peru marking the end of the Cenepa war (1995) and delimited the 78 pending kilometres of one of the oldest border conflicts in Latin America; and endured a severe economic crisis (banking and financial, above all) that led the country to abandon the sucre (its currency) and become the only state in the South American Andean region to use a foreign currency as its own (the US dollar). Before this decision, Ecuador went through economic uncertainty including the so-called "banking holiday" — freezing of bank deposits similar to the "corralito" in Argentina in 2001. These events impacted the lives of Ecuadorian families, pushing many to migrate in pursuit of better living conditions in countries such as the United States and Spain.

The 2006 elections went to a second round, and Rafael Correa, an outsider and promoter of the Citizen Revolution, won. The Correísta government lasted 10 years. One of its first acts was to create a Constituent Assembly to draft a new constitution, which was endorsed by popular vote in 2008. The Constitution (still in force today) collects and expands rights of the natural environment or the recognition of Sumak Kawsay (a Kichwa word that means "good living"). This means that the citizens of Ecuador can enjoy and exercise their rights and demand that the authorities comply with them and install institutional mechanisms for that purpose.

The 10 years of Rafael Correa's term represented the political stability missing from the preceding years. However, the regime drifted into authoritarianism, increasingly characterised by the president's unilateral decisions; political persecution of social leaders and political opponents; pressure and intimidation of the media, and violations of freedom of expression, in addition to numerous cases of corruption related, above all, to the overpricing of public works.

Correa's government routinely and increasingly violated freedom of the press and expression in the country, especially from June 2013 when the Organic Law of Communication came into force after four years of deliberation. Among its most controversial aspects was the idea of "media lynching", which penalised dissemination of information designed to discredit a natural or legal person. Before this regulation, the country debated freedom of the press and expression when journalist Emilio Palacio published an opinion column titled "No to lies" (February 6, 2011) in the newspaper El Universo (Palacio). The column discussed the facts of the police revolt that occurred on September 30, 2010 in Quito, which the government described as a coup. Correa argued that the article affected his honour (implying slander) since the journalist called him a dictator and accused him of having issued an order to "fire at will" in a hospital full of civilians. The legal dispute lasted just over a year. At the same time Correa also sued journalists Juan Carlos Zurita and Christian Zurita for the publication of the book El Gran Hermano, which accused Correa of nepotism after his brother Fabricio obtained contracts with the state. In 2012, Correa, through a satellite signal and a chain transmission, and after a long lawsuit, decided to pardon the directors of El Universo, and the journalists.

The following year, pressure on the media and journalists increased, in particular because of two organisations created by the Organic Law of Communication: the Superintendence of Communication (Supercom) and the Council for the Regulation and Development of Information and Communication (Cordicom). These organisations tried to control the press and harassed journalists, accusing them of manipulation or misrepresentation, harming honour and reputation, and following up on requests for rectification and reply. While this was happening, in 2012 the Correa government offered asylum to the activist and founder of Wikileaks, Julian Assange, who took refuge in the Embassy of Ecuador in London. The asylum sought to prevent Assange's extradition to the United States. But, seven years later, in April 2019, new president Lenín Moreno withdrew the offer for allegedly violating international conventions and the "coexistence protocol" (Comunicación Ecuador; Noack and O'Grady).

In the regulatory field, the constitutional amendments of 2015 declared communication a public service, raising concerns about the risks for journalism. Moreover, on the last day of his administration in 2017, Correa introduced a bill to regulate acts of hate and discrimination on social networks and the internet. A weekly Saturday program called "Enlace Ciudadano" (Citizen Link) was one of those affected, even though it had been active throughout the Correa administration. The provocative show included segments such as "la caratucada (scoundrel) of the week" or "freedom of expression belongs to everyone", intended to expose or parody politicians and media alike.

> *Surveillance and persecution of journalists is common in Ecuador, usually organised by the National Intelligence Secretariat (Senain), an entity created by Rafael Correa. Media leaks revealed contracts between Hacking Team (Italy) and Senain, which had as an intermediary a company that monitors social networks: Illuminati Lab (Argentina).*

Surveillance and persecution of journalists is common in Ecuador, usually organised by the National Intelligence Secretariat (Senain), an entity created by Rafael Correa. Media leaks revealed contracts between Hacking Team (Italy) and Senain, which had as an intermediary a company that monitors social networks: Illuminati Lab (Argentina). Hacking Team sold a computer program that was housed in devices (phones, cell phones, tablets) and that spied on the user's activity through malware. With this software, called Galileo DaVinci RCS (Remote Control System), anyone who used Hacking Team's services could have access to all the information (calendar, calls, emails, web pages visited, among others) on the target's devices. After leaks at the end of 2013 and the beginning of 2014, the company maintained that the program was only offered to governments or government agencies to combat organised crime. For its part, at that time, Senain rejected the accusations and never openly addressed the issue, despite media requests.

A Wikileaks leak of 400 GB of information from the Hacking Team in mid-2015 revealed Ecuador was a client. And, despite these documents showing that Senain had contracts with the company between 2013 and 2016, Senain and high-ranking public officials denied these revelations . Former President Correa himself described the leaks as a "political show" and an "an invention of the opponents".

c. Egypt

The 2011 revolution that ended the thirty-year Mubarak regime was quickly undermined by the rise of the Muslim Brotherhood and the coup that removed them from office. Since then, digital authoritarianism has been on the rise. Today, Egypt is one of the world's biggest jailers of journalists. The Sisi administration relies on propaganda and the elimination of critics, and today, the government directly or indirectly controls almost the entire media landscape. Much of Egypt's independent journalism happens online, but the government has blocked 500 websites since 2017, including many news sites. Social media is also heavily policed, and there has been a raft of arrests and detentions, even of influencers perceived as threatening the national image. For instance, three young female influencers

were arrested and charged with human trafficking for their TikTok presence.
The 2018 cyber-crime and media laws made it possible to prosecute and imprison journalists and independent outlets (RSF). These laws enable the national security agencies to access the electronic data of internet and communication platform users without judicial oversight or precise regulation (Freedom House). The legislation also targets social media users as well as accredited journalists. Many people have been arrested for 'spreading false news' under these laws. In a recent report by Freedom House, Egypt scored 18/100 on the freedom scale and was classified as 'not free', going down three points compared to 2020. Indefinite arbitrary detention without trial with accusations of terrorism is common for Facebook posts. The Egyptian state also used the pandemic as an excuse to restrict freedom of expression. The Egyptian security body expelled The Guardian's correspondent in Egypt after the newspaper published a report criticising the government's measurements against COVID-19. Tens of doctors were arrested because they criticised the official narrative around COVID-19 (Malsin and El-Fekki).

> *The report showed that Egypt deployed mass surveillance over the human rights defenders and civil society using a cyber-surveillance system installed by three French companies.*

In 2021, digital rights nonprofit Citizen Lab confirmed that two prominent Egyptian dissidents abroad, Aymen Nour and an unnamed second, had been targeted by Predator spyware. Nour was hacked by Cytrox's Predator and NSO Group's Pegasus spyware. Citizen Lab confirmed Predator has customers in Egypt, and these two different government clients were operating these two pieces of Spyware (Marczak et al.). Both dissidents received links and images containing URLs on WhatsApp, which installed the spyware on their devices. After informing the Meta security team, they later deleted more than 300 Facebook and Instagram accounts linked to Cytrox, which was used in social engineering operations.

In November 2021, leaks from the French media outlet Disclose confirmed that the French ministry of defence, as well as the Elysée were involved alongside Egypt in the extrajudicial killing of civilians in the Western Desert ("Egypt Papers"). The report showed that Egypt deployed mass surveillance over the human rights defenders and civil society using a cyber-surveillance system installed by three French companies. These companies provided Egypt with a powerful search engine called Exalead. This system can link various databases and online activity to the people's identities on behalf of military intelligence. The report also revealed that France sold mass surveillance technologies to Egypt that were used to target and arrest LGBTQ+ people. Hours after publishing the documents, a Disclose journalist announced that their website was totally blocked in Egypt (Lavrilleux). Another piece of French software called Cerebro was sold to Egypt through an Emirati company. This software analyses data to understand the relationships and behaviour of dissidents, including retroactively to find relevant information in billions of recorded conversations ("Surveillance made in France"). The result of all the exported surveillance technology could be seen in the rising imprisonment of the opponents.

These events could explain campaigns of cyber-attacks against civil society and independent human rights defenders. Egyptian security services used phishing websites and emails to pull off such campaigns (Scott-Railton et al.). Amnesty International revealed that Egypt used “Fin spy” in one attack, targeting Windows, Linux and macOS computers and Android devices (Amnesty International). Moreover, since 2017 Egypt has blocked hundreds of websites to crack down on online spaces using Sandvine devices and through deep pocket inception (DPI) technology (Marczak et al.). The state also targets and harasses activists and human rights defenders on social media platforms using bots and fake accounts. Last year, Twitter announced that it had removed thousands of pro-government bots and accounts linked to the government in Egypt (Borger).

The exports of surveillance technology to Egypt enabled security forces to launch an unprecedented campaign against the LGBTQ+ community. The security officers registered themselves under fake identities to trap people on LGBTQ+ apps and social networks. Using the Cortex Vortex software, they geolocated their victims in real-time to arrest them. In 2020, the state targeted women influencers on Tik Tok (Amnesty International). At least three women have been sentenced to between two and 10 years in prison because of public morals violations (Begum). A mother and daughter were fined and charged for publishing scandalous videos, sentenced to six years in jail (“AFTE condemns”). The Egyptian dancer Sama El-Masry was sentenced to three years (the term has since been reduced to two) and fined for publishing videos that violated ‘public morals’ on social media platforms (“Egyptian belly-dancer”).

d. India

India is a sovereign, secular republic and holds elections regularly but is currently experiencing a rapid contraction in democratic space due to the persecution of religious minorities, as well as the silencing of journalists. The Bharatiya Janata Party (BJP), a right-wing party that supports the idea of Hindu nationalism, came to power in a landslide victory in 2014 under Prime Minister Narendra Modi. It was reelected in 2019. Modi has branded himself as a strong leader, taking swift actions on the economy, politics and diplomacy. However civil society organisations, media, the opposition, and scholars are concerned about the increasing intolerance towards minorities, and the dwindling acceptance for dissent in various forms (Gill). There has been an increase in the use of draconian laws, including anti-terror laws (“Parliament proceedings”) and sedition laws to censor dissent (Editors Guild of India). Press freedom is also on the decline. In 2021, India was ranked 142 out of 180 countries on the World Press Freedom Index (RSF), even while the government questioned the methodology used (Chakraborty). Journalists critical of the ruling establishment have faced legal actions, arrests, assaults, and intimidation (Alam; Rights and Risks Analysis group).

The BJP extensively uses social media platforms such as Twitter, Facebook, and Whatsapp to campaign during elections, and Modi remains one of the most followed politicians on Twitter. A year into its tenure, with a vision for digital governance, the government launched the ‘Digital India’ mission. This explains the extensive use of mobile apps, facial recognition, drones, online portals, artificial intelligence, and telecom data during the COVID-19 pandemic. However, this rapid adoption of technology is happening without adequate legislation and oversight. At present, the country does not have a data protection law. The forthcoming Data Protection Bill 2021 gives broad exemptions to the government, limiting checks and balances. In addition, the recently introduced Information Technology (Intermediary guidelines and Digital Media Ethics Code) Rules 2021 allows for increased government control of online spaces and digital news. Civil society members, media and some international organisations have described these rules as a threat to users' freedom of expression online (Xavier).

"The central government's contact tracing app, Aarogya Setu, was criticised during the COVID-19 pandemic after privacy experts highlighted the issues of privacy, surveillance and transparency"

Concerns about the misuse of technology are rife. Although the government denies it, India has allegedly used Pegasus software on high profile journalists, editors, opposition leaders, lawyers, activists, and politicians, many of whom have been critical of the ruling establishment (Varadarajan). The country is building a national automated facial recognition system (Jain) and law enforcement agencies have used FRT to identify and arrest protestors (Singh). Aadhaar, the country's digital ID system, is highly contested. While the government has pushed Aadhaar as an effective governance tool, privacy lawyers and civil society groups caution against the mass surveillance nature of the project, increasing state power and the possibility of exclusion. The central government's contact tracing app, Aarogya Setu, was criticised during the COVID-19 pandemic after privacy experts highlighted the issues of privacy, surveillance and transparency ("Eight organisations").

India is one of the largest markets for social media platforms, used by both politicians and ordinary citizens. However, there is a growing use of internet shutdowns and censorship of voices online. In 2020, India recorded the highest incidents of internet shutdowns globally (Taye et al.). Parts of the contested region of Jammu and Kashmir only regained high-speed internet services after nearly 18 months following countrywide protests over the abrogation of Article 370 by the Central Government ("4G internet"). internet shutdowns were used to clamp down on protestors opposing the Citizenship Amendment Act, a legislation that critics argue discriminates against Muslims and is unconstitutional (SFLC). In addition, the internet in the capital was disrupted during protests against the recently-introduced agricultural reforms (Mitra and Hollingsworth). Social media posts critical of the ruling establishment are also censored. In May 2021, the government directed social media platforms to remove posts critical of its handling of the COVID-19 crisis ("Twitter, FB and others"). In February 2021, the government instructed Twitter to remove 1,178 Twitter accounts concerning the farmers' protests, and threatened legal action for non-compliance (Bhargava).

Fake news, hate speech, and political propaganda are common, and lynching and violence due to fake news shared on social media platforms have occured (Dwoskin and Gowen). Messages inciting violence and polarisation along class and religious lines are widely shared (Bajoria). Politicians also share such content (Chaudhuri; Pandey). In addition, journalists and civil society members point out highly-organised mass trolling by accounts supporting the ruling party and targeting dissenting voices (HRW), women (Kapur), and minorities (Sodhi).

e. Morocco

Morocco is a constitutional monarchy with a multiparty, parliamentary national legislative system under which King Mohammed VI wields absolute de facto power through a combination of substantial formal powers and informal lines of influence in the state and society. The king chairs the Council of Ministers and shares executive authority with the head of government Prime Minister Aziz Akhannouch. The king however chooses the prime minister and proposes other key government appointees. Technically, judicial authority is constitutionally independent of the other two powers, where magistrates are appointed by decree on the proposal of the Superior Council of the Judiciary. However, the latter is presided over by the absolute monarch. Similarly, there are over a dozen political parties, the vast majority of which have always been in line with the palace, whereas the rest are dominated by the two traditional opposition parties, the Istiqlal Party and the Socialist Union of Popular Forces (USFP). Unsurprisingly, the king's executive dominance and de facto legislative ability leave civil rights and liberties in Morocco fragile and endangered at all times.

The wave of protests and political turmoil that swept the Arab world in 2011 ran out of steam in Morocco, although the situation remains tense even ten years after the February 20 protest movement later that year. During the February 20 movement, thousands of Moroccans, including representatives of political parties, human rights activists and journalists, organised on Facebook and gathered in 53 cities and towns across Morocco calling for reform of the country's political system, an end to corruption and social inequality, and a new constitution (Amouzai). In March, the king gave a televised speech in which he promised a "comprehensive constitutional review" as an enhancement of the 'democratic development model' ("Morocco's King Mohammed"). However the government's response to the protests was inconsistent, and featured increased violence against protestors. Protesters were allowed to demonstrate in the streets prior to the king's speech, but only a few days after his promise of change, police and security forces brutally cracked down on protestors in Casablanca, Rabat, and elsewhere (ElHachimi). Dozens of peaceful protestors were reportedly beaten, hundreds were injured and physically assaulted, and at least one activist, Kamal Ammari in Safi, died for participating in the February 20 movement (HRW).

In October 2016, demonstrations by the Hirak El-Rif movement began in and around Al Hoceïma city, after Mouhcine Fikri, a fishmonger, was crushed to death by a garbage collection truck while trying to recover his goods confiscated by the local authorities. The protesters demanded an end to the marginalisation of their communities through greater social justice. Between May and August 2017, Moroccan security forces arrested hundreds of protesters from the Hirak movement, including peaceful protesters Nasser Zefzafi and El Mortada Iamrachen (HRW; Amnesty). Authorities, alongside pro-government-aligned media, launched a public smear campaign to discredit the Hirak movement, calling them "traitors", "corrupt", or "terrorists" in order to deter protests. One of the major female leaders of the Hirak movement, Nawal Benaissa, was prosecuted over comments on Facebook encouraging residents of Al Hoceima to join protests. As soon as she joined the movement, hundreds of fake stories circulated on local media delving into her personal life. She was also accused of receiving funds from foreign countries to spread violence and destabilise the region ("Nawal Benaissa in selling matches storm").

Hundreds of protesters, journalists and human rights defenders were later convicted by the Al Hoceima court in trials, described by human rights organisations as unfair trials that "fall far short of international fair trial standards" (Amnesty International).

Broadcast media and key media outlets in Morocco, including radio stations, television channels and press agencies, are mostly dominated by the state and reflect the official line. However, the private press has succeeded in breaking taboos over some sensitive topics, including allegations of high-level corruption (Said). There are currently nine public TV channels run by the state, as well as 34 radio stations and 618 newspapers, including privately owned, party-affiliated, and government-controlled newspapers. The government also owns the official press agency, the Maghreb Arab Presse, the National Society of Radio and Television (SNRT), and the Arabic daily Al-Anbaa.

Media in Morocco face considerable restrictions through laws, such as:

- The Press Code of 2002 shifts the authority to prosecute journalists suspected of insulting the royal family from the executive to the courts. Judges appointed by the king, however, preside over instances involving the king's defamation.

- In 2016, Morocco adopted a new Press and Publications Code, replacing the 2002 Press Code, which compels the government to provide reasons for the confiscation of media — making it easier to launch publications. However, the law was heavily criticised by human rights organisations and the Moroccan Press Union for not completely abolishing penal sanctions, particularly for publications deemed threatening to public order. Indeed, the government retains broad powers under the revised law, including the authority to censor news content, suspend critical media outlets, and pursue fines and prison sentences against journalists.

- Although Morocco's 2011 constitution guarantees freedom of the press and prohibits prior censorship, its ambiguous language leaves the door wide open for interpretation and impedes enforcement of media protections.

- Moroccan authorities continue to suppress critical speech by wrongfully charging journalists and human rights activists and imposing draconian prison sentences under the Penal Code for a variety of broadly-defined offences linked to non-violent speech. Offences include disrespecting the king, offending state institutions, and insulting public servants while performing their duties (Amnesty International).

In recent years, the Moroccan authorities have silenced critical voices through judicial harassment, indefinitely detention and tenuous accusations, including sex crimes charges (Amnesty International). (Under Morocco's conservative criminal code, sex outside of marriage is illegal.) Journalists cannot report freely in certain areas, especially Western Sahara, where media blackouts and crackdowns on peaceful protests continue. According to Reporters Without Borders (RSF), Morocco ranked 133th out of 180 countries in its 2020 index. RSF repeatedly denounced the judicial harassment of independent journalists and harsh prison sentences based on false allegations.

During the global COVID-19 pandemic, the government introduced the "anti-fake news" bill or Law 20-22, which aims to penalise the dissemination of false information on social media networks or open broadcast networks with up to two years of imprisonment and a fine of 5,000 Moroccan dirhams (approximately USD 500). Human rights NGOs and some MPs criticised the government's proposal, calling for the law to be revoked immediately and warning that such vague terms can be used to muzzle journalists and human rights activists who criticise the government. At least a dozen people were arrested on charges of spreading fake news related to the coronavirus pandemic by mid-March, including individuals who criticised the government's response to the coronavirus. While the review of the law had been postponed following mass criticism by civil society and human rights organisations, these measures showcased how the Moroccan government had taken advantage of the COVID-19 outbreak to pass laws curtailing civil liberties ("Morocco: Government").

> *While Morocco categorically denied acquiring the Pegasus spyware and rejected allegations that its intelligence agencies and security forces had used it for surveillance, the consortium alleges that the monarch may have authorised the targeting of his own mobile phone to ensure his safety.*

During the COVID-19 pandemic, state control over the media in Morocco has intensified, with the country now witnessing the prosecution of bloggers, spying on journalists' personal communications, as well as restrictions on information access and free expression (Freedom House). Digital surveillance enables the government to extend its authoritarian reach by silencing the voices of dissent, independent media, and opposition figures. This comes with rising fears that digital surveillance will be sustained beyond the end of the COVID-19 health crisis.

The Moroccan government also uses biometric systems including facial recognition technology, a digital identity programme, and a contact tracing app to control the spread of COVID-19. While data-driven technologies can undoubtedly be put to highly beneficial uses, these technological developments carry very significant risks for human dignity, ethics and privacy and the exercise of human rights in general if they are not managed adequately. Although Morocco has a data protection regulation in place (Data Protection Law No. 09-08), the law does not provide adequate protection for people's personal information and allows authorities to process their data without any prior consent under the guise of "protecting the public interest".

In recent years, there have been increasing reports of journalists, political activists, and human rights defenders being unlawfully subjected to surveillance, detained, prosecuted on politically-motivated charges, tortured and ill-treated. According to recent leaks, many Moroccan journalists were wiretapped by the Pegasus spyware built by Israeli technology company, NSO, and are now in jail in Morocco facing charges of rape and sexual assault. Among them, Omar Radi, who was investigating land expropriation and who for years documented human rights abuses; the editor-in-chief of the Arabic-language daily Akhbar Al-Youm, Suleiman Raissouni, who writes frequent editorials critical of the authorities, and his niece Hajjar Raissouni, who is also a well-known journalist for the same newspaper.

Prominent Sahrawi activist Aminatou Haidar, who won multiple awards for her peace activism and human rights work, has also been unlawfully targeted by Pegasus spyware and is now facing a new form of insidious digital attack (Amnesty International). These are only a few of the Moroccan journalists and Western Sahara human rights defenders whose numbers appeared in the NSO's registry of phone numbers targeted by the company's clients (Rueckert and Schilis-Gallego). According to the Project Pegasus consortium, which exposed the spyware scandal, several members of Morocco's royal family were targeted by the Pegasus spyware, including Mohammed VI. While Morocco categorically denied acquiring the Pegasus spyware and rejected allegations that its intelligence agencies and security forces had used it for surveillance, the consortium alleges that the monarch may have authorised the targeting of his own mobile phone to ensure his safety. Morocco has also threatened legal action against anyone accusing it of deploying the NSO's spyware, and denounced what it called a "false, massive, malicious media campaign "(Bachir).

f. Myanmar

Myanmar was a pariah state while under the rule of an oppressive military junta from 1962 to 2011 ("Myanmar country profile"). Democratisation in 2011 led to multi-party democratic elections in 2015 that were a turning point for Myanmar. Led by a civilian government, the country's poverty rate fell from 48% to 25% between 2005 and 2017 (World Bank). It particularly dipped between 2015 and 2020, during the first term of cabinet for the de-facto leader, Aung San Suu Kyi. However, the optimism was destroyed by a military coup on February 1 2021, right after Aung San Suu Kyi's National League for Democracy (NLD) won the 2020 election by a landslide. Before starting their second term, most of the leaders of NLD, including the President U Win Myint and the State Counsellor Aung San Suu Kyi were detained by the military ("Myanmar: what has been happening").

The military declared a state of emergency and Min Aung Hlaing, the military chief, took power of state initially for a year, but later extended it indefinitely. The public rejected the coup with massive protests that saw millions of people taking to the streets. The opposition forces formed the "Civil Disobedience Movement (CDM)", where civil servants refused to go to their offices in order to weaken the bureaucratic mechanism of the military. A group of elected lawmakers and parliament members formed a parallel government in exile called the "National Unity Government (NUG)". The public in every corner of the country formed local militias under the name of the "People's Defence Forces (PDF)" to fight against the military forces.

Following the coup, the military killed and arrested hundreds of protesters, local resistance forces, human rights activists, journalists, politicians and students. According to the Assistance Association for Political Prisoners (Burma), the junta sentenced or arrested 9,206 citizens, charged 1,973 with a warrant, and killed 1,557 people as of February 18, 2022 (AAPP). The military also committed what the United Nations called a "textbook example of ethnic cleansing" on Rohingya people in 2017, and continued to employ massacres and burnings against other ethnic groups. In December, 2021, the military burned 11 civilians alive in Kayah State ("Eleven villagers"). About 600 of the town's 2,000 buildings were burned down in Thantlang, Chin State (Kelly et al.). The country is now in a state of civil war, resisting the terrorist military.

After the coup, the military is employing every possible digital repression tactic to limit freedom of expression, freedom of association and access to information to weaken digitally-mobilised resistance forces' activities and reporting of atrocities. These range from internet shutdowns, dual-use surveillance technologies, AI-powered CCTV systems to Chinese-assisted UAVs (Beech). Similarly, surveillance and censorship have been present in Myanmar's digital spaces since it opened the internet to the public in the early 2000s. In 2007, after the Saffron Revolution, publicly accessible internet was restricted through internet shutdowns, website censorship and hacking. Prior to the coup in February 2021, the NLD-led government imposed a 20 month-long internet shutdown in Rakhine and Chin. This was one of the world's longest internet shutdowns (HRW). The ministry of transport and telecommunication also announced a budget of 6 million USD to set up a social media monitoring team to monitor the usage of social media in Myanmar (OTF).

Beginning in 2021, the military-formed State Administration Council (SAC) has tried to enact the Cybersecurity Bill which is full of punitive clauses, as well as to amend the country's Privacy Law, Electronic Transaction Law, and Broadcasting Law, to legally oppress the digital space (HRW). A group of military-backed cronies are also trying to acquire Telenor Myanmar, an operator who sought to sell its local business because of military pressure to install surveillance equipment on its clients ("Junta cronies"). On the ground, digital security has become a survival skill. Military checkpoints involve phone searches. If the military find something offensive, one might be subjected to torture, arrest, harrassment or even extrajudicial execution. When it comes to mainstream social media, Facebook, Twitter and Instagram are banned (Nachemson). Using VPNs is criminalised with a sentence of three years imprisonment, according to the newly-drafted cybersecurity law (Chau and Oo). Telegram is now mainstream and public mobilisation on the internet mainly goes through apps like Telegram and Signal.

> *"Prior to the coup in February 2021, the NLD-led government imposed a 20 month-long internet shutdown in Rakhine and Chin. This was one of the world's longest internet shutdowns (HRW)."*

g. Russia

The internet in Russia has been shaped by the state's Soviet legacy as well as its aspirations to remain a global superpower. Following the fall of the USSR, there has been an increase in state control over citizens, and a contraction of human rights and civil liberties. Vladimir Putin was sworn in as president at the start of the 2000s, and his reign has been virtually uninterrupted since then, characterised by tightening state control over all spheres of life, exclusion of opposition actors from mainstream politics, and the emergence of a system dominated by his ruling United Russia party in what some scholars refer to as managed democracy (Lipman et al. 116) and others a consolidated authoritarian regime (Freedom House).

State security in Russia has always taken precedence over individual freedoms and rights of citizens. In the Soviet era, centralised state control over citizens' communications was achieved through censorship of mainstream media, foreign publications, and literary works; restrictions on ownership and use of technology such as photocopiers (Hansen) and through pervasive wiretapping and surveillance of citizen communications (Soldatov). Even so, Russian media were instrumental in the dissolution of the USSR (Oates) and remained influential in the Russian public sphere in the 1990s and 2000s, even though establishing control over the media sphere was a matter of national security.

The Putin regime is arguably one of networked authoritarianism (Mackinnon) as the state now aspires to control all spheres of mediated social life while still placing a high value on developing networked infrastructure and connectivity. Mainstream media is largely run or co-opted by the state, but until recently, the internet has remained a relatively free though contested space for alternative opinions and dissent (Oates). Technically, the Russian constitution guarantees freedom of speech and press freedom, but the politicised judicial system is routinely used to harass independent journalists and civil society activists. Dissenting internet users contend with an increasingly sophisticated state surveillance apparatus (Gunitsky). Russian law also contains a broad definition of extremism that officials use to silence critics of the government, including journalists and protesters. Enforcing this and other restrictive legal measures encourages self-censorship among media professionals and ordinary internet users.

In 2000, when Putin became president only two percent of the Russian population had internet access. By 2010, this had increased to 43% (ITU). By the start of the 2010s, some information networks retained their freedom, yet key political structures such as the ruling party were focused on retaining long-term control and self-enrichment, while social movements and civic activity were thin on the ground. Though there was comparative media diversity, the media system overall was not free, with a large proportion of national mainstream media channels owned or co-opted by the state. New independent media were aided by the proliferation of the internet (known colloquially in Russia as the RuNet).

Russian authorities have employed an evolving system of what Deibert et al. (2010) refer to as "information controls": techniques, practices and regulations that circumscribe the kinds of information technology, media channels and electronic communications available to citizens (Deibert et al.). This ecosystem works at many levels and may include technical means such as "filtering, distributed denial of service attacks, electronic surveillance, malware, or other computer-based means of denying, shaping, and monitoring information", as well as more opaque measures such as "laws, social understandings of 'inappropriate' content, media licensing, content removal, defamation policies, slander laws, secretive sharing of data between public and private bodies, or strategic lawsuit actions" (Citizen Lab). Meanwhile, independent media and opposition actors rely on digital platforms and networked media to spread alternative narratives about infighting, corruption, and human rights violations among Russian officials.

Since the massive protests against electoral fraud in 2011-2012, to which the internet and social media were crucial, the Kremlin has gone to considerable lengths to control the digital space and centralise internet governance, media censorship, and content regulation. Roskomnadzor, the regulatory body overseeing the internet, media, and telecommunications, is now enforcing more rules and restrictions. There are a host of new laws limiting foreign ownership of media and policing online speech, as well as recent legislation to secure greater control over national internet infrastructure. Criminal defamation was reintroduced in

2012, with large fines or weeks of forced labour as punishment. Another restrictive law from 2012 granted unprecedented blocking powers to Roskomnadzor and other state bodies (Rothrock). Yet another 2012 federal law mandated the creation of a "blacklist" registry of websites that disseminated allegedly illegal or otherwise harmful material. "Foreign agent" laws impose high penalties on newsrooms and journalists for violating highly bureaucratic regulations and set limits on the share of foreign ownership and amount of foreign funding in media companies (Wijermars et al. 1). A new "fake news" law passed during Russia's war of aggression on Ukraine in February 2022 introduced criminal liability for media reporting on the war that is not in line with the state narrative. A number of Russian independent media outlets are now working in exile, while others have shut down.

Internet penetration continues to grow dramatically — up from 43% in 2010 to 85% in 2020 (ITU). An infamous "bloggers' law" required popular bloggers with over 3,000 daily views to register with the state and disclose their personal information; a law creating a state-run list of "organisers of information distribution" requires social networks, portals, and similar sites to register and share certain data with the state; other measures limit the anonymous use of public Wi-Fi networks and ban sales of prepaid SIM-cards to customers without state IDs.

With regards to censorship and surveillance, measures include a data localisation law that came into force in 2016 and requires internet companies to store Russian users' data on servers located within Russia. Although some companies (e.g., eBay, Booking.com and Samsung) have complied with the demands, others (such as Facebook and Twitter) have yet to do so and have been fined or threatened with blocking. The professional social network LinkedIn has been blocked in Russia since 2016 for failing to comply with the legal requirements.

An "anti-extremism" package of amendments was adopted in the summer of 2016 and took effect in 2018. This includes measures such as increased sentences for the use online of "extremist" language (a designation that state authorities can apply with great discretion), a push for internet companies to share encryption keys with the state and to decrypt user communications, and requirements to store user communications for six months and metadata for up to three years. In 2018, Russian censors used these legal grounds to block Telegram after it refused to share encryption keys with law enforcement. The attempt proved mostly unsuccessful due to Telegram's sophisticated circumvention efforts and the state's clumsy blocking approach; the ban was ultimately lifted in 2020.

Social media content is regularly deleted or blocked on grounds of intolerance or disrespect toward government officials, and users have been fined and even jailed for posting, sharing, or liking content deemed to contain extremist language, calls to mass disorder, or unverified information about public figures.

"A new "fake news" law passed during Russia's war of aggression on Ukraine in February 2022 introduced criminal liability for media reporting on the war that is not in line with the state narrative. A number of Russian independent media outlets are now working in exile, while others have shut down."

Data from Russia's Supreme Court shows that convictions under the charge of extremism more than tripled between 2012 and 2017; a large number of these have involved online activity (Gainutdinov). In 2019, the Kremlin began implementing a comprehensive "sovereign internet" strategy. A set of new regulations and technical upgrades aimed at more autonomy and state control over internet infrastructure, the "sovereign internet" was presented as a means of protecting Russian cyberspace from external threats (Epifanova). So far, however, it has mostly been used to consolidate control over information flows within Russia's borders, imposing new centrally controlled and less transparent website blocking mechanisms and targeting opposition websites and social media platforms (Lipman and Lokot). During Russia's invasion of Ukraine in February 2022, state censors blocked access to Facebook and many independent online media (Russian and Ukrainian ones), with Twitter and YouTube facing a similar fate and being throttled.

"In 2012, the Sudanese General Intelligence Service (GIS) bought a cyber-weapon called Remote Control System from the "Hacking Team," an Italian company. This system enables government surveillance of a target's encrypted internet communications, even when the target is connected to a network that the government cannot wiretap ..."

h. Sudan

After a revolution in 2019, Sudan has been in a state of constant political upheaval, culminating in the resignation of Abdullah Hamdok, leader of the transitional authority. The National Intelligence and Security Service (NISS) spearheaded the Bashir regime's censorship, arresting journalists, shutting down newspapers, confiscating entire issues as they came off the press, and imposing red lines that could not be crossed with impunity. According to RSF's information, the Cyber Jihadist Unit, which was created to for internet surveillance and to monitor journalists' activities online, continues to operate and to spread false information on social media with the aim of undermining the transitional government and protecting the interests of certain old regime figures who still control most of the media (RSF).

While there was hope for a democratic system after the revolution in 2019, a counter-coup on October 25, 2021 put the military back in power. Lt. Gen Burhan led a military coup against his partners in the transitional government which came after the Sudan uprising (Hamad). Since the coup, Sudanese people have protested daily, rejecting any military action against democratic transition. The UN, the Troika (Norway, UK and the US), the European Union (EU) and African Union (AU) condemned the coup and the state's violation of protestors' rights ("Sudan's military fires"). The UN, represented in its mission in Sudan to assist the democratic transition (UNITAMS), introduced an initiative to solve the "crisis" — as it described — and many members of Sudanese society are involved in discussions and negotiations to save the country from collapse ("UNITAMS releases").

In the last decade, digital authoritarianism has been on the rise in Sudan. In 2012, the Sudanese General Intelligence Service (GIS) bought a cyber-weapon called Remote Control System from the "Hacking Team," an Italian company. This system enables government surveillance of a target's encrypted internet communications, even when the target is connected to a network that the government cannot wiretap (Marczak et al.). Sudan also bought a surveillance system from Blue Coat, a Canadian company that enables monitoring and filtering of web content (Nakashima).

Similarly, while Sudan has ratified key international human rights instruments which guarantee the right to freedom of assembly and freedom of expression, according to Freedom House's 2021 report on Sudan, the country only scores 17/100 and is "not free" (Freedom House). Sudan has a poor press freedom record, being among the worst countries on the World Press Freedom Index where it is ranked 159th out of 180 countries (RSF). Despite the success of the revolution in ousting the Islamist regime of Al-Bashir in 2019, civic space remains restricted. For example, the transitional government represented in the Press and Publications council suspended two newspapers, Al-Intibaha and Al-Saihah, in September 2021 using the same law that was issued by the Al-Bashir regime ("The Press and Publications Council").

The military regime depends on the "Constitutional Declaration of 2019" to advance their authoritarian agenda of restricting freedom of speech. This document forms the legal basis for Sudan's polity during the transitional period that started in 2019. Article (57) of the document guarantees the right of freedom of expression of the citizens (Constitute Project). In spite of this guarantee, security forces routinely restrict freedom of expression by using teargas and live bullets against protestors. Since 2018, the military has also implemented various restrictions to internet access, including internet shutdowns, blocking websites and calls, and SMS shutdowns ("internet blackout"). The internet has been shut down more than five times during the last four years (Hamad et al.). Sudanese feeds on social media platforms such as Twitter and Facebook are also filled with fake accounts or real accounts that influence public opinion and work to measure people's feedback. In June 2021, Facebook reported that it was removing 53 accounts, 51 pages, three groups, and 18 Instagram accounts in Sudan that targeted domestic audiences and were linked to a political party that led a campaign against secularism, feminism, and the transitional government (Facebook).

i. Tanzania

Tanzania is an East African country with a population of approximately 60 million (Kemp). From independence in 1961 as the Union of Tanganyika and Zanzibar to the present it has been under the rule of the CCM (Chama cha Mapinduzi) party. The last elections in 2020 saw then-president Magufuli win with 84.4% of the votes, followed by opposition leader Tundu Lissu at 13% (National Bureau of Statistics). President Magufuli ran a strict authoritarian government that arguably fought corruption while restricting the rule of law, and passing legislation that constricted human rights both offline and online. Tanzania's civic space transformed dramatically under Magufuli, particularly its digital ecosystem. Law and policy changes constrained digital expression, and punitive licensing and taxation measures targeted online expression. There was also an internet shutdown during the 2020 elections. Social justice organisations have been greatly affected by new laws that limited their freedom to operate and fulfil their role in their communities.

> *Tanzania is also a client for the Hacking Team's Remote Control System (RCS) which allows governments to intrude in communications systems across mobile networks.*

Article 18 of the Constitution guarantees every person the right to freedom of expression and the right to seek, receive, and impart information. However, various laws limit this freedom. In 2020, Tanzania passed the Electronic and Postal Communications (Online Content) Regulations that affect anyone who uses digital media to express themselves and access information. During the COVID-19 pandemic, laws like the Online Content Legislation were used to silence people from discussing the pandemic.

After his death in 2020, Magufuli was replaced by President Samia Suluhu Hassan. On April 6 2021, the new president lifted bans and restrictions on media outlets that had been shut down. However, with laws remaining unchanged, outlets may still fall prey to repressive actions. In September 2021, Tanzania suspended Raia Mwema, a leading Swahili press outlet, for "repeatedly publishing false information and deliberate incitement." It was the second newspaper to be suspended during Samia's reign. First was the newspaper Uhuru, after it published a story claiming Samia would not run for office in 2025. Journalist Azory Gwanda, a fierce critic of the Magufuli regime, remains missing and unaccounted for.

The internet also remains vulnerable. In August 2021, Tanzania published the proposed Electronic and Postal Communications (Online Content) (Amendment) Regulations 2021 (EPOCA amendment regulations), adding to existing restrictions. These new amendments target the right to privacy, requiring content creators to share a lot of personal information to get services and be registered. Currently, Tanzania has no data protection and privacy policy and there are more restrictive laws like the Cybercrime Act than there are protective measures and regulations.

Tanzania is also a client for the Hacking Team's Remote Control System (RCS) which allows governments to intrude in communications systems across mobile networks. In 2015, the country also cloned the Jamii Forums website, a forum for civic engagement, in an effort to monitor conversations on the platform (CIPESA). The Electronics and Postal Communication (SIM card regulations) Act of 2020 was published on February 7 2020, making it mandatory for all SIM card users in Tanzania to register their cards biometrically. To do so, one must have a national identification number (NIN) and ID, even though there is no law governing data protection and privacy. This regulation also requires individuals to provide personal data accessible by public agencies such as telecoms companies. Tanzania does not recognise a right to anonymity.

During Tanzania's 2020 election, major social networks were blocked across the country on the eve of the election, with users relying on virtual private networks (VPNs) to send messages and to access information (Sakpa). At the same time, opposition leaders were criticised for being vocal on social media. Civil society, human rights defenders and activists have pushed back against oppression, both online and offline. In 2021, Universal Periodic Review (UPR) process recommendations were submitted to Tanzania covering attacks on the political opposition, press freedom and freedom of expression, and the rights of sexual and gender minorities, women, girls, refugees, children, and people with disabilities.

Tanzania has supported recommendations to investigate attacks against journalists and to address concerns on interference with freedom of expression (HRW).

j. Turkey

Since the Justice and Development Party came to power in 2002 under the leadership of the strongman Recep Tayyip Erdogan, the independent and critical media environment, as well as overall freedoms in Turkey, have been on the decline. The crisis of basic freedoms in the country is compounded by increasing digital censorship (IPI). The infamous law No. 5651 (also known as the Internet Law), adopted in 2007 and amended in 2014, 2015, and 2020, enables the authorities to block access to various websites, individual URLs, Twitter accounts, tweets, YouTube videos, and Facebook content (Akdeniz).

Signs of control were already visible in 2006 when the ruling government of AKP made amendments to the Terrorism Law, enabling an environment of persecution for sharing content online and legalised the use of "personal data and communications to pursue criminal investigations and persecute suspects when the alleged crimes were related to terrorism or sympathy for terrorism" (Celik 102). The following year, the authorities began deploying "increasingly authoritarian measures to control and manage online communication and confine the networked public sphere" (Celik 102), including internet filtering and blocking, legal restrictions, content removal directives, and blocking of websites, to name a few. By 2008, hundreds of journalists, military personnel, dissidents, civil rights activists, and those affiliated with the Kurdish rights-based movements were put on trial based on the evidence collected through wire-tapping and/or digital surveillance (Celik 102). The law is still a popular tool to sentence journalists and government critics. According to an International Press Institute report, out of 241 journalists on trial in Turkey in 2022, at least half were facing terrorism charges (IPI).

The year 2013 marked another milestone in digital censorship. On the heels of the protests in Gezi Square, the notorious internet Law was amended in 2014 allowing "the state to block what it regarded as troublesome URLs and to keep records of internet traffic for up to 2 years" (EDRi). The decision came as the ruling party was mired in a corruption scandal in what appeared to be leaks of audio recordings of the then Prime Minister Erdogan, his family members, high ranking ruling party officials and businessmen affiliated with the ruling government.

The authorities also amended the Law on State Intelligence Services and the National Intelligence Agency (Yaman). Dated April 2014, the approved amendments granted "the National Intelligence Agency (MIT) the ability to use any technical and human intelligence means necessary to collect, record, analyse and share information, documents, news and data pertaining to foreign intelligence, national security, counterterrorism, international criminal acts, and cyber security "(Ergun).

During these years, as it became evident in reports released in the following years, Turkey also became a popular client of pervasive digital surveillance technology. The country was listed among the clients of the Hacking Team and its Remote Control System was reportedly in use at least between 2011 and 2014 (Marczak et al.).

There is also evidence of Pegasus (Marczak et al.) and Candiru spyware (Marczak et al.), network injection (Kenyon), and DPI technology (Marczak et al.) deployed in Turkey over the years.

Erdogan further consolidated his powers following the failed coup in 2016, granting his government, under emergency rule, broad powers to silence any perceived opponents. Following the attempted coup, some 100 media outlets were shut down (Weise), tens of thousands of citizens were arrested, and nearly 150,000 civil servants, military personnel, and others were sacked or suspended ("Turkey orders"). The wide-ranging crackdown has also expanded beyond the country's borders (Freedom House).

Under the state of emergency, the Decree Laws 670, 671, and 680 allowed for interception of all digital communication of individuals whom Turkish authorities alleged were either involved or believed to have been involved in the coup. The interception extended to the family members of said individuals. The laws authorised "Turkey's Information and Communication Technologies Authority (Bilgi Teknolojileri ve İletişim Kurumu, BTK) to take over any service telecommunication providers" perceived as a threat to national security, health and what is vaguely defined as morals of the public; as well as allowing "the State Cyber Crimes Division to intercept any internet data traffic without a court order or supervision" (Unver). Six years on, authorities in Turkey continue to jail prominent activists, journalists, politicians, and other representatives of civil society relying on various national laws while having taken almost entire control of the existing media landscape (Sari).

Constitutional changes that were voted on in a country-wide referendum in 2017, replacing the existing structure from parliamentary government to a presidential one, and the subsequent election of Erdogan as the nation's president in 2018, have only deepened the powers of the ruling government to systematically silence dissent in the country. In 2019, Turkey's Radio and Television High Council (RTÜK) was granted (Uğurtaş) expanded powers to monitor online broadcasting (ranging from on-demand platforms such as Netflix, to regular and/or scheduled online broadcasts to amateur home video makers), compelling online broadcasters to obtain a licence from RTUK (IPP). On February 9, 2022, the government body gave the Turkish language websites of VOA, Deutsche Welle, and Euronews 72 hours to apply for a publication licence ("US urges Turkey"). As a result, Turkey ranks "not free" in Freedom House, Freedom in the World, and Freedom on the Net reports (Freedom House).

Several pieces of key legislation have been passed to enable the control of digital spaces in Turkey. Law No. 5651 aka the Internet Law, was enacted in 2007. Initially introduced as a safeguard mechanism for protecting children, it soon became evident the law was a tool to censor content online. The law was first used in 2008 to block access to YouTube, which remained blocked until 2010. The first set of amendments to the law that were introduced in 2014 and 2015 widened its scope, enabling "the criminal judgeships of peace to block access to internet content involving personal rights violations, privacy violations as well as content deemed to breach national security and public order". The law was later used to once again block access to YouTube, but also Twitter, and Wikipedia. "The widespread use of the Law No. 5651 measures as well as some additional legal measures resulted in access to 408,494 websites, 130,000 individual URL addresses, 7,000 Twitter accounts, 40,000 tweets, 10,000 YouTube videos, and 6,200 pieces of Facebook content being blocked from Turkey by the end of 2019"(Yaman).

In July 2020, the Turkish parliament ratified the Social Media Law (Law on the Regulation of Publications on The internet and Suppression of Crimes Committed By Means of Such Publications), which went into effect on October 1, 2020 (Geybullayeva). The law requires all social media companies to register with the authorities, as well as to follow content removal requests within 48 hours; it has troubling localisation provisions (Freedom House). The law was back on the agenda in 2021 as Turkey's internet legislation called for sites with more than a million daily users to appoint local representatives, announcing hefty fines and imposing ad bans for those failing to comply with new regulations (Geybullayeva).

In August 2021, the ruling party announced plans to set up a regulatory body to monitor social media for what president Erdogan described as the "terror of lies," as well as introduce a new law that would hold distributors of "misinformation" and "disinformation" accountable with a possible prison sentence for a maximum of five years ("Report: Turkey"). The decision came following a summer of wildfires that wreaked havoc across Turkish coasts. Citizens took to social media to criticise the authorities for their lack of swift measures in fighting the wild fires (Celik and Geybullayeva).

A commonly used accusation levelled against critics of the ruling government as well as the president is "insults". But it isn't only used in charges against the president. In February of this year, four journalists were accused of "insulting" the president's son, Bilal Erdogan, with a prosecutor seeking prison sentences of up to four years for the journalists ("Turkish prosecutors"). Insulting the president is a crime according to Article 299 of the Penal Code with a maximum prison sentence of four years. Since the former prime minister Erdogan took over the presidential seat in 2014, the convictions based on article 299 have skyrocketed. Sedaf Kabas is the most recent case, as was another citizen who was charged under the article for the citizen's enthusiasm expressed online after hearing the news that President Erdogan and his spouse Emine Erdogan had contracted Covid ("Turkey: prominent journalist"). Another recent case involves a former Olympic swimmer who jokingly tweeted about the Erdogan family's infection. The swimmer was suspended from the Swimming Federation of Turkey after the tweet. "According to the Turkish ministry of justice, more than 31,000 investigations into alleged insults against the president were opened in 2020 alone. Since Erdogan became president in 2014, that figure has totaled 160,000. Nearly 39,000 people have stood trial for the alleged crimes," reported DW on February 12, 2022 ("Turkey marshals law").

> *In August 2021, the ruling party announced plans to set up a regulatory body to monitor social media for what president Erdogan described as the "terror of lies," as well as introduce a new law that would hold distributors of "misinformation" and "disinformation" accountable with a possible prison sentence for a maximum of five years*

In October 2021, the European Court of Human Rights condemned the law saying that it did not comply with the spirit of the European convention ("European court"). Other recent examples include RTUK (Radio and Television Supreme Council) announcing a probe against a Fox TV anchor on the grounds of violating the principle of impartiality ("Turkey's media watchdog"). Also in January, President Erdoğan threatened Turkish media with reprisals if they disseminated content that damaged the country's core values, in a move that might be a prelude to further censorship in the sector ("Erdoğan threatens").

k. Zimbabwe

Zimbabwe gained independence in 1980, with a legal system based on Roman-Dutch law. The late strongman Robert Mugabe ruled the country from independence to his eventual deposition in a 2017 coup, in what was effectively the first and so far only political transition. Unfortunately, under President Emmerson Mnangagwa, authoritarian governance continues with increasingly violent repression of dissenting voices on digital platforms. Mnangagwa was one of Mugabe's most powerful ministers who held - at various times - the defence, justice and state security portfolios. His administration regularly enters into transnational deals with Russian, Chinese and East European actors, including to sign cyber-related contracts, which are covered in a deep veil of secrecy.

Networked authoritarianism explains the survival of Zimbabwe's repressive digital regime. A digital expert (Gwagwa) argues that Zimbabwe has increasingly used national security and criminal legislation as a means to gain powers to keep citizens under surveillance, and to infringe upon their privacy rights. For instance, the Data Protection Act (Chapter 10:11) gazetted on December 3, 2021 (MISA Zimbabwe) amends three laws, namely the Interception of Communications Act, the Criminal Procedure and Evidence Act, and the Criminal law (Codification and Reform Act). The Data Protection Act also regulates the collection, storage and transmission of data with the stated objective of dealing with cybercrimes. However, critics argue that this law stifles the work of civil society and journalists in violation of section 61 of the Constitution that provides for freedom of expression and freedom of the media. Under this law, publishing false data attracts a five-year prison term. Additionally, this law provides for a Cyber Security Centre housed in the Office of the President, which is authorised to issue interception of communications warrants. The law is also unclear on internet shutdowns.

Zimbabwe is signatory to Article 9 of the African Charter on Human and Peoples' Rights which guarantees freedom of expression. The country is also signatory to Article 12 of the 1945 Universal Declaration of Human Rights and Article 17 of the 1966 International Covenant on Civil and Political Rights (UN OHCHR) The International Covenant on Civil and Political Rights states that no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. However, the government remains in violation of pre-trial and fair trial rights, with regard to free speech, opinion and press enshrined by local and international law.

Even so, press freedom is poor in Zimbabwe as harassment and intimidation of journalists continue unabated. Persecutions related to free expression, especially after the 2017 military coup, continue. A pattern of repressive autocracy poses an existential threat to the future of free discourse on social media and open internet in Zimbabwe. For example, while conferring ranks to newly promoted Airforce of Zimbabwe officers on January 7, 2022, Air Marshal Elson Moyo declared social media and matters related to cybersecurity as "enemies of the state" (Mabika). Similarly, the controversial Data Protection Act contains an ambiguous definition of "false data" that critics argue might lead to the persecution of journalists.

Meanwhile, journalists continue to face threats for their work and the law remains a potent tool for effecting those threats. Jeffery Moyo, a freelance journalist affiliated with the New York Times, was arrested on May 26, 2021 on charges of violating section 36 of the Immigration Act based on flimsy media accreditation status charges against two American journalists. He was eventually released after three weeks but concerns about press intimidation are rife as the state intends to resuscitate the case.

Zimbabwe is one of the flagship countries for technology partnerships and transfers with China, particularly the Smart Cities Projects. In September 2021 the government signed an agreement with Chinese mobile giant Huawei to roll out mobile broadband in Zimbabwe (Privacy International). Smart city initiatives are designed to consolidate data collection activities across participating states, with the nominal goal of improving service delivery. However, in authoritarian countries like Zimbabwe, Smart City initiatives are directly linked to increased surveillance of state critics, as well as misappropriation of public funds on projects with marginal returns. In a deal between the Government and CloudWalk Technology, Zimbabwe is also currently running a biometric pilot project to train Chinese Artificial Intelligence algorithms to recognise faces with darker skin tones (Dzoma).

Chinese company Huawei won network upgrade contracts with NetOne, which is a state-owned Mobile Network Operator (MNO). As the country's second largest MNO, NetOne has rolled out mobile telecommunications equipment nationwide, supplied by Huawei over the years. At the end of 2017, Net-One secured a USD 71 million financing agreement with China Exim Bank for further Huawei led expansion of its network infrastructure (Privacy International). However, critics remain concerned about the privacy and data security of citizens, concerns which seem well placed. China's National Intelligence Law, promulgated in June 2017, requires all Chinese companies to collect secret information and provide such private data to the Chinese government. Hidden from the end user are backdoors and so-called middleboxes, which are distribution stations that transmit information and are able to filter and manipulate information (Ryals).

The government of Zimbabwe has also invited more Chinese businesses to build Smart cities. Chinese company, Hikivision, is currently piloting an ambitious smart city project in Zimbabwe's fourth largest city, Mutare. Yet, Hikivision is sanctioned by Western governments for human rights abuses against the Muslim Uyghur minority community (Africa Defence Forum). A smart city dubbed MelfortSmart City (MSC) is to be built, 60 km east of the capital, along the Harare-Mutare highway. A third smart city in Mt Hampden, located about 20 km north of the capital city, sponsored by the

> *... while conferring ranks to newly promoted Airforce of Zimbabwe officers on January 7, 2022, Air Marshal Elson Moyo declared social media and matters related to cybersecurity as "enemies of the state"*

government of China, will accommodate the parliament building, government ministries, residential areas, shopping malls, hotels and industries. These plans continue despite the fact that China has been accused of spying on the African Union headquarters (Dahir).

Zimbabwe was named in the Pegasus leaks for acquiring mobile phone hacking technology in 2019 from Israeli firm NSO Group (Chutel). The Pegasus mobile malware permits the Central Intelligence Organisation (CIO) to spy on the communications of targeted activists, opposition politicians and journalists as the country heads towards elections in 2023. Pegasus can also penetrate applications like WhatsApp, even though they are end-to-end encrypted, and extract photographs, emails and call records.

Despite intimidation tactics employed by the state to stifle online discourse, Zimbabweans still use social media to express dissenting political opinions and to form online campaigns. The launch of popular opposition leader, Nelson Chamisa's new political party has inspired hashtags on Twitter such as #ZANUPFMustGo. These political moments are often followed by coordinated inauthentic behaviour and misinformation campaigns led by government supporters (Moyo). Internet shutdowns remain a constant threat in Zimbabwe as well. In January 2019, mass protests against fuel hikes were followed by internet shutdowns and lethal army crackdowns against protesters ("Zimbabwe imposes"). However, a week after the protest, a court ruled that the shutdown was illegal and that the government exceeded its mandate by imposing it (Dzirutwe).

Thematic Focuses

5

This section highlights some of the cross-cutting themes in digital authoritarianism, to aid in developing an approach that can be used across various national and political contexts. The themes in digital authoritarianism are grouped into the following categories:

1. ***Data Governance*** (including privacy, data protection and surveillance)
2. ***Speech*** (including freedom of expression, freedom of information and opinion)
3. ***Access*** (Including service interruptions, punitive taxation and legislation).
4. ***Information*** (including coordinated inauthentic behaviour and influence campaigns, disinformation, misinformation and malinformation)

1. DATA GOVERNANCE

Of all the practices associated with digital authoritarianism, surveillance is perhaps the one most likely to emerge in countries regardless of whether or not they are considered democratic. Zuboff coined the term **surveillance capitalism** to refer to the politics of data accumulation that promotes the centralisation of data contexts. As tech companies make data collection a central part of their innovation models, societies broadly become desensitised to this kind of surveillance (Zuboff). Surveillance capitalism is therefore one part of normalising surveillance in the public sphere. Similarly, there is a growing practice of countries exporting surveillance technology, particularly in advanced economies facilitating technology transfers with military regimes in the global south (Feldstein).

In a global analysis of the surveillance industry, Privacy International found that of the 528 surveillance companies it monitored, the vast majority were based in economically advanced, large arms exporting states. It identified the USA, UK, France, Germany and Israel as the top five countries where these companies are headquartered (Privacy International). In 2018, Hintz and Milan conducted a survey on surveillance and massive data collection in liberal democracies in the European Union and the Americas. They found that the diffused character of surveillance in Western democracies can often go unnoticed because it is perpetrated by private capital or subnational entities like the police. But understanding such practices even in nominally democratic countries is crucial, they argue, because it allows us to identify their transnational character, to place them in proper organisational and social contexts and to examine their long term consequences (Hintz and Milan 3944). Hintz and Milan emphasise the role of private capital and private-public partnerships, particularly with social media companies as a way of deepening surveillance capacities (Hintz and Milan 3946). They argue that for real accountability to be created, we have to pay attention to surveillance in all contexts. Similarly, Steven Feldstein analyses the surveillance efforts of 179 countries and concludes that the main users of the surveillance technologies are not only authoritarian regimes, such as China, but also liberal democracies, such as the United States. Therefore, we need a broader understanding of surveillance regarding its relationship with different regimes, repression, and human rights.

Technology-enabled surveillance is an underlying characteristic of digital authoritarianism. It facilitates regime watching, controlling, and punishing people for their undesirable acts. One of the earliest definitions of data-enabled surveillance, named dataveillance, was made by Roger Clark in 1988. According to Clark, dataveillance is "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons." A government can practise dataveillance in two ways. First, it can monitor the activities of a specifically identified person (e.g., an anti-regime political actor, activist, or fundraiser) through a systemic use of data systems. Second, it can practise mass surveillance of the society to investigate and monitor the societal behaviours, reactions, and organisations.

Data governance also concerns the right to privacy, which refers to the right to protect an individual's information from public scrutiny, ensuring that individuals must provide their informed consent for their information to be collected and processed by both public and private institutions. It implies that even where information is given to the state voluntarily, there is an obligation to handle the information with respect to this right, regardless of the conditions under which it was provided. The right to privacy is guaranteed by international conventions like Article 12 of the United Nations Declaration of Human Rights (UDHR): "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." Similarly, Article 17 of the International Covenant on Civil and Political Rights (ICCPR) states that: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour or reputation. Everyone has the right to the protection of the law against such interference or attacks." Article 14 of the UN Convention on Migrant Workers, Article 16 of the UN Convention on the Rights of the Child, and Article 8 of the European Convention on Human Rights are several of the international regulations to protect individuals' privacy.

Despite these protections, privacy is often framed as a private concern rather than a collective or a political responsibility. Video and voice surveillance are also on the rise, particularly at international borders and with refugee or minority populations, preceded by large scale data collection exercises that violate individual privacy. One report estimated that the video and voice surveillance market in the world is worth an estimated USD 33.5 billion (Privacy International).

The increased use of CCTV in public places also enables a culture of surveillance in urban areas. Smart cities are the latest development in governance innovation in which digital technology is combined with public administration, with the promise of improving service delivery. Smart cities integrate data collection across various services, such as utilities, transport, security and more. Governments building and using smart city technology may create backdoors for information sharing between agencies, violating privacy rules because they encourage the use of data beyond the scope that it was collected for. Smart city projects sometimes involve external or international data processing, which creates vulnerabilities concerning data colonialism, where rich countries build smart city infrastructure in emerging countries with the unstated intention of harvesting and processing that data for other purposes. Smart city projects deployed in this way violate the privacy rights of these countries' citizens and give them no course for redress as they occur outside the civic relationship between citizens and states.

Hacking and cybersecurity violations are an omnipresent threat where technology is increasingly used in public administration. In July 2019, the largest hacking incident of civic data recorded occurred in Bulgaria, where the tax records of 5 million Bulgarians were hacked and made public (Kottosová). Cybersecurity experts note that almost all governments were vulnerable to these types of hacks because they are unwilling or unable to make the kind of large-scale investments that would actually make government data genuinely secure. Governments have demonstrated that they are more eager to collect data than to protect it. More importantly, they rarely provide avenues for citizens to complain or demand action in cases where this kind of hacks occur.

One obvious response to this is to pass more effective data protection laws. Still, data protection laws only work where governments are willing to be constrained by the legal regime, which has not been the case even in countries that are seen as democratic. In 2016, the ACLU reported that the police department in Baltimore purchased Geofeedia technology that allowed it to conduct surveillance on anti-police brutality protesters and to use that information to intimidate protesters by enforcing past warrants or outstanding fines (ACLU). Similarly, governments often carve large exceptions for national security into data protection and data privacy laws that undermine the overall effectiveness of the laws or allow them to be used discriminatorily.

2. SPEECH

The former UN High Commissioner for Human Rights defined freedom of expression as part of a family of rights, including association and freedom of assembly, that enable people to share ideas, form new thinking and join together to claim their rights (Donders and McGonagle 1). These rights are fundamental to the protection of other rights and, more broadly, to the protection of democracy because they influence our ability to understand and respond to the political information that exists in our societies. They are fundamental to our ability to persuade others to change their behaviour and to our participation in public life (Donders and McGonagle 3). Donders and McGonacle (2015) argue that the distinction between freedom of information, opinion and expression is subtle and hinges on sequencing, in that we need there to be freedom to generate information so that we can form opinions on them and then subsequently express those opinions in the public sphere (Donders and McGonagle 3).

However, they also argue that the relationship is cyclical, in that those opinions, once expressed, then become new forms of information that must be responded to. Other experts therefore argue that freedom of expression is a compound right that consists of the freedoms of opinion and information as well as a few more elements. The broad theoretical consensus however is that information is vital to healthy democracies, and the freedom to generate it, form opinions on it and react to it by expressing those opinions is central to free societies. These freedoms are intimately connected to the idea of press freedom, because the press is the central method through which most of us receive our political information. Press freedom can be defined as "the right to publish and disseminate information, thoughts,and opinions without restraint or censorship"(Merriam-Webster).

Several states have relied on legislative measures to regulate the exercise of the right to freedom of expression. This has been done either by relying on existing legislation such as national security laws, anti-terrorism laws and penal laws or by enacting laws intended to regulate online content. According to the UN OHCHR, at least 40 social media laws were

enacted in the last two years, with another 30 laws under consideration.
Constraining speech in the public sphere and press freedom particularly is a key practice of digital authoritarianism and is achieved through a variety of methods. In several authoritarian regimes, the government views the press as an extension of the power centre — either the military or the party state — and not only does it expend significant resources to suppress contending ideas, but also to diminish the perception of threat by contaminating the airwaves with banality (Chan 66). The advent of digital technologies therefore impacts press freedom first by affecting the ability of journalists and independent media houses to operate but also by increasing the ability of the state to influence output through some of the other practices outlined here. States like China have also invested in specific technologies that allow them to monitor and respond to public opinion down to the level of an individual's account (Chan 67), as evidenced in the case of the missing tennis player, Peng Shuai.

Fisking or fiscal blackmail is one practice that occurs in quasi-authoritarian regimes as a method of controlling press freedom. Governments make it difficult for media to remain independent by creating economic conditions that make running the media impossible, including raising taxes on operations, creating increasingly elaborate financial reporting systems, or, in countries where the government is the largest advertiser, withholding government advertising contracts in order to create financial precarity (Committee to Protect Journalists). This maintains an illusion of press freedom while undermining the ability of the press to operate truly freely.

Legislation is also routinely framed as operating in the public interest even though it primarily advances the authoritarian interests of the state. Ecuador's Organic Law of Communication is an example of such a law. After it was passed at least 1081 cases were filed against the media and journalists and most resulted in nuisance and punitive action that is not directly designed to criminalise the press but certainly to distract them from their core work, and to bog them down in litigation. According to one study, the Supercom agency created by the bill collected USD 531,288 in fines in four years (Higuera). Private actors too can use the judicial system to frustrate the free press as in the case of UK journalist Carole Cadwalladr who was sued for libel after rightly reporting on the influence of Russian politics in UK politics in 2021 (Siddique). Cadwalladr eventually won the lawsuit but endured significant financial hardship while it was active.

While restrictions to freedom of expression are permissible in emergency situations, it is important that these restrictions do not render the right illusory. Legislation relied on often "… employs broad terms that grant authorities significant discretion to restrict expression and provide individuals with limited guidance about the lines dividing lawful from unlawful behaviour" (UN General Assembly). Restrictions should be provided by law, necessary and proportionate to protect a legitimate objective and subject to independent oversight. Unfortunately, governments regularly use emergency contexts to bring in punitive legislation to restrict speech in the public sphere. Turkey's continuous campaigns against journalists and activists following the attempted coup in 2016 is an example of restrictions of freedom of speech that are not only excessive in the moment but have also endured far beyond a reasonable timeline.

The criminalisation of certain types of speech online is also a growing concern. In countries like Egypt and Turkey these restrictions are framed as efforts to control misinformation and hate speech online, although in Egypt, three TikTok influencers were charged with human trafficking for their online presence which remains an unprecedented use of the state's power to criminalise speech online (Osman). Some of the penalties and fines are levelled against media companies and social networking sites directly, as with the Russian ban of Facebook as extremist organisations (Sauer).

Overall, constraining speech has become a major tactic used to advance digital authoritarianism, particularly by using legislation and the judicial system to either criminalise various acts of speech, the work of journalists and the ability of speech to reach specific audiences.

3. ACCESS

The digital divide is a term that refers to the relationship between poorer members of society and their inability to access internet and information communication technologies. According to a report by the International Telecommunication Union (ITU), most offline populations live in the least developed countries. The internet penetration in developed countries is 87% but just 47% in developing countries and 19% in the least developed countries. Moreover, the digital gender gap is growing fast in developing countries. This means that in all regions, men have more access to the internet than women. In parallel, two-thirds of the world's school-age children do not have access to the internet (UNICEF), the largest source of information in the world.

During the past few years, the digital divide has exacerbated most of today's inequalities and pre-existing social issues. As dependency on the internet increased during the COVID-19 pandemic, people without robust internet access were left behind academically and financially. In turn, governments worldwide are abusing their power to arbitrarily impose restrictions over internet access, thus increasing the gap between those who benefit from access to the new information communications technologies and those who do not.

There are many practices that are used to reduce wholesale access to the internet in order to advance authoritarian agendas. Bandwidth throttling (or just 'throttling') occurs when the speed of the internet is deliberately slowed down at source. It is usually done by the main telecoms provider or the government regulator, who limit the speed of incoming (received) data or the outgoing data in a network device. It is not possible to circumvent throttling except by switching to a satellite service (versus a broadband or a GSM provider). Social media shutdowns occur when selected networking sites are blocked in various locations, and usually require the compliance of an internet service provider or a mobile internet service provider as they only target specific websites.

An internet shutdown occurs when a government, generally through the regulator, disrupts internet traffic and makes the internet effectively unusable for a specific population or a location, in order to stop the flow of information (UNICEF). A complete internet shutdown occurs when the government shuts down the entire internet either for a specific region or for the whole country. Internet shutdowns are possible in countries where the government maintains extensive control over the telecommunications system, either by owning the main provider or through the main regulator, or where the government can exert significant influence over the ISPs by threatening to revoke their licence or charges. In 2020, the Access Now global coalition recorded at least 155 internet shutdowns in 29 countries around the world. Most of these shutdowns were in Africa (10), but also in the Middle East and North Africa (8) and in Asia-Pacific (Access Now).

Other forms of violations have been recorded, as when Uganda applied a social media tax that charged people extra for using their phones to connect to specific social networking sites (Mwesigwa). Governments can also choose to tax internet platforms heavily in order to force them to pass the cost to users which then makes them less popular. Moreover, there are also service interruptions - such as direct denial of service attacks - that are perpetrated by private actors that can create opportunities for authoritarian entrepreneurship, particularly by providing justification for harsher prevention against the general population. These are worth cataloguing and understanding.

Under the pretext of protecting national security and preventing violence during protests, governments often implement internet shutdowns as a means to control the free flow of information. Moreover, as authoritarian regimes increase in all regions, governments find it easier to curtail online freedom of expression to contain dissenting opinions. However, deliberate internet outages have knock on effects, including costing billions of dollars to the global economy. The 257 major shutdowns in 46 countries since 2019 have cost USD 18.1 billion. Myanmar (USD 2.8 billion) is the most affected nation, followed by Nigeria and India (Woodhams and Migliano).

The growing ruthlessness of authoritarian regimes around the world shows that shutdowns are most common during election times (Ryan-Mosley). For example, in Uganda, an internet shutdown occurred in the middle of the presidential elections and the blackout was only lifted 100 hours later. As a result of the almost five-day shutdown, the Ugandan economy was affected by nearly USD 9 billion. Authorities explained that the interruption was to prevent interference in the election. However, digital rights movements explained that the government's internet blackout was a deliberate decision to keep citizens and the rest of the world in the dark during the election period (Bhalla and McCool).

Similarly, in Belarus, the internet was interrupted for 61 hours following the 2020 elections. The shutdowns continued to occur after the pro-democracy protests that led to more than 500 journalists and activists being arrested. Moreover, the authorities took additional measures to limit access to information during the elections, including blocking civil society organisations' websites, forcing dissenting opinions to be removed and labelling some Telegram channels as "extremists"(Freedom House).

For repressive and authoritarian regimes, shutting down the internet is a popular tactic to suppress dissenting voices and to hide human rights abuses. Further, as protests movements rely increasingly on the internet (Carpenter), internet lockdowns are taking place to prevent collective political protests ("Digital Siege"). To date, the most severe internet shutdown has been in Kazakhstan, after protests over rising fuel prices turned into anti-government violence (Hart). The government's use of internet outages to censor protests impacted people, local businesses, and major industries. Media outlets could not connect with people on the field and left many citizens uninformed and unaware of the troops being deployed in their country (Krapiva et al.).

Kazakhstan's experience illustrates how internet shutdowns are part of any modern conflict. According to Mijhail Klimarev, executive director of the internet Protection Society, "in the event of a real military conflict, it is the internet infrastructure that will be destroyed in the first place" (Satariano et al.). There is a growing fear that the internet will be turned off or interrupted by an outside source, leaving many people disconnected, and affecting many other services. As a result, it is expected that many internet shutdowns will occur during the following days, especially in the areas closer to the border between Russia and Ukraine. In turn, Russia is intensifying censorship, adding pressure to some of the world's largest tech companies. The government gave Google, Meta, Apple, Twitter, TikTok, and others that they had until the end of February 2022 to comply with its so-called landing law (Satariano). The new law introduced a fine of up to 10% of any company's annual revenue if the website failed to take down content deemed illegal under Russian law. According to civil society organisations, the law makes companies and their employees more vulnerable to Russia's censorship tools, stifles dissent, and suppresses peaceful protests (HRW). As at the time of writing, many of these websites have been banned in Russia (Bond and Allyn).

4. INFORMATION

Information is the raw material for governance and political behaviour, and the manipulation of information in the public sphere is one of the main ways through which authoritarian regimes can advance their agendas (Nyabola). Historically, there is evidence of actors using false information to achieve political goals long before the invention of the printing press ("A brief history"). However, technology has allowed information to be shared at a greater speed and scale, culminating in the mastery of propaganda, which aims to use information to change people's political views, sometimes by providing incomplete information or even using falsehoods.

The development of digital means and the proliferation of social media brought a broad category of political communication to a certain level of sophistication caused by the increasing complexity of communication channels. UNESCO highlights three reasons for the intensification of the spread of false and misleading information: collapsing traditional business models in journalism and advertising; digital transformation of newsrooms and storytelling, and creations of news ecosystems (Ireton and Posetti). Multiple actors are now taking on the role of gatekeepers, producers and consumers of politically-motivated content. The behaviour of these actors is often affected by technological algorithms, targeting and advertising techniques. News and political information are now circulating in smaller networks of users, making it harder to access confronting positions and views to create a more balanced perspective. These factors contribute to the formation of a new architecture of political communication in which the public becomes more prone to manipulating information accessible via digital means.

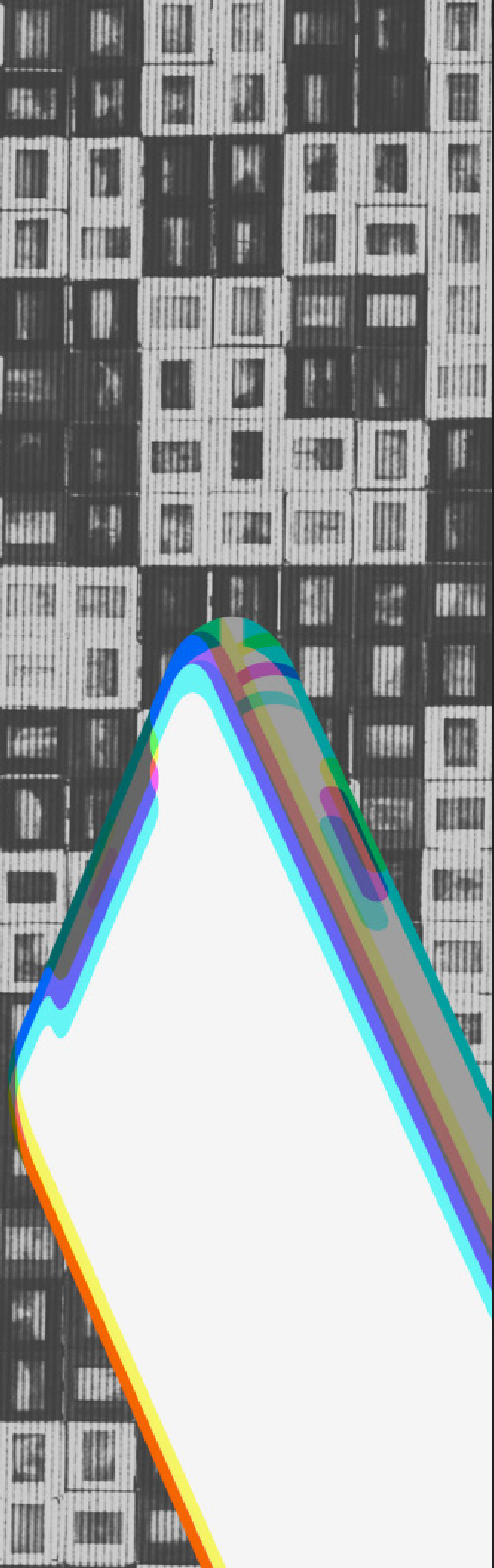
There are different practices in the digital sphere that essentially amount to the same root practice — interfering with people's ability to receive factual and accurate information about their society to make informed political decisions. This list includes misinformation, disinformation, mal-information, coordinated inauthentic behaviours and political astroturfing. These practices have garnered increasing attention on the internet, particularly as social media has become a potent site for political discourse. The distinctions occur at the level of intent in the practice and technological means used. Misinformation occurs when incorrect information is spread without the intent to harm. It is the case of circulating unverified or poorly sourced information that appears to be false. This may be harmful, but it is inevitable at the given pace of content production in the data-driven world.

Disinformation occurs when false information is shared with the intent to cause harm. It is a manipulation technique aimed strategically to persuade content consumers into a specific way of thinking or to take a politically motivated course of action. Some authors acknowledge the value-driven side of disinformation, highlighting its aims to "engender public cynicism, uncertainty, apathy, distrust, and paranoia, all of which disincentive citizen engagement and mobilisation for social or political change" (National Endowment for Democracy). Mal-information happens when factual information is manipulated and distributed with the intent to cause harm. Similar to the practice of propaganda, mal-information aims to create a favourable opinion of a particular idea by the audience.

Commonly, the subjects of mis/dis/mal-information can be individuals, organisations and states. Even though the phenomenon is not new as a communication practice, the digital means that shape and amplify the circulation of such information may significantly enhance the spread of false information or foster the perception of false information as true. In some cases, the agents spreading the incorrect information are private actors paid to capitalise on the algorithms these platforms run on to amplify this. Bot farms are essentially coordinated efforts to create and amplify misinformation through the creation of fake accounts, while troll farms perform the same function but are usually run by real people paid poorly to develop a vision of dynamic online behaviour ("Election security"). The collective action of these platforms is known as coordinated inauthentic behaviour and is routinely paid for by governments to advance specific authoritarian narratives (Gleicher).

Another form of using unreal social media accounts to create an impression of significant public support is known as political astroturfing — "political campaigns disguised as spontaneous 'grassroots' behaviour that a single person or organisation, in reality, carries out" (Ratkiewicz et al. 297). Such cases of orchestrated public support are not exclusive to authoritarian states, but on the contrary, become a good ideological fit for the democratic setting.

If, in many authoritarian countries, the largest purveyor of misinformation, disinformation and mal-information is the government itself, in more democratic societies that allow a plurality of opinions, the same methods can be used by political leaders to achieve their goals. Moreover, the complex digital media ecosystems involve multiple actors who may facilitate or limit cases of information manipulation, namely internet companies that provide online information services. Therefore, it is important to contextualise these practices as part of a longer history of political communication and propaganda to advance political agendas, paying attention to the interests of providers of digital infrastructure.



Conclusion

6

Digital authoritarianism refers to a specific orientation towards internet governance focused on constraining civic discourse, undermining press freedom, and restricting the ability of individuals and organisations to criticise power. It is particularly visible in societies where the executive, either in the form of a president, a military ruler or a monarch, exercises disproportionate power over other arms of government. However, it is also evident in societies where the executive can collude with other branches of government to bring about the same outcome. The main digital tactics focus on:

1. Constraining people's ability to access the internet, including internet access restrictions, internet and social media shutdowns, bandwidth throttling, punitive internet taxes and ISP controls.

2. Monitoring or surveilling people on the internet and on digital platforms, including public digital surveillance, the use of internet enabled devices, and analogue strategies like physical surveillance and the use of informants, as well as online tracking.

3. Manipulating the online information ecosystem, through influence campaigns, misinformation and malinformation, coordinated inauthentic behaviour and other forms of propaganda.

4. Controlling access to technology including banning Virtual Private Networks, banning services and using device based surveillance.

5. Controlling freedoms of privacy, data protection, expression, movement and media

6. System attacks like hacking, fisking and direct denial of service (DDOS attacks).

Each of these attacks is premised on the same idea: that quality public information is central to functional democracy, and that the internet makes access to information easier for ordinary people and that constraining access to the internet is a crucial way of extending authoritarian rule because poorly or less informed people are less likely to organise resistance to authoritarian regimes. Some are premised on preventing the information from being generated (fisking, DDOS, hacking, surveillance; some on preventing it from being transmitted (legislation and judiciary misuse, restrictions on public freedoms); and others yet on misrepresenting the information altogether and contorting the public's perception of truth (mis-, dis-, mal-information).

Even so, it is important to note that digital authoritarianism is not a purely domestic challenge. Indeed, as mentioned, much of the technology used to advance these authoritarian impulses is provided by a handful of countries that in themselves are arguably democratic. Israel (NSO Group), Italy (The Hacking Team), and the UK (Cambridge Analytica) are just some of the countries where companies implicated in some of the most visible technology transfers to advance digital authoritarianism are registered. Without constant vigilance and concerted efforts to resist it, all countries by some measure are vulnerable to digital authoritarianism. Thus responses to digital authoritarianism must be multilateral by definition, and must include action against those governments and corporations that enable digital authoritarianism.

This report shows that digital authoritarianism is not a preserve of certain styles of government, but rather an indication of a shifting culture towards governance that sees the executive particularly as being entitled to wield unconstrained power over civilians. At the same time, it is a culture that uses legislation as a means of entrenching and extending this power, thereby giving the power grab a semblance of legitimacy. It is also a culture that connects global capital to specific national or regional political interests, where a handful of companies operating from democratic countries create technology that is sold to authoritarian regimes around the world in order to expand the practices of digital authoritarianism. It is a culture that has no tolerance for freedom of the press and freedom of expression. Finally, it is a culture that has no regard for the welfare of citizens in the face of these rising threats, often enabling violent suppression of dissenting voices in the interests of preserving power. While the responses to digital authoritarianism may vary depending on local contexts, by raising awareness of common threats and how each of them manifests in various countries, this report has argued that it is crucial to address the challenge resolutely in all contexts and prevent it from spreading unchecked to contexts where systems to protect civilians against excesses of power may not be as robust.

Works Cited

"#KeepItOn FAQ." *Access Now*, https://www.accessnow.org/keepiton-faq/.

"2020 Tanzania in Figures."*National Bureau of Statistics*, Ministry of Finance and Planning, June 2021, https://www.nbs.go.tz/nbs/takwimu/references/2020_Tanzania_in_Figure_English.pdf.

"4G Internet To Be Restored Across Jammu And Kashmir After 18 Months." *NDTV*, 5 Feb. 2021, https://www.ndtv.com/india-news/4g-mobile-internet-services-being-restored-in-entire-jammu-and-kashmir-tweets-top-official-2364068.

"A Brief History of Fake News." *BBC Bitesize*, BBC, 4 Dec. 2020, https://www.bbc.co.uk/bitesize/articles/zwcgn9q.

"Advox." *Advox*, Global Voices, https://advox.globalvoices.org/about/.

"AFTE Condemns the Five-Year Prison Sentence against Content Creators 'Sherry and Zomoroda', and Calls for a Halt to Tiktok Trials." *Association of Freedom of Thought and Expression*, 14 June 2021, https://afteegypt.org/en/advocacy-en/statements-en/2021/06/14/22936-afteegypt.html.

Africa Defense Forum. "Chinese Smart Tech Fraught with Risk." *DefenceWeb*, 17 Sept. 2021, https://www.defenceweb.co.za/joint/science-a-defence-technology/chinese-smart-tech-fraught-with-risk/.

Akdeniz, Yaman. "Turkish Internet Censorship during the COVID-19 Pandemic." *Article 19*, 11 Feb. 2022, https://www.article19.org/resources/blog-turkish-internet-censorship-during-the-covid-19-pandemic/.

Alam, Mahtab. "Attacked, Arrested, Left Without Recourse: How 2020 Was for India's Journalists." *The Wire*, 26 Dec. 2020, https://thewire.in/media/journalists-arrested-press-freedom-2020.

Amouzai, Ali. "The February 20 Movement in Morocco: Roots of Failure and Lessons for the Future." *Longreads*, TNI, 27 Oct. 2021, https://longreads.tni.org/fr/the-february-20-movement-in-morocco.

"Assistance Association for Political Prisoners." *AAPP*, https://aappb.org/.

Bachir, Malek. "Pegasus: From Its Own King to Algeria, the Infinite Reach of Morocco's Intelligence Services." *Middle East Eye*, 21 July 2021, https://www.middleeasteye.net/news/pegasus-morocco-king-macron-targeted-intelligence-reach.

Bajoria, Jayshree. "Coronajihad Is Only the Latest Manifestation: Islamophobia in India Has Been Years in the Making." *Human Rights Watch*, 1 May 2020, https://www.hrw.org/news/2020/05/01/coronajihad-only-latest-manifestation-islamophobia-india-has-been-years-making.

Beech, Hannah. "Myanmar's Military Deploys Digital Arsenal of Repression in Crackdown." *The New York Times*, 1 Mar. 2021, https://www.nytimes.com/2021/03/01/world/asia/myanmar-coup-military-surveillance.html.

Begum, Rothna. "Egypt Persecutes TikTok Women While Men Get Impunity for Sexual Violence." *Human Rights Watch*, 28 June 2021, https://www.hrw.org/news/2021/06/28/egypt-persecutes-tiktok-women-while-men-get-impunity-sexual-violence.

"Belarus: Freedom on the Net 2021 Country Report." *Freedom House*, https://freedomhouse.org/country/belarus/freedom-net/2021.

Bergamo, Mônica. "Jornalistas Mulheres Sofrem Um Ataque a Cada Três Dias No Brasil, Com Destaque Para Bolsonaro, Mostra Estudo [Women Journalists Suffer an Attack Every Three Days in Brazil, with Bolsonaro in Particular, Study Shows]." *Folha De S.Paulo*, 7 Mar. 2022, https://www1.folha.uol.com.br/colunas/monicabergamo/2022/03/jornalistas-mulheres-sofrem-um-ataque-a-cada-tres-dias-no-brasil-com-destaque-para-bolsonaro-mostra-estudo.shtml. Accessed 8 Mar. 2022.

Bhalla, Nita, and Alice McCool. "100 Hours in the Dark: How an Election Internet Blackout Hit Poor Ugandans." *Reuters*, 20 Jan. 2021, https://www.reuters.com/article/us-uganda-internet-rights-trfn/100-hours-in-the-dark-how-an-election-internet-blackout-hit-poor-ugandans-idUSKBN29P1V8.

Bhargava, Yuthika. "Govt. Asks Twitter to Remove 1,178 Accounts." *The Hindu*, 8 Feb. 2021, https://www.thehindu.com/news/national/govt-asks-twitter-to-remove-1178-accounts/article61753981.ece.

Borger, Julian. "Twitter Deletes 20,000 Fake Accounts Linked to Saudi, Serbian and Egyptian Governments." *The Guardian*, 3 Apr. 2020, https://www.theguardian.com/technology/2020/apr/02/twitter-accounts-deleted-linked-saudi-arabia-serbia-egypt-governments.

Cagle, Matt. "Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color." *American Civil Liberties Union*, 11 Oct. 2016, https://www.aclu.org/blog/privacy-technology/internet-privacy/facebook-instagram-and-twitter-provided-data-access.

Camporez, Patrik, et al. "Como Youtubers Bolsonaristas Ganham R$ 100 Mil Mensais Com Informações Privilegiadas Do Planalto [How Bolsonarista YouTubers Earn BRL 100,000 Monthly with Privileged Information from the Planalto]." *Estadão*, 4 Dec. 2020, https://politica.estadao.com.br/noticias/geral,como-youtubers-bolsonaristas-ganham-r-100-mil-mensais-com-informacoes-privilegiadas-do-planalto,70003539302. Accessed 16 Feb. 2022.

Campos Mello, Patrícia. "WhatsApp Admits to Illegal Mass Messaging in Brazil's 2018." *Folha De S.Paulo*, 9 Oct. 2019, https://www1.folha.uol.com.br/internacional/en/brazil/2019/10/whatsapp-admits-to-illegal-mass-messaging-in-brazils-2018.shtml. Accessed 16 Feb. 2022.

Carpenter, Scott. "Internet Shutdowns Are a Political Weapon. It's Time to Disarm." *TechCrunch*, 30 Oct. 2021, https://techcrunch.com/2021/10/30/internet-shutdowns-are-a-political-weapon-its-time-to-disarm/.

Çelik, Burçe. "Turkey's Communicative Authoritarianism." *Global Media and Communication*, vol. 16, no. 1, Apr. 2020, pp. 102–120, doi:10.1177/1742766519899123.

Celik, Doga, and Arzu Geybullayeva. "In Turkey, a Social Media Battle amid on-Going Blazes." *Global Voices*, 12 Aug. 2021, https://globalvoices.org/2021/08/12/in-turkey-a-social-media-battle-amid-ongoing-blazes/.

Chakraborty, Saumya. "Deciphering the World Press Freedom Index." *NITI Aayog*, 21 Jan. 2021, https://www.niti.gov.in/index.php/deciphering-world-press-freedom-index.

Chan, Joseph M. "From Networked Commercialism to Networked Authoritarianism: The Biggest Challenge to Journalism." *Journalism*, vol. 20, no. 1, Jan. 2019, pp. 64–68, doi:10.1177/1464884918806741.

Charner, Flora, and Marcia Reverdosa. "Far-Right Candidate Jair Bolsonaro Wins Presidential Election in Brazil." *CNN*, 29 Oct. 2018, https://edition.cnn.com/2018/10/28/americas/brazil-election/index.html. Accessed 16 Feb. 2022.

Chau, Thompson, and Dominic Oo. "Myanmar Renews Plans to Curb Internet Usage with VPN Ban." *Nikkei Asia*, 21 Jan. 2022, https://asia.nikkei.com/Spotlight/Myanmar-Crisis/Myanmar-renews-plans-to-curb-internet-usage-with-VPN-ban.

Chaudhuri, Pooja. "18 Times BJP Spokesperson Sambit Patra Shared Propaganda-Fuelled Misinformation." *The Wire*, 17 June 2020, https://thewire.in/politics/bjp-sambit-patra-fake-news-propaganda.

Chutel, Lynsey. “Pegasus Lands in Africa.” *Foreign Policy*, 28 July 2021, https://foreignpolicy.com/2021/07/28/nso-pegasus-africa-morocco-rwanda/.

CIPESA, 2014, *State of Internet Freedoms in Tanzania 2014*, http://www.cipesa.org/?wpfb_dl=182.

“Civic Media Observatory.” Global Voices, https://globalvoices.org/special/observatory/.

“Citizen Lab Summer Institute on Monitoring Internet Openness and Rights.” *Citizen Lab*, 19 June 2015, https://citizenlab.ca/summerinstitute/2015.html.

Comunicación Ecuador [@ComunicacionEc]. “Ecuador retira asilo a Julian Assange por violar reiteradamente convenciones internacionales y protocolo de convivencia #EcuadorSoberano [Ecuador withdraws asylum from Julian Assange for repeatedly violating international conventions and coexistence protocol #EcuadorSoberano].” *Twitter*, 11 Apr. 2019, https://twitter.com/ComunicacionEc/status/1116272104180154368

Deibert, Ronald, et al. *Access controlled: The shaping of power, rights, and rule in cyberspace*. the MIT Press, 2010.

Della Coletta, Ricardo. “Bolsonaro Ataca Barroso e Moraes, Do STF, e Os Acusa De Ameaçar Liberdades [Bolsonaro Attacks STF’s Barroso and Moraes and Accuses Them of Threatening Freedoms].” *Folha De S.Paulo*, 12 Jan. 2022, https://www1.folha.uol.com.br/poder/2022/01/bolsonaro-ataca-barroso-e-moraes-do-stf-e-os-acusa-de-ameacar-liberdades.shtml. Accessed 16 Feb. 2022.

Dello Coletta, Ricardo, and Afonso Benites. “Onda Conservadora Cria Bancada Bolsonarista No Congresso [Conservative Wave Creates Bolsonarista Bench in Congress].” *El País Brasil*, 8 Oct. 2018, https://brasil.elpais.com/brasil/2018/10/07/politica/1538947790_768660.html. Accessed 16 Feb. 2022.

“Digital Siege: Internet Cuts Become Favored Tool of Regimes.” *NBCNews.com*, 11 Feb. 2021, https://www.nbcnews.com/tech/tech-news/digital-siege-internet-cuts-become-favored-tool-regimes-rcna282.

Dragu, Tiberiu, and Yonatan Lupu. “Digital Authoritarianism and the Future of Human Rights.” *International Organization*, vol. 75, no. 4, 2021, pp. 991–1017, doi:10.1017/S0020818320000624.

Dwoskin, Elizabeth, and Annie Gowen. “Forget Facebook and Twitter, Fake News Is Even Worse on WhatsApp — and It Can Be Deadly.” *The Washington Post*, 23 July 2018, https://www.washingtonpost.com/business/economy/on-whatsapp-fake-news-is-fast--and-can-be-fatal/2018/07/23/a2dd7112-8ebf-11e8-bcd5-9d911c784c38_story.html.

Dzirutwe, MacDonald. “Zimbabwe Court Says Internet Shutdown Illegal as More Civilians Detained.” *Reuters*, 21 Jan. 2019, https://www.reuters.com/article/us-zimbabwe-politics-idUSKCN1PF11M.

Dzoma , Garikai. “Zimbabwe Government Is Sending Our Faces to China so China’s Artificial Intelligence System Can Learn to See Black Faces.” *Techzim*, 8 Nov. 2018, https://www.techzim.co.zw/2018/11/zimbabwe-government-is-sending-our-faces-to-china-so-chinas-artificial-intelligence-system-can-learn-to-see-black-faces/.

Editors Guild of India [@IndEditorsGuild]. “The Editors Guild of India has issued a statement.” *Twitter*, 13 May 2020, https://twitter.com/indeditorsguild/status/1260501321695854593

“Egypt: Freedom on the Net, 2021 Country Report.” *Freedom House*, https://freedomhouse.org/country/egypt/freedom-net/2021.

“Egypt: One of the World’s Biggest Jailers of Journalists.” *RSF* (Reporters Without Borders), https://rsf.org/en/taxonomy/term/156.

“Egypt Papers.” *Disclose*, 21 Nov. 2021, https://egypt-papers.disclose.ngo/en.

"Egypt: Survivors of Sexual Violence and Online Abuse among Prosecuted Women Tiktok Influencers." *Amnesty International*, 13 Aug. 2020, https://www.amnesty.org/en/latest/news/2020/08/egypt-survivors-of-sexual-violence-and-online-abuse-among-prosecuted-women-tiktok-influencers/.

"Egyptian Belly-Dancer given Three-Year Jail Term for 'Inciting Debauchery'." *The Guardian*, 27 June 2020, https://www.theguardian.com/world/2020/jun/27/egyptian-belly-dancer-given-three-year-jail-term-for-inciting-debauchery.

"Eight Organizations and 145 Individuals Write to Govt on Concerns on Aarogya Setu App." *The Economic Times*, 18 Sept. 2020, https://economictimes.indiatimes.com/news/politics-and-nation/eight-organizations-and-145-individuals-write-to-govt-on-concerns-on-aarogya-setu-app/articleshow/78189485.cms?from=mdr.

"Election Security Q&A: What Are Bot Farms and Why Do Hackers Target Elections?" *CBS News*, 31 Oct. 2018, https://www.cbsnews.com/news/what-are-bot-farms-and-why-do-hackers-target-elections-cybersecurity/.

"Eleven Villagers Shot and Burned Alive by Myanmar Soldiers, Reports Say." *The Guardian*, 9 Dec. 2021, https://www.theguardian.com/world/2021/dec/09/eleven-villagers-shot-and-burned-alive-by-myanmar-soldiers-reports-say.

ElHachimi, Mohamed. "From Activism to Artivism: New Forms of Youth Activism in the Aftermath of the 20 February Movement." *IEMed*, 29 Jan. 2016, https://www.iemed.org/publication/from-activism-to-artivism-new-forms-of-youth-activism-in-the-aftermath-of-the-20-february-movement/.

Ellis, Leonardo. "Após Breve Trégua, Bolsonaro Volta a Lançar Dúvidas Sobre Urna Eletrônica [After a Brief Truce, Bolsonaro Again Casts Doubts on Electronic Voting Machines]." *Veja*, 5 Jan. 2022, https://veja.abril.com.br/coluna/maquiavel/apos-breve-tregua-bolsonaro-volta-a-lancar-duvidas-sobre-urna-eletronica/. Accessed 16 Feb. 2022.

"Em Nove Meses, Bolsonaro Cometeu 299 Ataques Ao Jornalismo [In Nine Months, Bolsonaro Committed 299 Attacks on Journalism]." *Fenaj*, 14 Oct. 2020, https://fenaj.org.br/nove-meses-bolsonaro-299-ataques/. Accessed 16 Feb. 2022.

Epifanova, Alena. "Digital Sovereignty on Paper: Russia's Ambitious Laws Conflict with Its Tech Dependence." *The Russia File*, Wilson Center, 23 Oct. 2020, https://www.wilsoncenter.org/blog-post/digital-sovereignty-paper-russias-ambitious-laws-conflict-its-tech-dependence.

"Erdoğan Threatens Media with Reprisals over 'Harmful' Content." *Duvar English*, 29 Jan. 2022, https://www.duvarenglish.com/erdogan-threatens-media-with-reprisals-over-harmful-content-news-60258.

Ergun, Fevzi Doruk. "National Security vs. Online Rights and Freedoms in Turkey: Moving beyond the Dichotomy." *Edam*, 3 Apr. 2018, https://edam.org.tr/en/national-security-vs-online-rights-and-freedoms-in-turkey-moving-beyond-the-dichotomy/#_ftn15.

"European Court Condemns Turkish Law Banning Insults of Erdogan." *Euronews*, 19 Oct. 2021, https://www.euronews.com/2021/10/19/european-court-condemns-turkish-law-banning-insults-of-erdogan.

Facebook, 2021, *June 2021 Coordinated Inauthentic Behavior Report*, https://about.fb.com/wp-content/uploads/2021/07/June-2021-CIB-Report-Final.pdf.

Falcão, Márcio, and Fernanda Vivas. "PF Diz Ao STF Que Milícia Digital Usa Estrutura Do 'Gabinete Do Ódio' [PF Tells STF That Digital Militia Uses 'Hate Office' Structure]." *G1*, 10 Feb. 2022, https://g1.globo.com/politica/noticia/2022/02/10/pf-diz-ao-stf-que-milicia-digital-usa-estrutura-do-gabinete-do-odio.ghtml. Accessed 16 Feb. 2022.

Feldstein, S. (2020). When It Comes to Digital Authoritarianism, China is a Challenge—But Not the Only Challenge. *War on the Rocks*. https://warontherocks.com/2020/02/when-it-comes-to-digital-authoritarianism-china-is-a-challenge-but-not-the-only-challenge/

"Fiscal Blackmail." Committee to Protect Journalists, 25 Apr. 2017, https://cpj.org/2017/04/fiscal-blackmail/.

Fleck, Giovana, and Laís Martins. "Influenciadores Digitais Receberam R$ 23 Mil Do Governo Bolsonaro Para Propagandear 'Atendimento Precoce' Contra Covid-19 [Digital Influencers Received BRL 23,000 from the Bolsonaro Government to Advertise 'Early Care' against Covid-19]." *Agência Pública*, 31 Mar. 2021, https://apublica.org/2021/03/influenciadores-digitais-receberam-r-23-mil-do-governo-bolsonaro-para-propagandear-atendimento-precoce-contra-covid-19/. Accessed 16 Feb. 2022.

Fuchs, Christian. *Digital Demagogue: Authoritarian Capitalism in the Age of Trump and Twitter*. Pluto Press, 2018.

Gainutdinov, Damir, and Pavel Chikov. "Internet Freedom 2017: Creeping Criminalisation." *Agora International Human Rights Group*, 2018, http://en.agora.legal/articles/Report-of-Agora-International-"Internet-Freedom-2017-Creeping-Criminalisation"/8.

"German-Made Finspy Spyware Found in Egypt, and Mac and Linux Versions Revealed." *Amnesty International*, 25 Sept. 2020, https://www.amnesty.org/en/latest/research/2020/09/german-made-finspy-spyware-found-in-egypt-and-mac-and-linux-versions-revealed/.

Geybullayeva, Arzu. "Turkey Reins in Social Media - One Platform at a Time." *Advox*, 11 Feb. 2021, https://advox.globalvoices.org/2021/02/11/turkey-reins-in-social-media-one-platform-at-a-time/.

Gill, Prabhjote. "Ndia Is Ramping up the Use of Facial Recognition to Track down Individuals without Any Laws to Keep Track of How This Technology Is Being Used." *Business Insider*, 10 Feb. 2021, https://www.businessinsider.in/tech/news/what-is-facial-recognition-technology-and-how-india-is-using-it-to-track-down-protestors-and-individuals/articleshow/80782606.cms.

"The Global Surveillance Industry." *Privacy International*, http://privacyinternational.org/explainer/1632/global-surveillance-industry.

Gleicher, Nathaniel. "Coordinated Inauthentic Behavior Explained." *Meta*, 6 Dec. 2018, https://about.fb.com/news/2018/12/inside-feed-coordinated-inauthentic-behavior/.

Gunitsky, Seva. "Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability." *Perspectives on Politics*, vol. 13, no. 1, 2015, pp. 42–54., doi:10.1017/S1537592714003120.

Gwagwa, Arthur. "Communications & Political Intelligence Surveillance on Human Rights Defenders in Zimbabwe, A Research Report." *The Zimbabwe Human Rights Forum*, 2013, https://www.hrforumzim.org/wp-content/uploads/2014/01/BPUK15104_Insides.pdf.

Hamad, Khattab. "How Burhan's Coup Could Halt Sudan's Return to the International Community." *Global Voices*, 4 Nov. 2021, https://globalvoices.org/2021/11/04/how-burhans-coup-could-stop-sudans-return-to-the-international-community/.

Hamad, Khattab and CIPESA writer. "Sudan's Bad Laws, Internet Censorship and Repressed Civil Liberties." *CIPESA*, 23 Dec. 2021, https://cipesa.org/2021/12/sudans-bad-laws-internet-censorship-and-repressed-civil-liberties/.

Hanson, Elizabeth C. *The Information Revolution and World Politics*. Rowman & Littlefield, 2008.

Hart, Robert. "Kazakhstan Reportedly Hit by Internet Blackout as Oil-Rich Nation Breaks out in Rare Anti-Government Protests." *Forbes*, 6 Jan. 2022, https://www.forbes.com/sites/roberthart/2022/01/05/kazakhstan-reportedly-hit-by-internet-blackout-as-oil-rich-nation-breaks-out-in-rare-anti-government-protests/?sh=2d29faed19a6.

Higuera, Silvia. "Ecuador's National Assembly Eliminates Controversial Sanctioning Body with Reforms to Communications Law." *LatAm Journalism Review*, Knight Center, 20 Dec. 2018, https://latamjournalismreview.org/articles/ecuadors-national-assembly-eliminates-controversial-sanctioning-body-with-reforms-to-communications-law/.

Hintz, Arne and Stefania Milan. "Authoritarian Practices in the Digital Age| "Through a Glass, Darkly": Everyday Acts of Authoritarianism in the Liberal West." *International Journal of Communication* vol. 12, 2017, pp 3939-3959.

Lavrilleux, Ariane [@AriaLavrilleux]. "#EgyptPapers Our website @Disclose_ngo has been blocked in Egypt after our revelation about French operation supporting Egyptian bombings
Not surprising, Sisi regime is familiar with online&media censorship in the name of so-called counterterrorism You can use a VPN/Tor." *Twitter*, 23 Nov. 2021, https://twitter.com/AriaLavrilleux/status/1463041119630077958?s=20

"Huawei and Surveillance in Zimbabwe." *Privacy International*, 18 Nov. 2021, https://privacyinternational.org/long-read/4692/huawei-and-surveillance-zimbabwe.

"Human Rights Watch Submission to the Universal Periodic Review of the United Republic of Tanzania." *Human Rights Watch*, 25 Mar. 2021, https://www.hrw.org/news/2021/03/25/human-rights-watch-submission-universal-periodic-review-united-republic-tanzania.

"India: Government Policies, Actions Target Minorities." *Human Rights Watch*, 19 Feb. 2021, https://www.hrw.org/news/2021/02/19/india-government-policies-actions-target-minorities.

"India: Modi Tightens His Grip on the Media ." *RSF (Reporters without Borders)*, https://rsf.org/en/india.

"Information Controls in an Unprotected Legal Landscape." *Open Technology Fund*, 9 Nov. 2020, https://www.opentech.fund/news/information-controls-unprotected-legal-landscape/.

"International Covenant on Civil and Political Rights." *UN OHCHR*, 16 Dec. 1966, https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

International Telecommunications Union, 2021, *Percentage of Individuals Using the Internet*.
Russia Country ICT Data 2021, https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2021/PercentIndividualsUsingInternet_Nov2021.xlsx.

"Internet Blackout Continues, Mobile Phone Service Restored in Sudan." *Dabanga*, 1 Nov. 2021, https://www.dabangasudan.org/en/all-news/article/internet-blackout-continues-mobile-phone-service-restored-in-sudan.

"Internet Censorship and Surveillance in Turkey." *European Digital Rights (EDRi)*, 12 Mar. 2014, https://edri.org/our-work/internet-censorship-surveillance-turkey/.

"IPI: At Least 241 Journalists Faced Trial in Turkey in 2021 – Nearly Half on Terrorism Charges." *International Press Institute*, 6 Feb. 2022, https://ipi.media/ipi-at-least-241-journalists-faced-trial-in-turkey-in-2021-nearly-half-on-terrorism-charges/.
Ireton, Cherilyn, and Julie Posetti. Journalism, fake news & disinformation: handbook for journalism education and training. Unesco Publishing, 2018.

"Issue Brief: Distinguishing Disinformation from Propaganda, Misinformation, and 'Fake News.'" *National Endowment for Democracy*, 10 Oct. 2018, https://www.ned.org/issue-brief-distinguishing-disinformation-from-propaganda-misinformation-and-fake-news/.

Jain, Anushka. "NCRB's National Automated Facial Recognition System." *Panoptic Tracker*, 16 Mar. 2022, https://panoptic.in/case-study/ncrbs-national-automated-facial-recognition-system.

"Junta Cronies Eye Telenor's Myanmar Business." *The Irrawady*, 11 Nov. 2021, https://www.irrawaddy.com/news/burma/junta-cronies-eye-telenors-myanmar-business.html.

Kapur, Manavi. "Rape Threats, Islamophobia, Casteism: Life of Female Indian Politicians on Twitter." *Quartz India*, 23 Jan. 2020, https://qz.com/india/1789905/amnesty-says-female-indian-politicians-face-massive-abuse-on-twitter/.

Kelly, Meg, et al. "'Burn It All down'. How Myanmar's Military Villages to Crush a Growing Resistance." *The Washington Post*, 23 Dec. 2021, https://www.washingtonpost.com/world/interactive/2021/myanmar-military-burn-villages-tatmadaw/.

Kemp, Simon. "Digital in Tanzania: All the Statistics You Need in 2021." *DataReportal*, 12 Feb. 2021, https://datareportal.com/reports/digital-2021-tanzania.

Kenyon, Miles. "Western Tech Used for Hacking in Turkey and Syria." *The Citizen Lab*, 9 Mar. 2018, https://citizenlab.ca/2018/03/western-tech-used-for-hacking-in-turkey-and-syria/.

Kottasová, Ivana. "An Entire Nation Just Got Hacked." *CNN*, 21 July 2019, https://edition.cnn.com/2019/07/21/europe/bulgaria-hack-tax-intl/index.html.

Krapiva, Natalia, et al. "Kazakhstan Internet Shutdowns and Protests: Timeline." *Access Now*, 12 Jan. 2022, https://www.accessnow.org/kazakhstan-internet-shutdowns-protests-almaty-timeline-whats-happening/.

Lipman, Masha, and Michael McFaul. "'Managed Democracy' in Russia: Putin and the Press." *Harvard International Journal of Press/Politics*, vol. 6, no. 3, June 2001, pp. 116–127, doi:10.1177/108118001129172260.

Lipman, Maria, and Tanya Lokot. "Disconnecting the Russian Internet: Implications of the New 'Digital Sovereignty' Bill." *PONARS Eurasia*, 21 Feb. 2019, https://www.ponarseurasia.org/disconnecting-the-russian-internet-implications-of-the-new-digital-sovereignty-bill/.

Mabika, Columbus. "Zimbabwe: 8 Air Force Officers Promoted." *The Herald*, 8 Jan. 2022, https://allafrica.com/stories/202201080120.html.

MacKinnon, R. (2013). *Consent of the networked: The worldwide struggle for internet freedom*. Basic Books.

Malsin, Jared, and Amira El-Fekki. "Egypt Is Arresting Doctors Who Raise Alarms Over Coronavirus Approach." *The Wall Street Journal*, 30 June 2020, https://www.wsj.com/articles/egypt-is-arresting-doctors-raising-alarms-over-coronavirus-approach-11593533638.

"Manifestantes Fazem Maior Protesto Nacional Contra o Governo Dilma [Protesters Stage Biggest National Protest against Dilma Government]." *Política*, 13 Mar. 2016, https://g1.globo.com/politica/noticia/2016/03/manifestacoes-contra-governo-dilma-ocorrem-pelo-pais.html. Accessed 16 Feb. 2022.

Marczak, Bill, et al. "BAD TRAFFIC Sandvine's PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads?" *Citizen Lab*, 9 Mar. 2018, https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/.

Marczak, Bill, et al. "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries." *The Citizen Lab*, 18 Sept. 2018, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.

Marczak, Bill, et al. "Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus." *The Citizen Lab*, https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/.

Marczak, Bill, et al. "Mapping Hacking Team's 'Untraceable' Spyware." *The Citizen Lab*, 17 Feb. 2014, https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/.

Marczak, Bill, et al. "Pegasus vs. Predator: Dissident's Doubly-Infected IPhone Reveals Cytrox Mercenary Spyware." *Citizen Lab*, 16 Dec. 2021, https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/.

"Maroc. La Condamnation D'el Mortada Iamrachen Doit Être Annulée [Morocco. The Conviction of El Mortada Iamrachen Must Be Annulled]." *Amnesty International*, 30 Apr. 2018, https://www.amnesty.org/fr/latest/news/2018/04/morocco-quash-conviction-of-el-mortada-iamrachen/.

"Maroc. Après Un Procès Entaché d'Irrégularités, Le Jugement En Appel Des Contestataires Du Hirak El-Rif Doit Déboucher Sur La Justice [Morocco. After a Trial Marred by Irregularities, the Appeal Judgment of the Hirak El-Rif Protesters Must Lead to Justice]." *Amnesty International*, 17 Dec. 2018, https://www.amnesty.org/fr/latest/news/2018/12/morocco-hirak-el-rif-appeal-must-deliver-justice-after-deeply-flawed-trial/.

Martins, Laís. "Autoridades Brasileiras Já Bloquearam Mais De 300 Jornalistas [Brazilian Authorities Have Already Blocked More than 300 Journalists]." *Núcleo Jornalismo*, 11 Jan. 2022, https://www.nucleo.jor.br/curtas/2022-01-11-bloqueio-jornalistas-twitter/. Accessed 16 Feb. 2022.

McGonagle, Tarlach, and Yvonne Donders, eds. *The United Nations and freedom of expression and information: critical perspectives*. Cambridge University Press, 2015.

"Measuring Digital Development: Facts and Figures 2021." *International Telecommunication Union*, 2021, https://www.itu.int/en/itu-d/statistics/pages/facts/default.aspx.

Media Institute for Southern Africa Zimbabwe. "Analysis of the Data Protection Act." *Kubatana*, 6 Dec. 2021, https://kubatana.net/2021/12/06/analysis-of-the-data-protection-act/.

Mitra, Esha, and Julia Hollingsworth. "India Cuts Internet around New Delhi as Protesting Farmers Clash with Police." *CNN*, 3 Feb. 2021, https://edition.cnn.com/2021/02/01/asia/india-internet-cut-farmers-intl-hnk/index.html.

"Moderating Online Content: Fighting Harm or Silencing Dissent?" *UN OHCHR*, https://www.ohchr.org/EN/NewsEvents/Pages/Online-content-regulation.aspx.

"Morocco and Western Sahara: End Prosecution of Activists under New Health Emergency Law." *Amnesty International*, 9 June 2020, https://www.amnesty.org/en/latest/news/2020/06/morocco-and-western-sahara-end-prosecution-of-activists-under-new-health-emergency-law/.

"Morocco: Freedom on the Net 2020 Country Report." Freedom House, https://freedomhouse.org/country/morocco/freedom-net/2020.

"Morocco: Government Must Fully Withdraw Draft Law on Social Media." *Article 19*, 10 July 2020, https://www.article19.org/resources/morocco-social-media/.

"Morocco's King Mohammed Pledges Constitutional Reform." *BBC*, 9 Mar. 2011, https://www.bbc.com/news/world-africa-12695092.

"Morocco: Police Violence a Test for Revised Constitution." *Human Rights Watch*, 11 July 2011, https://www.hrw.org/news/2011/07/11/morocco-police-violence-test-revised-constitution.

"Morocco: Shocking Verdict against Activists, a Journalist." *Human Rights Watch*, 10 Apr. 2019, https://www.hrw.org/news/2019/04/10/morocco-shocking-verdict-against-activists-journalist.

"Morocco/Western Sahara: Activist Targeted with Pegasus Spyware in Recent Months – New Evidence." *Amnesty International*, 9 Mar. 2022, https://www.amnesty.org/en/latest/news/2022/03/morocco-western-sahara-activist-nso-pegasus/.

Moyo, Dumisani. “A Vicious Online Propaganda War That Includes Fake News Is Being Waged in Zimbabwe.” *The Conversation*, 24 July 2018, https://theconversation.com/a-vicious-online-propaganda-war-that-includes-fake-news-is-being-waged-in-zimbabwe-99402.

Mwesigwa, Daniel. “Africa in the Crosshairs of New Disinformation and Surveillance Schemes That Undermine Democracy.” *CIPESA*, 9 Dec. 2019, https://cipesa.org/2019/12/africa-in-the-crosshairs-of-new-disinformation-and-surveillance-schemes-that-undermine-democracy/.

Mwesigwa, Daniel. “Uganda Abandons Social Media Tax but Slaps New Levy on Internet Data.” *CIPESA*, 1 July 2021, https://cipesa.org/2021/07/uganda-abandons-social-media-tax-but-slaps-new-levy-on-internet-data/.
“Myanmar Country Profile.” *BBC*, https://www.bbc.com/news/world-asia-pacific-12990563.

“Myanmar: End World’s Longest Internet Shutdown.” *Human Rights Watch*, 19 June 2020, https://www.hrw.org/news/2020/06/19/myanmar-end-worlds-longest-internet-shutdown.

“Myanmar: Post-Coup Legal Changes Erode Human Rights.” *Human Rights Watch*, 2 Mar. 2021, https://www.hrw.org/news/2021/03/02/myanmar-post-coup-legal-changes-erode-human-rights.

“Myanmar: What Has Been Happening since the 2021 Coup?” *BBC*, 1 Feb. 2022, https://www.bbc.com/news/world-asia-55902070.

Nabben, Kelsie, et al. “The Four Internets of COVID-19: The Digital-Political Responses to Covid-19 and What This Means for the Post-Crisis Internet.” *2020 IEEE Global Humanitarian Technology Conference (GHTC)*, 2020, pp. 1–8., https://doi.org/10.1109/ghtc46280.2020.9342859.

Nachemson, Andrew. “Why Is Myanmar’s Military Blocking the Internet?” *Al Jazeera*, 4 Mar. 2021, https://www.aljazeera.com/news/2021/3/4/myanmar-internet-blackouts.

Nakashima, Ellen. “Report: Web Monitoring Devices Made by U.S. Firm Blue Coat Detected in Iran, Sudan.” *The Washington Post*, 8 July 2013, https://www.washingtonpost.com/world/national-security/report-web-monitoring-devices-made-by-us-firm-blue-coat-detected-in-iran-sudan/2013/07/08/09877ad6-e7cf-11e2-a301-ea5a8116d211_story.html.

“نوال بنعيسى في قلب العاصفة بعد اتهامها بـ’بيع الماتش‘ والأخيرة ترد [Nawal Benaissa Is in the Middle of the Storm after Being Accused of ‘Selling the Match’, and the Latter Responds].” *Al Maghrabi Al Yaoum*, 29 Sept. 2017, https://almaghribialyaoum.com/نوال-بنعيسى-في-قلب-العاصفة-بعد-اتهامها/.

Noack, Rick, and Siobhán O’Grady. “How Ecuador Soured on Assange.” *The Washington Post*, 11 Apr. 2019, https://www.washingtonpost.com/world/2019/04/11/how-ecuador-soured-assange/.

Nyabola, Nanjala. *Digital democracy, analogue politics: How the Internet era is transforming politics in Kenya.* Zed, 2018.

Oates, Sarah. *Revolution stalled: The political limits of the Internet in the post-Soviet sphere*. Oxford University Press, 2013.

Odilla, Fernanda. “5 Anos Depois, o Que Aconteceu Com as Reivindicações Dos Protestos Que Pararam o Brasil Em Junho De 2013? [5 Years Later, What Happened to the Claims of the Protests That Stopped Brazil in June 2013?].” *BBC Brasil*, 9 June 2018, https://www.bbc.com/portuguese/brasil-44353703. Accessed 16 Feb. 2022.

Osman, Nadda. “Egypt: Tiktok Influencers Sentenced to up to 10 Years in Prison for Violating ‘Social Values’.” *Middle East Eye*, 21 June 2021, https://www.middleeasteye.net/news/egypt-tiktok-influencers-sentence-prison-mawada-adham-haneen-hossam.

Palacio, Emilio. “NO a Las Mentiras [NO to Lies].” *El Universo*, 6 Feb. 2011, https://www.eluniverso.com/2011/02/06/1/1363/mentiras.html.

Pandey, Neelam. “PM Modi Appeals for Peace in Riot-Hit Delhi, but BJP Leaders’ Tweets Are Far from Pacifying.” *ThePrint*, 26 Feb. 2020, https://theprint.in/politics/pm-modi-appeals-for-peace-in-riot-hit-delhi-but-bjp-leaders-tweets-are-far-from-pacifying/371608/.

“Parliament Proceedings | Over 72% Rise in Number of UAPA Cases Registered in 2019.” *The Hindu*, 10 Mar. 2021, https://www.thehindu.com/news/national/parliament-proceedings-over-72-rise-in-number-of-uapa-cases-registered-in-2019/article34029252.ece.

“Popularidade De Bolsonaro Cai Para 19%, Diz Pesquisa Da Consultoria Atlas [Bolsonaro’s Popularity Drops to 19%, Says Survey by Consultoria Atlas].” *Congresso Em Foco*, 29 Nov. 2021, https://congressoemfoco.uol.com.br/area/governo/popularidade-de-bolsonaro-cai-para-19-diz-pesquisa-da-consultoria-atlas/. Accessed 16 Feb. 2022.

“Press freedom.” *Merriam-Webster*. “https://www.merriam-webster.com/dictionary/freedom%20of%20the%20press.

“مجلس الصحافة والمطبوعات يعلق صدور صحيفتي الانتباهة والصيحة [The Press and Publications Council Suspends the Publication of the Al-Intibahah and Al-Sahih Newspaper].” *Sudan News Agency*, 20 Sept. 2021, https://www.suna-news.net/read?id=723089.

“Promotion and Protection of the Right to Freedom of Opinion and Expression.” *UN General Assembly*, 6 Sept. 2016, https://www.refworld.org/docid/57fb6b974.html.

Ratkiewicz, Jacob, et al. “Detecting and tracking political abuse in social media.” *Proceedings of the International AAAI Conference on Web and Social Media*. Vol. 5. No. 1. 2011.

“Report: Turkey to Establish Regulatory Body for Social Media.” *Bianet English*, 17 Aug. 2021, https://m.bianet.org/english/media/248915-report-turkey-to-establish-regulatory-body-for-social-media.

Rights and Risks Analysis Group, 2020, *India: Media’s Crackdown During COVID- 19 Lockdown*, http://www.rightsrisks.org/wp-content/uploads/2020/06/MediaCrackdown.pdf.

Rothrock, Kevin. “Russia: A Great Firewall to Censor the RuNet?” Global Voices, 10 July 2012, https://globalvoices.org/2012/07/10/russia-a-great-firewall-to-censor-the-runet/.

Rueckert, Phineas, and Cécile Schilis-Gallego. “HACKED: The Story behind the Israeli Spyware Targeting Moroccan Journalists.” *Forbidden Stories*, 22 June 2020, https://forbiddenstories.org/the-story-behind-the-israeli-spyware-targeting-moroccan-journalists/.

“Russia: Social Media Pressured to Censor Posts.” *Human Rights Watch*, 5 Feb. 2021, https://www.hrw.org/news/2021/02/05/russia-social-media-pressured-censor-posts.

Ryals, Mary R. “Africa Embraces Huawei Technology despite Security Concerns: Africa: DW.” *Softworld Net*, 8 Feb. 2022, https://softworldnet.com/africa-embraces-huawei-technology-despite-security-concerns-africa-dw/.

Ryan-Mosley, Tate. “Why You Should Be More Concerned about Internet Shutdowns.” *MIT Technology Review*, 9 Sept. 2021, https://www.technologyreview.com/2021/09/09/1035237/internet-shutdowns-censorship-exponential-jigsaw-google.

Said, Mohammed. Friedrich Ebert Stiftung, Rabat, pp. 1–140, *La Liberté De La Presse, La Déontologie Et Les Conditions d’Exercice Du Journalisme Au Maroc [Freedom of the Press, Ethics and the Conditions for Practicing Journalism in Morocco].*

Sakpa, Delali. “Tanzania Restricts Social Media during Election.” *Deutsche Welle*, 29 Oct. 2020, https://www.dw.com/en/tanzania-restricts-social-media-during-election/a-55433057.

Sarı, Mehmet Şafak. "What's behind Turkey's New Internet Law?" *Heinrich-Böll-Stiftung*, 28 Sept. 2020, https://tr.boell.org/en/node/21327.

Satariano, Adam, et al. "Kazakhstan's Internet Shutdown Offers Lessons for Russia-Ukraine Crisis." *The New York Times*, 18 Feb. 2022, https://www.nytimes.com/2022/02/18/technology/kazakhstan-internet-russia-ukraine.html.

Satariano, Adam. "Russia Intensifies Censorship Campaign, Pressuring Tech Giants." *The New York Times*, 26 Feb. 2022, https://www.nytimes.com/2022/02/26/technology/russia-censorship-tech.html.

Sauer, Pjotr. "Russia Bans Facebook and Instagram under 'Extremism' Law." *The Guardian*, 21 Mar. 2022, https://www.theguardian.com/world/2022/mar/21/russia-bans-facebook-and-instagram-under-extremism-law.

Scott-Railton, John, et al. "Nile Phish Large-Scale Phishing Campaign Targeting Egyptian Civil Society." *Citizen Lab*, 2 Feb. 2017, https://citizenlab.ca/2017/02/nilephish-report/.

"Servidores De 'Gabinete Do Ódio' Alimentavam Sites Bolsonaristas Que Lucravam Até R$ 100 Mil Por Mês ['Hate Cabinet' Servers Fed Bolsonarista Websites That Profited up to R$ 100 Thousand per Month]." *O Globo*, 4 Dec. 2020, https://oglobo.globo.com/politica/servidores-de-gabinete-do-odio-alimentavam-sites-bolsonaristas-que-lucravam-ate-100-mil-por-mes-24781083. Accessed 16 Feb. 2022.

"Shutdowns during Anti-CAA Protests ." *Internet Shutdowns Tracker*, Software Freedom Law Center, https://internetshutdowns.in/static-page/caa-protest/.

Siddique, Haroon. "Arron Banks's Lawsuit against Reporter a Freedom of Speech Matter, Court Hears." *The Guardian*, 14 Jan. 2022, https://www.theguardian.com/uk-news/2022/jan/14/arron-banks-carole-cadwalladr-libel-trial.

Singh, Vijaita. "1,100 Rioters Identified Using Facial Recognition Technology: Amit Shah." *The Hindu*, 12 Mar. 2020, https://www.thehindu.com/news/cities/Delhi/1100-rioters-identified-using-facial-recognition-technology-amit-shah/article31044548.ece.

Sodhi, Tanishka. "How the Hindu IT Cell Hounded a Muslim Journalist." *Newslaundry*, 1 Sept. 2021, https://www.newslaundry.com/2021/09/01/how-the-hindu-it-cell-hounded-a-muslim-journalist.

Soldatov, Andrei, and I. Borogan. 2015. The Red Web: *The Struggle between Russia's Digital Dictators and the New Online Revolutionaries*, 1st ed. New York, NY, Public Affairs.

Sozeri, Efe Kerem. "Turkey Paid Hacking Team 600K to Spy on Civilians." *The Daily Dot*, 7 July 2015, https://www.dailydot.com/debug/hacking-team-turkey.

"Sudan: Freedom in the World 2021 Country Report." *Freedom House*, https://freedomhouse.org/country/sudan/freedom-world/2021.

"Sudan : Media in Need of Rebuilding." *RSF (Reporters Without Borders)*, https://rsf.org/en/sudan.

"Sudan's Constitution of 2019." *Constitute Project*, 26 Aug. 2021, https://www.constituteproject.org/constitution/Sudan_2019.pdf?lang=en.

"Sudan's Military Fires on Anti-Coup Protesters, Killing Several." *Al Jazeera*, 25 Oct. 2021, https://www.aljazeera.com/news/2021/10/25/sudans-military-fires-on-anti-coup-protesters-killing-several.

"Surveillance Made in France." *Disclose*, 23 Nov. 2021, https://egypt-papers.disclose.ngo/en/chapter/surveillance-dassault.

Taye, Berhan, et al. “Internet Shutdown News and Report: A Year in the Fight to #KeepItOn.” *Access Now*, 3 Mar. 2021, https://www.accessnow.org/keepiton-report-a-year-in-the-fight/.

Threatened Voices, Global Voices, http://threatened.globalvoicesonline.org/about/.

Topcu, Elmas. “Turkey Marshals Law to Defend Recep Tayyip Erdogan’s Honor.” *Deutsche Welle*, 12 Feb. 2022, https://www.dw.com/en/turkey-marshals-law-to-defend-recep-tayyip-erdogans-honor/a-60733191.

“Turkey Case Study: Understanding Transnational Repression.” *Freedom House*, https://freedomhouse.org/report/transnational-repression/turkey.

“Turkey: Freedom in the World 2021 Country Report.” *Freedom House*, https://freedomhouse.org/country/turkey/freedom-world/2021.

“Turkey: Freedom on the Net 2021 Country Report.” *Freedom House*, https://freedomhouse.org/country/turkey/freedom-net/2021.

“Turkey Orders 532 Arrests in Military Probe over Gulen Links.” *Reuters,* 26 Apr. 2021, https://www.reuters.com/world/middle-east/turkey-orders-532-arrests-military-probe-over-gulen-links-anadolu-2021-04-26/.

“Turkey: Prominent Journalist Detained for Insulting President Erdoğan.” *The Guardian*, 23 Jan. 2022, https://www.theguardian.com/world/2022/jan/23/turkey-prominent-journalist-detained-for-insulting-president-erdogan.

“Turkey: Regulator Must Not Use License Powers to Pressure International Media.” *International Press Institute*, 9 Feb. 2022, https://ipi.media/turkey-regulator-must-not-use-license-powers-to-pressure-international-media/.

“Turkey’s Media Watchdog Probes Anchor over Criticism of Govt’s Economic Policies.” *Duvar English*, 21 Jan. 2022, https://www.duvarenglish.com/turkeys-media-watchdog-probes-anchor-selcuk-tepeli-over-criticism-of-govts-economic-policies-news-60192.

“Turkey’s Press Freedom Crisis Compounded by Increasing Digital Censorship.” *International Press Institute*, 9 Oct. 2021, https://ipi.media/turkeys-press-freedom-crisis-compounded-by-increasing-digital-censorship/.

“Turkish Prosecutors Seek Jail Term for Journalists for ‘Insulting’ President’s Son in News Reports.” *Duvar English*, 9 Feb. 2022, https://www.duvarenglish.com/turkish-prosecutors-seek-jail-term-for-journalists-for-insulting-presidents-son-bilal-erdogan-in-news-reports-news-60335.

“Twitter, FB and Others Remove Nearly 100 Posts after Govt Order.” *Times of India*, 25 Apr. 2021, https://timesofindia.indiatimes.com/india/twitter-fb-and-others-remove-nearly-100-posts-after-govt-order/articleshow/82242666.cms.

“Two Thirds of the World’s School-Age Children Have No Internet Access at Home, New UNICEF-ITU Report Says.” *UNICEF*, 1 Dec. 2020, https://www.unicef.org/eap/press-releases/two-thirds-worlds-school-age-children-have-no-internet-access-home-new-unicef-itu.

Uğurtaş, Selin. “New Powers of Turkey’s Media Watchdog Threaten Last Bastion of Free Press: The Internet.” *Free Turkey Journalists*, 22 Oct. 2019, https://freeturkeyjournalists.ipi.media/new-powers-of-turkeys-media-watchdog-threaten-last-bastion-of-free-press-the-internet/.

“UNITAMS Releases 7-Point Note to Explain Initiative to Achieve Transition in Sudan.” *Sudan Tribune*, 13 Jan. 2022, https://sudantribune.com/article254014/.

Unver, Akin. “The Logic of Secrecy: Digital Surveillance in Turkey and Russia.” Turkish Policy Quarterly, 28 Sept. 2018, http://turkishpolicy.com/article/923/the-logic-of-secrecy-digital-surveillance-in-turkey-and-russia.

"US Urges Turkey to Respect Freedom of Press after Move against Int'l News Websites." *Duvar English*, 11 Feb. 2022, https://www.duvarenglish.com/us-urges-turkey-to-respect-freedom-of-press-after-move-against-intl-news-websites-news-60353.

Varadarajan, Siddharth. "Revealed: How The Wire and Its Partners Cracked the Pegasus Project and What It Means for India." *The Wire*, 30 July 2021, https://thewire.in/media/revealed-how-the-wire-partners-cracked-pegasus-project-implications-india.

Weise, Zia. "Turkey Once Had a Free Press - Even under Erdogan." *The Atlantic*, 23 Aug. 2018, https://www.theatlantic.com/international/archive/2018/08/destroying-free-press-erdogan-turkey/568402/.

"Where Is Azory Gwanda?" *Committee to Protect Journalists*, https://cpj.org/whereisazory/.

Wijermars, Mariëlle, and Katja Lehtisaari, eds. Freedom of expression in Russia's new mediasphere. Routledge, 2019.

Winter, Brian. "Revisiting Brazil's 2013 Protests: What Did They Really Mean?" *Americas Quarterly*, 1 Mar. 2017, https://www.americasquarterly.org/article/revisiting-brazils-2013-protests-what-did-they-really-mean/. Accessed 16 Feb. 2022.

Woodhams, Samuel, and Simon Migliano. "The Global Cost of Internet Shutdowns." *Top10VPN*, 21 Mar. 2022, https://www.top10vpn.com/research/cost-of-internet-shutdowns/.

"The World Bank In Myanmar." *World Bank*, https://www.worldbank.org/en/country/myanmar/overview.

Xavier, John. "India's New Digital Media Rules Will Harm Open Internet: Mozilla." *The Hindu*, 4 Mar. 2021, https://www.thehindu.com/sci-tech/technology/indias-new-digital-media-rules-will-harm-open-internet/article33987347.ece.

Yaman, Alev. 2014, *Surveillance, Secrecy and Self Censorship: New Digital Freedoms Challenges in Turkey*, https://pen-international.org/app/uploads/Surveillance-Secrecy-and-Self-Censorship-New-Digital-Freedom-Challenges-in-Turkey.pdf.

Zanini, Fábio. "Sob Tensão, Democracia é Frágil e Requer Defesa, Dizem Representantes Da Política, Economia e Sociedade Civil [Under Tension, Democracy Is Fragile and Requires Defence, Say Political, Economic and Civil Society Representatives]." *Folha De S.Paulo*, 27 Feb. 2021, https://www1.folha.uol.com.br/poder/2021/02/sob-tensao-democracia-e-fragil-e-requer-defesa-dizem-representantes-da-politica-economia-e-sociedade-civil.shtml. Accessed 16 Feb. 2022.

Zetter, Kim. "American Gets Targeted by Digital Spy Tool Sold to Foreign Governments." *Wired*, 4 June 2014, https://www.wired.com/2013/06/spy-tool-sold-to-governments.

Zetter, Kim. "Hacking Team Customer in Turkey Was Arrested for Spying on Police Colleagues [or: The Spy Story That Spun a Tangled Web]." *Zero Day (Substack)*, 8 Sept. 2021, https://zetter.substack.com/p/hacking-team-customer-in-turkey-was?s=r.

"Zimbabwe Imposes Internet Shutdown amid Crackdown on Protests." *Al Jazeera*, 18 Jan. 2019, https://www.aljazeera.com/news/2019/1/18/zimbabwe-imposes-internet-shutdown-amid-crackdown-on-protests.

Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* Profile Books, 2019.

GlobalVoices advox

The
Un~~freedom~~
Monitor