The Unfreedom Monitor

The Unfreedom Monitor

A Methodology for Tracking Digital Authoritarianism Around the World

OBSERVATORY REPORT

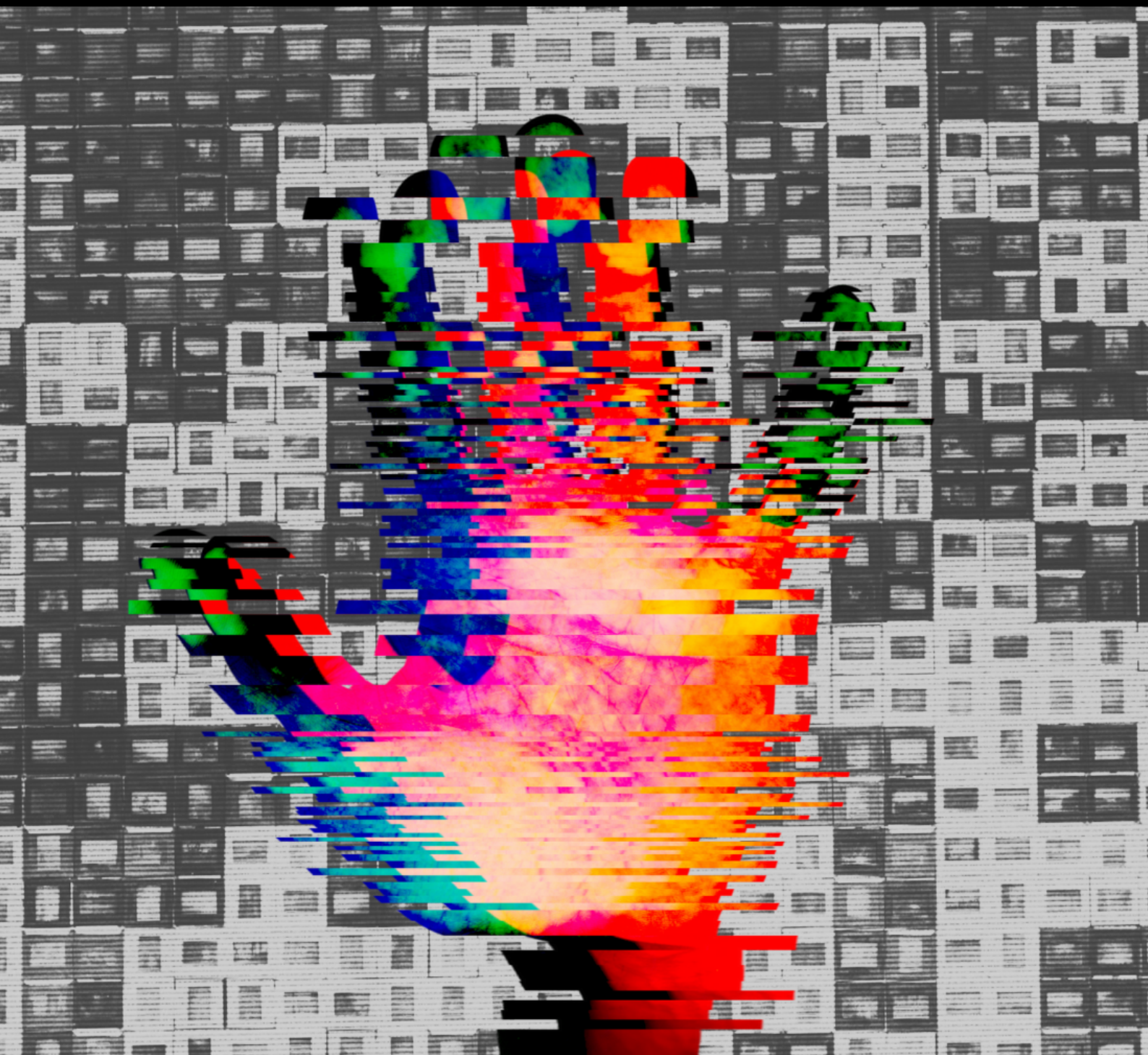


Table of Contents

Acknowledgements

The Unfreedom Monitor is the collective work of dozens of researchers and writers spread across multiple countries and time zones. 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 "Global Voices Advox." Any errors or omissions should also be addressed to Advox 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, as well as by other Global Voices supporters, a list of which can be found on our sponsors page.

Published by Advox under CC BY-NC 4.0

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

Published by Advox under CC BY-NC 4.0, August 2023
This work is licensed under a Creative Commons Attribution 4.0 International License

EXECUTIVE SUMMARY

Authoritarian regimes have a complicated relationship with media and communications technologies, using them to advance their messaging and propaganda goals while restricting access for others in order to shape and warp reality, conceal abuses, and maintain power. This dynamic has intensified with the growth of the internet and related digital technologies.

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 practices. The initial phase of the project tracks and documents key developments in digital authoritarianism in select countries. The project also articulates the technological and regulatory scaffolding that underpins authoritarianism, which restricts access to rights and narrows space for freedoms.

The Unfreedom Monitor aims to provide a foundation for understanding how authoritarian entities employ information technologies in real life. The research focuses on four main themes — data governance, speech, access, and information — all of which involve the shaping and control of information ecosystems to restrict freedoms and rights, limit privacy, and erode people's ability to participate meaningfully in civic life. We look at countries in context, and also examine how they are related to similar practices in other countries. Notably, we explore the reliance of many countries on transnational access to technologies, observing similar approaches and justifications in different contexts.

We examine the tools and methods used to restrict freedoms, target opposition movements, activists, journalists, and artists, and repress the universal rights of citizens at a mass scale, and the claims states make to persuade people to accept those restrictions. We explore, in depth, the narratives that authoritarian powers promote to justify their actions in the restricted information spaces these actions create, as well as narratives of resistance that opponents use to counter authoritarian claims.

The logic of the Unfreedom Monitor's approach is based on the insight that understanding narratives and illuminating the cognitive frames states use to justify restricting freedoms allows us to move beyond a piecemeal and atomised analysis of disinformation and misinformation. We use a method of analysis rooted in a taxonomy that helps researchers generate detailed descriptions and explanations of authoritarian incidents. This ensures a standardised approach to all incidents, facilitating impartial analysis and providing a basis for comparison.

Our research shows that technological approaches to the shaping of information ecosystems are not limited to censorship or regulatory restrictions. Authoritarians are investing in technologies of control and surveillance, from spyware that tracks the online behaviour of individuals, to mass online surveillance through deep packet inspection and similar technologies, to AI-based technologies such as facial recognition that allow states to engage in comprehensive surveillance of public spaces. Such technologies allow states to identify and follow individuals across both real-world and digital spaces, buttressing those technological choices with regulatory approaches that make resistance difficult.

Many states are also pursuing a range of information operations and campaigns, flooding information ecosystems with misinformation and disinformation and propaganda at scale, to push narratives designed to persuade people that authoritarian practices serve their interests. A comparative examination of these narratives demonstrates a persistent effort to justify authoritarian acts in terms of public safety, national security, public health, and other claimed benefits, as well as mobilising populist narratives that define in-groups and demonise enemies. Furthermore, information operations are themselves often defended by states with the deceptive argument that they should be protected as free expression.

Due to the complex, multisectoral nature of state use of technology, strategies for countering digital authoritarianism are not simple. They require expertise in multiple domains of knowledge, from international trade regulations to corporate governance of social media platforms, from international freedom of expression mechanisms to national-level implementation of media regulations, from an understanding of telecommunications infrastructure to user behaviour of mobile internet at national and local levels, as well as an understanding of national politics and how they intersect with international communications networks.

The Unfreedom Monitor foregrounds the study of narratives that underpin authoritarian practices. This emphasis helps communities at local, regional and global levels to identify when authoritarian practices are on the rise, and could inform strategies of resistance, as well as advocacy and policy responses. This publicly available research may also be used by various civil society actors such as journalists and academics to bolster their work. The study:

- Offers a language and taxonomy that facilitates analysis as a precursor to policy responses
- Identifies common approaches many states have taken to restrict freedoms
- Recognises that policy responses are often siloed by subject, initiative, technology, and legal jurisdiction
- Underscores the need to develop comprehensive policy responses that can address all vectors of repression
- Suggests that advocacy to restrain digital authoritarianism needs to include local, regional and international stakeholders

This report summarises the findings of the project after 18 months of research, and provides a roadmap for using the project's dataset. It should be read alongside the project's other key outputs, including a briefing note, country and topic studies, published stories, and a comprehensive dataset of incidents, media items, themes and narrative frames.

INTRODUCTION

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 20 countries.

Authoritarianism is characterised by a lack of accountability, transparency, and legitimacy in the exercise of power. Technologies can be said to enable authoritarian practices when they are employed without citizen oversight, public discussion about harms, or proportionality. In the project's initial briefing note, we cite the challenge of finding an appropriate balance in how to regulate or support information technologies as they relate to civic participation, 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."[1]

The Unfreedom Monitor combines research into regulatory and technological restrictions on rights and freedoms with information ecosystem analysis. With this approach, we aim to deepen understanding of the motivation, dynamics and possible future directions of digital authoritarianism globally, and to build a roadmap for research that can be applied in many country contexts. This report provides a theoretical and analytical framework for understanding this work.

SUMMARY OF OBSERVATIONS

Authoritarian practices are not strictly limited to authoritarian states; they are employed by regimes that span the political spectrum.

The research approach argues for expanding the understanding of key authoritarian strategies to include persuasion alongside coercion and cooptation, which are identified in academic literature as key approaches to consolidating power and building stability in authoritarian states.

States are not only restricting access to information technologies, but are also actively investing in technologies of control, as well as shaping media ecosystems.

States employ a range of strategies that often work in combination, such as: restricting information access, targeting expression, and pushing narratives.

State opacity about the extent of their repressive capacities is a feature, not a bug. This allows states to make claims about their capabilities that create fear and distrust even if inaccurate or untrue.

1. "The Unfreedom Monitor: A Methodology for Tracking Digital Authoritarianism Around the World," Global Voices Advox, April 2022, p. 12, https://advox.globalvoices.org/wp-content/uploads/2022/04/GV_Unfreedom_Monitor_Briefing_Note_Apr2022.pdf.

The combined use of information technologies to surveil, censor, and shape information ecosystems aid in "preventative repression," making resistance and opposition more difficult and costly.

Policy recommendations to help resist authoritarian practices face the complicated challenge of how to regulate dual-use and surveillance technologies that were developed for security and commercial applications, but that also facilitate authoritarian practices.

There is an active debate about whether surveillance for commercial or consumer purposes, border controls and policing is mostly or inherently authoritarian in practice.

PROJECT SCOPE

In the first phase of the Unfreedom Monitor, we articulated a theoretical framework to examine the use of technology to advance repressive political interests. This framework is articulated in the project's briefing note and encoded in the database taxonomy.

Working with local researchers and writers around the world, we then began studying and reporting on what we term "incidents" of authoritarian practice, which include actual harms to individuals and groups. We documented the information ecosystems affected by these incidents, and explained and contextualised the narratives employed by various actors to justify or counter them.

The Unfreedom Monitor publishes both country-level and thematic studies, and also produces journalistic stories that synthesise and draw from that analysis. The stories, studies and information in the dataset are referenced throughout this paper, available on the Unfreedom Monitor page.[2] The project has to date analysed technologically augmented restrictions on freedoms and rights in 20 countries, focused on the four key themes of the project: data governance, speech, information, and access to communications technologies.

The selection of the first 20 countries in the Unfreedom Monitor was influenced by a range of factors: government type; approach to human rights, including rankings in indexes, and approach to the use of communications and surveillance technologies. The countries are: Brazil, Cameroon, Ecuador, Egypt, El Salvador, Hong Kong, Hungary, India, Kazakhstan, Kenya, Kyrgyzstan, Morocco, Myanmar, Philippines, Russia, Sudan, Tanzania, Turkey, Venezuela and Zimbabwe.

Desk research into each country's history, regulatory approach, and practices provided a foundation for the study of incidents and media items. The researchers explored key themes, events, actors, and narrative frames to provide a framework for understanding how digital authoritarianism functions in real life.

A relational dataset of qualitative research and analysis was built using the database platform Airtable. We analysed 67 incidents; 1,239 media items that illustrate local perceptions and provide supporting documentation; 172 narrative frames; and four major themes.

2. Unfreedom Monitor, 2022-2023, https://advox.globalvoices.org/special/unfreedom-monitor/.

We continue to produce stories that synthesise the analysis, over 90 of which have been published at the time of this report. The data analysis and stories explain the incidents in detail, unpack the narratives being used to support or oppose authoritarian practices, illuminate specific histories, and discuss the actions of activists, politicians, and other figures of influence.

RESEARCH OBJECTIVES

The objective of the Unfreedom Monitor is to explain the dynamics of technologically augmented authoritarian practices by examining the narrative frames and themes that underpin claims about digital authoritarianism in national and transnational contexts. The Unfreedom Monitor dataset unpacks the stories governments tell about the nondemocratic application of power, how publics and civil societies receive and counter these stories, and how these stories are connected to other major events. The project aims to help readers understand the contextual shifts that might signal the emergence of digital authoritarianism, including shifts in narratives about key human rights concerns or the role of technology in public spheres.

The term "digital authoritarianism" describes the use of technology to advance repressive political interests. A related term, "networked authoritarianism," coined by Global Voices co-founder Rebecca MacKinnon, emphasises the idea that people can be co-opted into supporting authoritarian power by participating in networked information systems, for example, by giving up their privacy in order to access services, or by using heavily censored discussion platforms that distort available information.[3]

Authoritarian states do not simply want to restrict access to the internet, media and other communications technologies. Many states invest in communications technologies that work to curb freedoms. The use of these technologies, buttressed by regulation, create what Tiberiu Dragu and Yonatan Lupu call "preventative repression," which diminish the possibilities for civic action and participation.[4] Together, these practices create what we call an "enabling environment" for authoritarianism.[5]

Authoritarian practices are not purely confined to authoritarian regimes. Democratic states also use advanced technology to track and/or surveil citizens, spread mis- and disinformation, and disempower citizens' civic and political participation in ways not in alignment with core democratic values of accountability, legitimacy, and transparency.

3. Rebecca MacKinnon, "Liberation Technology: China's 'Networked Authoritarianism,'' Journal of Democracy, Volume 2, Issue 2, pp. 32-46, April 2011, https://muse.jhu.edu/article/427159.

4. Tiberiu Dragu, 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.

5. "The Unfreedom Monitor: A Methodology," p 13.

Nor is it only states that perpetrate digital authoritarianism: many political and corporate entities are implicated in its logic. Corporations located in democratic countries are key suppliers of these technologies. Users' identities, behaviour, location, opinions and attitudes are being tracked to the point of ubiquity, from CCTV cameras, doorbells and weight sensors, to machine visioning, facial recognition, and integration of artificial intelligence into a wide range of technology functions.

Technologically augmented authoritarianism is not only about the coercion and cooptation of citizens to accept nondemocratic governance.[6] It is often accompanied by efforts to shift perceptions of state power and governmental activities, and supported by narratives designed to diminish criticism or gain support. In our research, we have found that state-authored narratives that justify and build support for authoritarian practices are often opposed by countervailing narratives promoted by civil society and activists, or through critical analysis of the dominant narrative frames.

By understanding the processes through which technology is used to aid authoritarianism, and by describing the political actions that constitute those processes, we can start to decode the ways technologies are enabling the repression of rights and freedoms.

6. There is substantial political science literature that describe models of repression and cooptation in stable authoritarian regimes. See for example Xu Xu, "To Repress or Co-opt? Authoritarian Control in the Age of Digital Surveillance," American Journal of Political Science, Volume 65, Issue 2, April 2021, pp. 309-325, https://doi.org/10.1111/ajps.12514.

DATASET ROADMAP

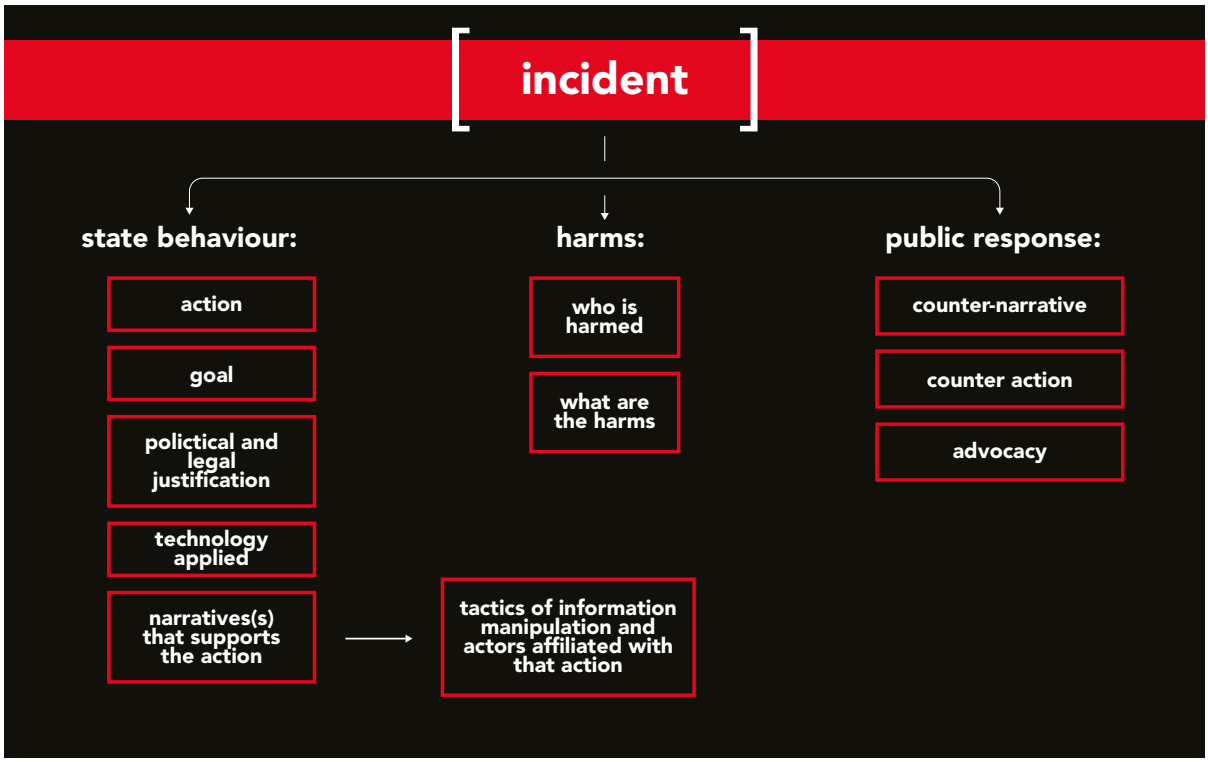
The dataset underlying the Unfreedom Monitor was built using the relational database Airtable, on the basis of Global Voices' Civic Media Observatory, which was developed in 2019 to investigate and decode how people understand information and create knowledge in complex and seemingly chaotic media ecosystems. The Observatory method was adopted in order to incorporate analysis of incidents and to document harms to individuals and groups. The dataset offers qualitative analysis of incidents, narratives and themes in editorial media, social media, other online media, and offline media. The research does not employ statistical methods and the data are not statistically representative: quantitative statements about the data refer only to the material in the set.

This report refers to an analysis completed between January 2022 and March 2023, focusing on incidents of digital authoritarianism in Brazil, Cameroon, Ecuador, Egypt, El Salvador, Hong Kong, Hungary, India, Kazakhstan, Kenya, Kyrgyzstan, Morocco, Myanmar, Philippines, Russia, Sudan, Tanzania, Turkey, Venezuela and Zimbabwe, as well as on cross-cutting themes.

Country research was carried out in three stages, each lasting approximately six months. In the first phase, we analysed 11 countries and produced background papers by country as well as on cross-cutting themes. Simultaneously, we began compiling analyses of incidents, narratives and media items in the dataset. As a consequence, the briefing note and the first 11 background papers do not feature incidents. In stage two, we expanded the research on a subset of the first 11 countries, and added three more. In stage three, we added six more countries.

We refer to material from the dataset throughout this report in hyperlinks and endnotes. We reference media item entries in the dataset by author, publication, date, and a hyperlinked item number in the dataset. We refer to entries in other tables in the dataset by title and hyperlinked short code. The full dataset is publicly available on Airtable.

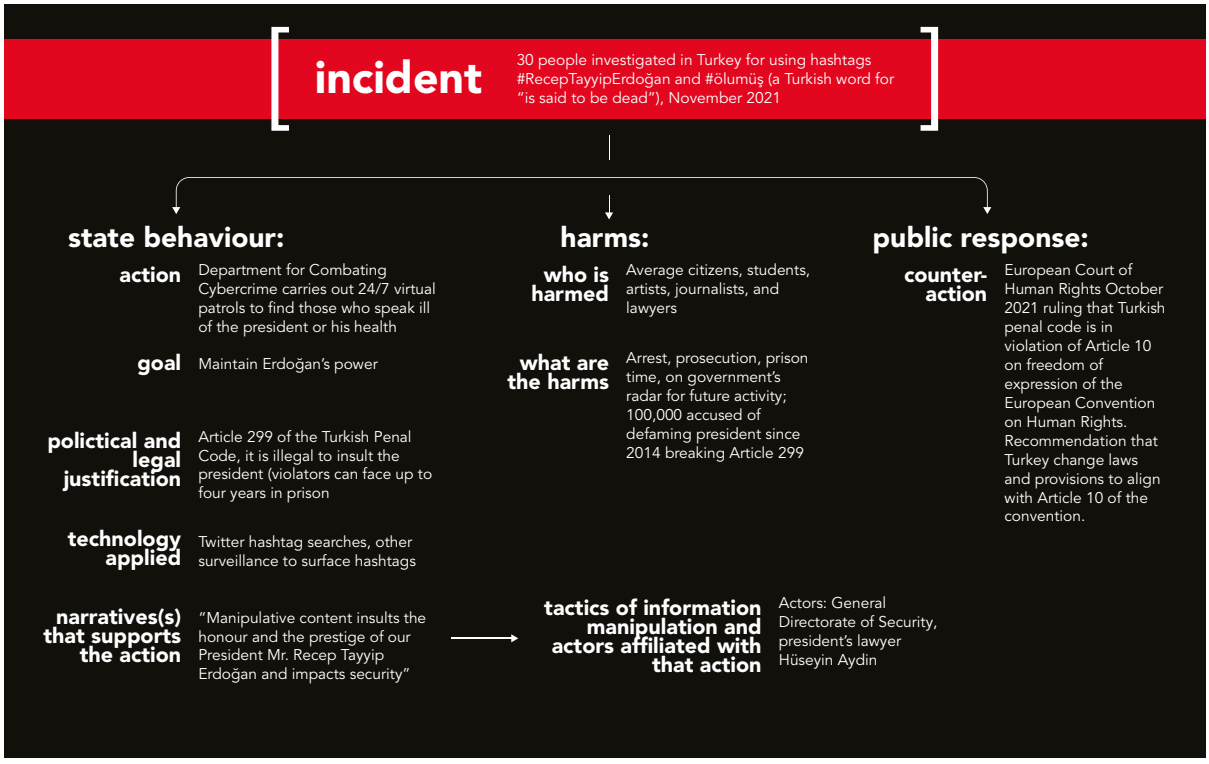
Following are visualisations of the research data workflow. They explain the relationship between incidents, state behaviours, harms and public reaction or resistance.



The Unfreedom Monitor

Data workflow

We begin analysis at the incident level and then enter data based on the state, harms and public response



The Unfreedom Monitor

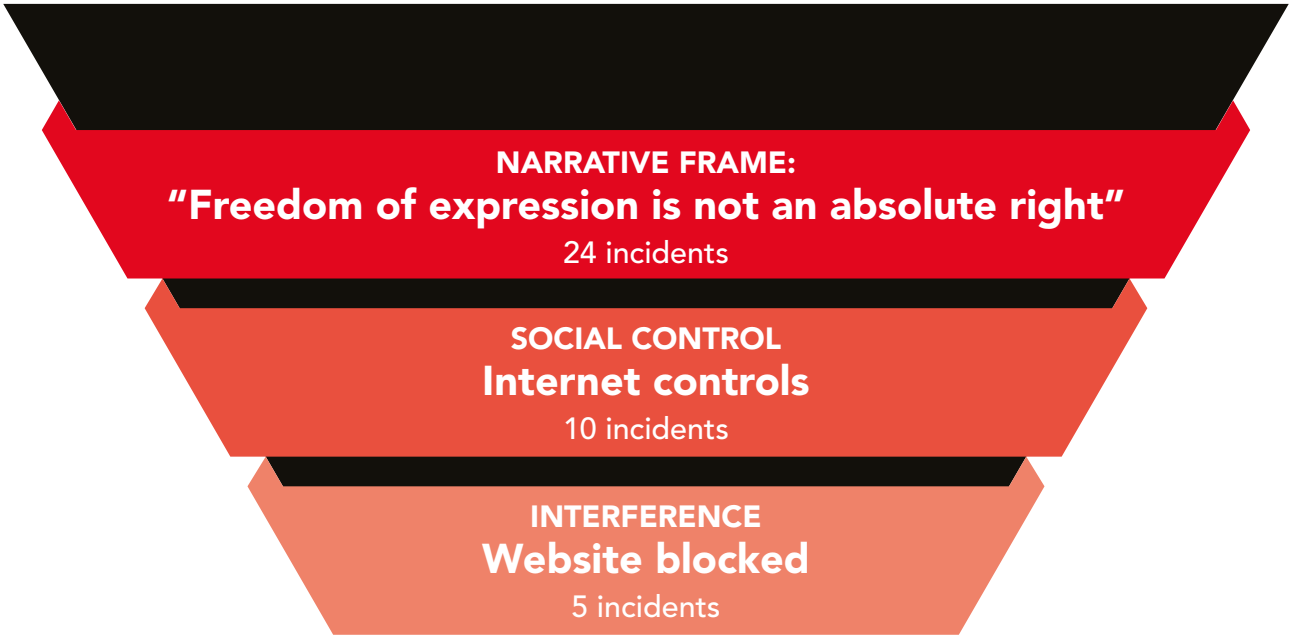
Example: Turkey

From the article "In Turkey, 30 people face investigation over social media posts that 'insulted the president'"

POINTS OF ENTRY

Airtable is a relational database that offers rich interlinking within and between tables, allowing researchers to build multiple pathways between data points. Users of the dataset can explore the data from many starting points, including by incident, theme, country, narrative frame, media source, media item, harms, and type of social control.

Airtable also allows users to build custom filters using multiple conditions, to create fine-grained slices of data. For example, a user can filter for matches of narrative frames and type of social control to examine how specific frames are linked to particular state responses. Filtering for the narrative "Freedom of expression is not an absolute right" and the social control "Internet controls," for instance, yields 10 incidents. Adding a third condition, "Type of interference: website blocked" further refines the data subset to five incidents.



1. **Independent UN experts condemn internet and communication shutdown in Kashmir.**
2. **Venezuelan regional elections spark rise of website and digital media blocks.**
3. **Turkish state grants the Turkish Football Federation the right to block websites.**
4. **Court blocks access to news about suicide of a student.**
5. **Philippine government agency blocks websites of 2 media outlets, 25 others.**

Below we highlight the key tables in the dataset, and explain their use.

Narrative frames

The dataset includes 172 narrative frames.[7] Narrative frames are claims made by various actors to influence discussions about events and phenomena. Frames emerge out of researchers' examination of media items and the perspectives and ideologies that exist in information ecosystems. Each narrative frame is accompanied by a detailed description of its context and meaning. They are linked in the dataset to analysis of relevant media items, to themes, and to incidents. Narrative frames that share commonalities are grouped under the heading of Parent Frames that feature in multiple countries and contexts, such as "Justifications for internet controls and content blocking" or "Arguments that defend surveillance." The dataset also includes counter-narratives arguing in support of freedoms, such as "Arguments in favor of a free press."

It is important to understand that the narrative frames in this dataset are a product of the researchers' focus. Researchers scan available information based on their subject matter, regional, and linguistic expertise using a range of methods, from open internet search tools, to CrowdTangle, to digital investigation techniques. Narrative frames are reviewed and approved by the project's research manager and editors before they are added to the dataset, which helps avoid confirmation bias and ensures that narrative frames are within the scope of the project. Note that quantitative data attached to narratives in the dataset are not statistically meaningful, but are meant to help the reader navigate the dataset.

Themes

Researchers work within four cross-cutting themes: **data governance**, **speech**, **access**, **information**:

Data governance concerns practices such as surveillance and privacy violations. Surveillance as a digital authoritarian practice has emerged in countries regardless of whether they are considered democratic or autocratic. Many companies that produce surveillance technologies are based in economically advanced countries with democratic systems of governance. Many of the countries in this study have been linked to purchases of malware, spyware and other cyber-surveillance weapons, such as NSO Group's Pegasus software. Data governance also encompasses subjects such as COVID-19 contact tracing technologies, national registration and digital I.D. systems, and the use of facial recognition and AI-powered CCTV.

Constraining **speech** is an important aspect of digital authoritarianism that includes restrictions on freedom of expression, freedom of opinion, and freedom of information. In many countries in our study — for example, Ecuador, Morocco, Russia and Turkey — media laws have placed heavy constraints on freedom of expression, especially online. Such regulations are digital authoritarian in nature both in that they control expression in digital spaces, and in that they often are enforced by employing mass online tracking and surveillance technologies. Many media laws don't apply to just journalists and media

7. Unfreedom Monitor dataset, Narrative Frames table.

organisations, but also to all people online within national jurisdictions, and sometimes even to national citizens residing in other states. In Egypt, for example, at least 500 websites have been blocked since 2017, and social media policing is widespread. Individuals in Morocco, too, have been prosecuted for the content of their Facebook posts under the country's media laws.

If users do not have **access** to the internet and telecommunications services, their ability to engage in civic and political discourse is drastically reduced. Governments have implemented a range of access restrictions on communications technologies during times of upheaval, using legislation and regulation, punitive taxation, and technological restrictions such as blocking social media platform access, bandwidth throttling, and full internet shutdowns. Recent examples of events precipitating access restrictions include the military coup in Myanmar, citizen protests in India, and the run-up to elections in Tanzania. Access restrictions stifle the free flow of information and have costly economic side effects.

States and government-affiliated bodies also seek to control **information** by shaping information ecosystems, running influence operations, conducting large-scale disinformation campaigns, and engaging in other activities that influence what people know and believe. In Brazil, for example, former president Jair Bolsanaro was linked to a government-funded "digital militia" that has spread false news about COVID-19-related topics. Influencers in many countries have been paid to spread unverified information. In India, Prime Minister Narendra Modi and his BJP party and its followers have long used their social media presence to promote their brand and troll religious and political minorities.

The four cross-cutting themes each have sub-themes. The sub-themes are extensible, and are based on what researchers actually found during their analysis; as such, they can be expanded or elaborated on in future research. They are linked in the dataset to analysis of specific media items, which allows users of the dataset to sort media items, narratives and incidents by sub-theme. Themes and sub-themes were defined by the research team during a scoping exercise and their definitions are included in the dataset, found in appendix A. Theme definitions were tested and refined during data gathering and analysis. The following chart depicts the full menu of themes.

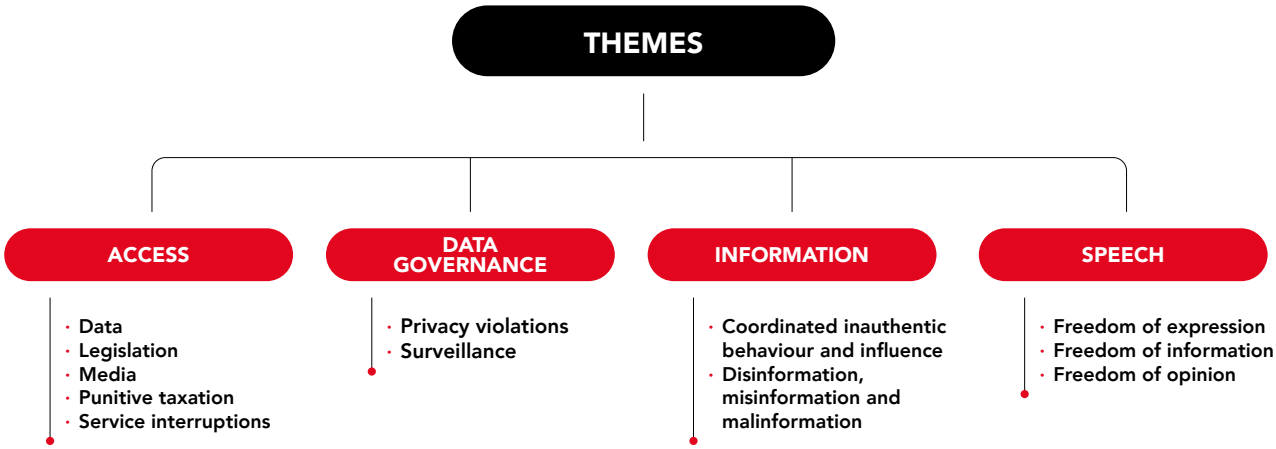


Table 01: Taxonomy of themes

Incidents

Incidents are instances of digital authoritarian practice. In the context of the dataset, an incident may be as narrow in scope as the arrest of a single individual, or as wide as the invasion of another country; what incidents have in common is an underlying logic that reinforces a system of power.

The focus on incidents is meant to illuminate how technologies support or enable actual authoritarian practices and cause harm. Researchers select at least two incidents per country. The incidents table includes detailed descriptions of events, lists of relevant actors, technologies, regulations, and individuals or groups harmed, and instances of resistance and advocacy, where relevant. We link incidents to separate tables of media items, narrative frames, themes, and people and entities of interest. We examine incidents and accompanying media items by looking both at what governments say about them, and how local communities, individuals, civil society and other groups respond. Examples of incidents include "Myanmar's ruling junta expands the rollout of surveillance cameras to more cities," and "Blocking of Wikipedia in Russia."

Also included in the incidents table is a selection of common technological approaches that authorities use to implement rights-restricting practices, which we call "social controls." Researchers append these to specific incidents using an extensible menu of options based on analysis by the research team of frequently used forms of social control. In many of the incidents we document, authoritarian actors will combine several approaches. The following chart depicts the full menu. Definitions can be found in the Appendix.

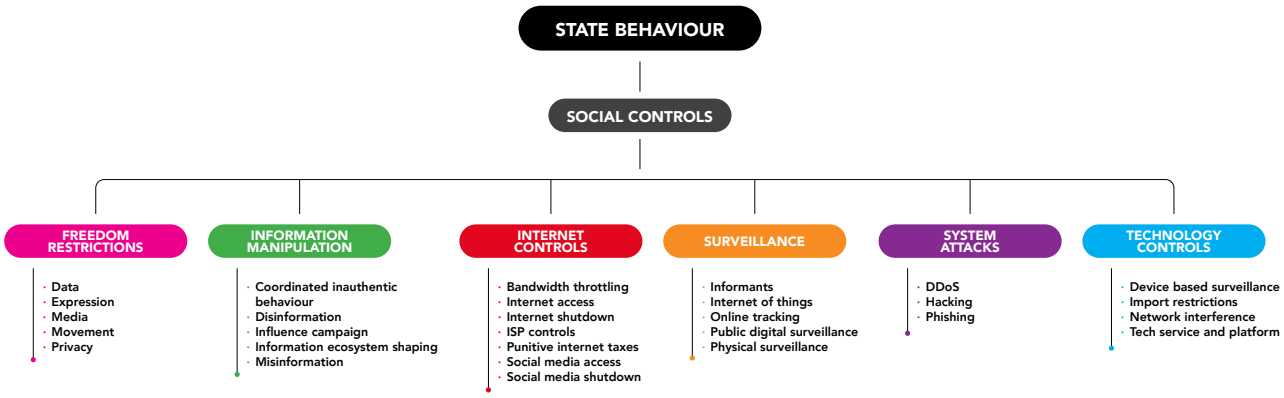
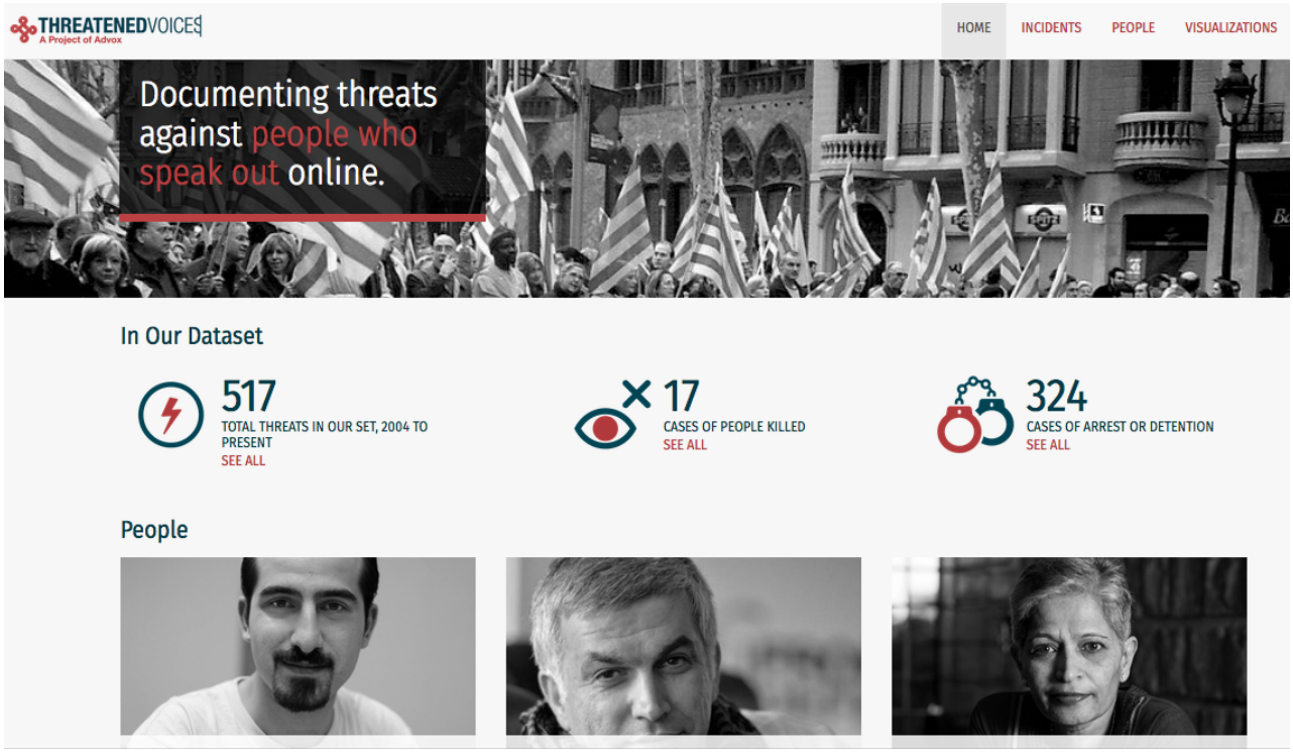


Table 02: Taxonomy of social controls

The database taxonomy is designed to allow more granular analysis and description of the entities responsible for perpetrating incidents of authoritarianism. Options include: state authority, political party, parastatal, corporate, unknown, private individual, and others. The database also includes fields where researchers can name the authority in question and describe their actions in detail.

When analysing incidents, researchers record not only the actions of the entities responsible for restricting rights and freedoms, but also the actual harm done to individuals, groups, and societies as a whole. The Unfreedom Monitor's harms taxonomy is based on Threatened Voices, a Global Voices research project which ran from 2009 to 2016 and documented nearly 1,000 cases of attacks on online expression. Threatened Voices was designed and built with the input of numerous human rights and freedom of expression partner organisations, including the Berkman Klein Center for Internet & Society, Article 19, the Committee to Protect Journalists, UNESCO, the Electronic Frontier Foundation, and the UN High Commission for Human Rights. The harms portion of the dataset includes both extensible menus that researchers use to categorise incidents, and free text fields for detailed descriptions of events. The top-level harms are: technical interference, intimidation, physical harm, and judicial threat. The following chart depicts the full menu of options.



Screenshot of Threatened Voices website, 2017

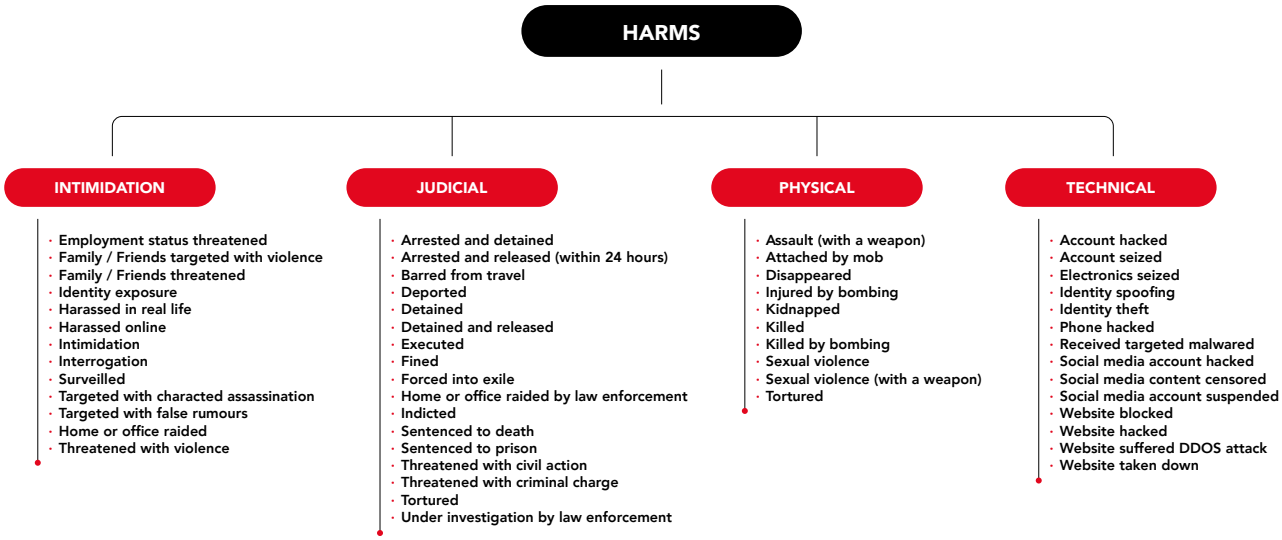


Table 03: Taxonomy of harms

Media items

To understand how narratives function in information ecosystems and which themes are prevalent, researchers perform in-depth readings on media items. Media items may be any piece of information that is relevant to the incident. They are categorised in the dataset as "editorial media," "social media," "online: other" and "offline: other." They include media sources such as news articles, social media posts, academic writing, policy papers, propaganda videos, but also promotional materials, commercial merchandise, and so forth. For each incident, researchers identify 15–20 media items that exemplify and illuminate the narratives in media discourse, and provide background information and context. In analysing media items, researchers explore context, subtext, accuracy, and credibility. Media items are also assigned a Civic Impact Score, a ranking from -3 to +3 that describes the civic value of the item, based on human rights norms. The score is accompanied by a written explanation for the choice. We describe the Civic Impact Score in detail in the Appendix. As of May 2023, the Unfreedom Monitor dataset contains 1,239 items composed primarily of social media and editorial media items.

Media sources and platforms

The dataset contains 454 media sources. A media source is added to the dataset once a researcher has selected a media item from that source. Media source entries include descriptions of the source's political and financial influences, ownership, editorial bias, and content policies, to help the reader understand the intentions, context and subtext underlying media items from that source. Also included in the media sources list are platforms, discussion forums, advocacy groups and propaganda agents.

People and entities of interest

The database contains a table that lists and describes key actors linked to incidents, such as political figures, journalists, activists, propagandists, regulators, technology companies and representatives, coalitions, organisations, associations, ministries, judicial bodies, and international organisations.

Synthesis table

This table offers researchers a structure for summarising complex stories into simple descriptive categories: what is happening, why is the issue or trend important, and what are the potential impacts. Researchers often put items into the synthesis table as a precursor to writing a story or newsletter, to facilitate sharing on social media platforms, or to provide further reporting on an incident based on new developments. The table contains 56 records as of May 2023.

UNDERSTANDING THE RELATIONSHIPS BETWEEN TABLES

The following charts and graphs illuminate the relationship between the incidents and other key tables in the dataset, including themes, narrative frames, and harms.

THEMES AND INCIDENTS

All incidents in the dataset fit within at least one of the four primary themes. The distribution of themes by incident reflects an evaluation of how authoritarianism is developing in each country, rather than a quantitative indicator of wider trends.

Incidents involving threats to speech provide a useful example, as they are well represented in the dataset: 42 of the 67 incidents and 1,108 of the media items are related to speech. Perhaps this is unsurprising, as speech rights and freedoms are at the heart of many governmental efforts to shape information spaces, control access and surveil activities of populations.

Attacks on freedom of expression, a sub-theme of the Speech theme, are abundant in the dataset: the researchers categorised 37 of the incidents as a restriction on expression. A number of these were arrests or attacks on small groups or numbers of individuals that appear designed to make an example of them, or to illustrate a technological or legal approach. Examples include the arrest of a prominent journalist in Cameroon, the arrest and charging of a dissident leader in Kazakhstan, the sentencing of a Rwandan critic to a 15-year prison sentence, and the El Salvador government's threat to sue two journalists.[8]

Numerous incidents focus on mass arrests for acts of expression, in which the targets were identified through the monitoring of online platforms. Examples include China's detention of 897 people for sharing or expressing ideas about COVID-19, Turkey's Interior Ministry's detention of 400 people for comments critical of the government's response to COVID-19, or Kyrgyzstan's arrest of 27 people for criticising the government's peace deal with Uzbekistan on social media.[9]

It is common for incidents to relate to more than one theme: only 13 out of the 67 incidents focus exclusively on one theme. The fact that incidents often involve multiple themes helps us to see that the efforts of states to restrict rights and freedoms involves multiple domains. For example, Kyrgyzstan has been surveilling an opposition group, which is a data governance issue, while also restricting their opinions and expression, which is an issue of speech.[10]

8. Unfreedom Monitor dataset, "Cameroon journalist jailed for reports and social media posts about the ongoing Anglophone Conflict," UM_Incident_69, "In Kazakhstan: dissident arrested and charged with spreading 'false information' on social media," UM_Incident_70, "Popular Rwandan Government Critic on YouTube sentenced to 15 years," UM_Incident_58, "Bukele's government threatens lawsuit against two women journalists," UM_Incident_38.

9. Unfreedom Monitor dataset, "China detained 897 people within the first two months of the COVID-19 pandemic for their online speech or information-sharing," UM_Incident_51, "Turkey's Interior Ministry detains 400 social media users for COVID-19 comments," UM_Incident_18, "Kyrgyzstan: Mass detention of critics who protested on social media against the controversial border deal with Uzbekistan," UM_Incident_59

10. UM_Incident_56.

Themes	Number of incidents reflecting theme[11]
Data governance	26
Sub-themes: Privacy violation | Surveillance	
Speech	42
Sub-themes: Freedom of opinion | Freedom of expression | Freedom of information	
Access	32
Sub-themes: Punitive taxation | Service interruptions | Legislation	
Information	17
Sub-themes: Coordinated inauthentic behaviour and influence campaigns | Disinformation, misinformation and malinformation	

Table 04: Themes and incidents

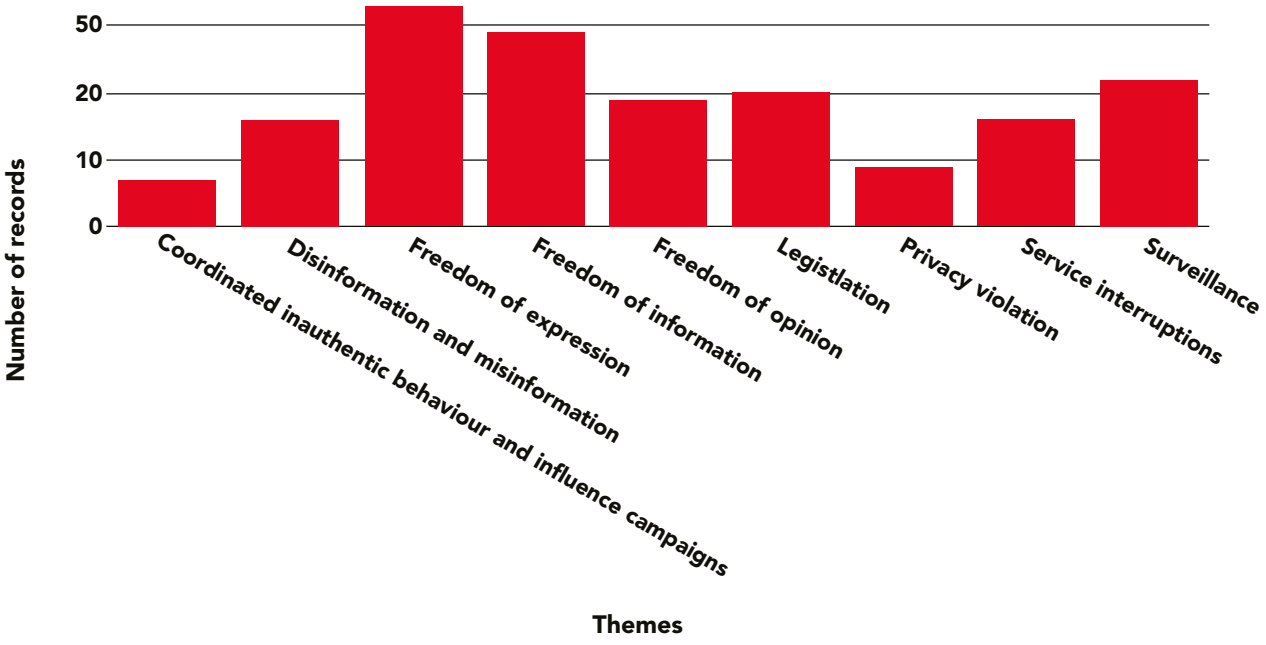


Table 05: Sub-themes and incidents

Researchers also associate themes with media items in the dataset, which facilitates thematic sorting across all countries. Researchers analyse approximately 15–20 media items per incident. Filtering for freedom of expression by media item, keeping with our example above, yields 546 media items.

11. Percentages do not total to 100 percent as incidents can be associated with multiple themes.

Themes	Number of sub-themes	Number of media items referencing theme[12]
Data Governance	1	531
Speech	3	1,108
Access	3	429
Information	2	424

Table 06: Themes and media items

SOCIAL CONTROLS AND INCIDENTS

Technologically enabled authoritarian practice is, by design, sometimes difficult to see and therefore to understand. One signifier of authoritarian approaches is opacity in the deployment and function of the technologies used to surveil, monitor behaviour, restrict actions, and shift opinions, sometimes accompanied by misinformation about the actual technical capacities of the state.

Looking in detail at the social controls employed to implement authoritarian practices helps us examine how states exercise power. In the dataset, many of the incidents show authoritarian actors employing multiple social controls in combination to restrict freedoms.

Even in highly visible instances of authoritarian acts, the actual capabilities of the state may be unclear. This is the situation with Russia, for example, which has slowly built up the technological and bureaucratic capacity to censor platforms and restrict information access in the way its enacted laws require. Whether the claims Russia makes about its capabilities are strategic preventative repression or a failure of intent depends on the timeline, as Russia's capabilities have improved since 2019, when it rolled out a Deep Packet Inspection system that expanded its capacity to see data online, and to block internet traffic.[13]

Table 07 depicts the complete taxonomy of social controls. Here we show the number of incidents associated with top level controls. In many incidents, authoritarians are applying more than one type of social control. Freedom restrictions is the most common control in the data set, pointing to the frequent use of regulatory, judicial and legal approaches documented in the dataset. Of the 49 incidents of freedom restrictions, 39 of them involve restrictions on freedom of expression. This is more than half of the full dataset of incidents.

The second-most prevalent social control in the dataset is surveillance, which appears in 38 incidents, of which 24 involve public digital surveillance.

12. Percentages do not total 100 percent as media items can be associated with multiple themes.

13. Andrei Zakharov and Ksenia Churmanova, "How Russia tries to censor Western social media," BBC Russia, December 2021, https://www.bbc.com/news/blogs-trending-59687496.

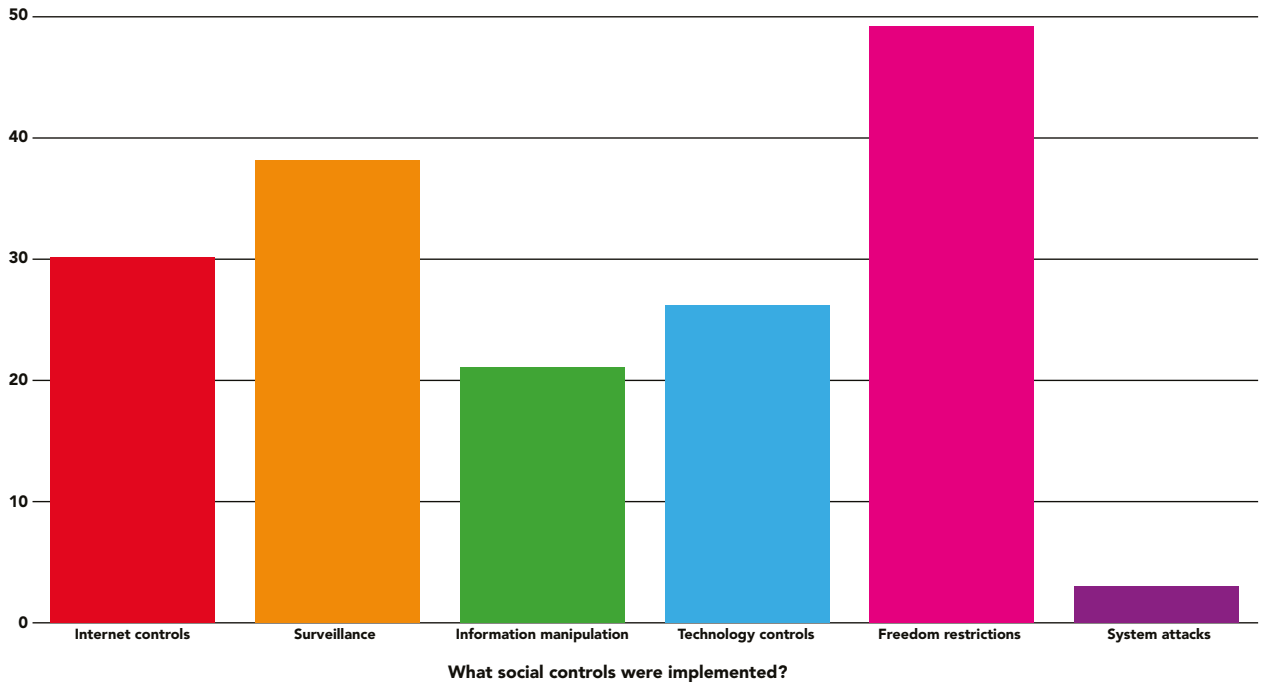


Table 07: Social controls and incidents

HARMS AND INCIDENTS

Within the incidents table, researchers record the specific harms to individuals, groups, and entire populations. Injured parties may experience more than one category of harm. In the dataset, intimidation — a threat without physical attack — was the most common harm, and physical harm, interestingly, was the least common. Although this dataset is not comprehensive, this distribution does correlate with the hypothesis of the political scientists Dragu and Lupu, that digital authoritarianism, in the form of preventative repression, may involve fewer physical attacks on individuals. Fewer physical violations of human rights, however, should not necessarily be read as an improvement in human rights, but possibly as evidence of the employment of different methods by authoritarians.[14]

14. Tiberiu Dragu and Lupu Yonatan, "Digital Authoritarianism and the Future of Human Rights." International Organization, vol. 75, no. 4, 2021, p.1010, doi:10.1017/S0020818320000624.

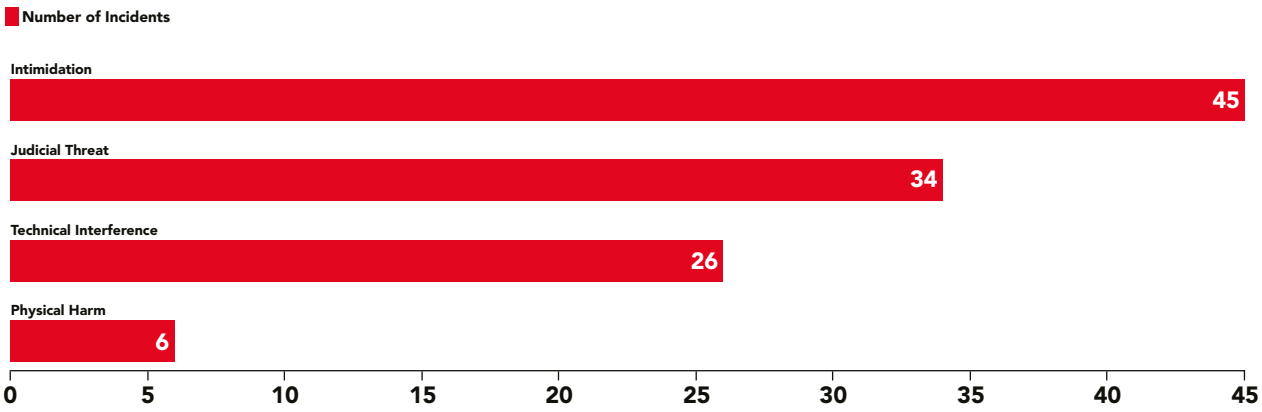


Table 08: Harms and incidents

SELECTING NARRATIVE FRAMES: WHY NARRATIVE ANALYSIS MATTERS

Narrative frames underpin claims that either advance or oppose ideas and material outcomes.[15] They are the often unspoken assumptions, beliefs or ideologies that compose the worldviews through which we understand and interpret the information we encounter in the world. Narratives help shape information into language that is familiar and intelligible to local communities. Analysing the effects of narratives requires us to both identify them and be explicit as to their meaning. The narratives that accompany and justify acts of repression can be useful signposts for authoritarian practices.

In our research, narratives about digital authoritarianism emerge from analysis of stories and commentary around events. The narratives we present have emerged empirically out of close reading of a range of media items: texts, videos, photographs, social media posts, government press releases and statements, journalism, academic texts, research reports, public opinion polls, and other media. Narratives are not static; they change over time in reaction to events, changes in attitudes, and policies. The narratives in the dataset should thus be understood as contextual in both time and place.

The following tables present a synopsis of the most frequently occuring pro-authoritarian and anti-authoritarian narrative frames, as well as a complete breakdown by Parent Frame. These findings reflect the research focus of the researchers, based on the incidents we selected for analysis; they do not represent a universal set of all narratives in play at the time.

Notably, in both pro- and anti-authoritarian contexts, a relatively small number of narrative frames are in wide use across many contexts. Thirty-nine percent of the narrative frames are associated with only one incident and 59 percent of the narratives are found in only one or two incidents. This points to the contextual nature of many of the arguments and claims.

Narrative frames often reference a particular country, incident or political environment, such as "Bolsonaro's supporters are being unfairly targeted for their online activities," referring to the activities of Brazil's "milícias digitais," a group of online disinformation agents affiliated with former president Bolsonaro's government.[16]

Even when narrative frames are context-specific, however, they often employ an underlying logic that is applicable in other situations. For this reason, we have grouped narrative frames with common intent into Parent Frames. This helps to explain the relationship of specific narratives to behaviours that we see replicated across contexts. For the Brazil example above, for example, the Parent Frame frame is "Denial of digital authoritarianism by the state."

15. Connie Moon Sehat, "Why the News Frame Matters (part 1 of 2)", Global Voices, February 9, 2017, https://newsframes.globalvoices.org/2017/02/09/why-the-news-frame-matters/; "Spotting the News Frame," Global Voices, April 3, 2017, https://newsframes.globalvoices.org/2017/04/03/spotting-the-news-frame/.

16. Unfreedom Monitor dataset, Narrative Frames table, UM_NarrativeFrame_12.

More broadly, we group narrative frames into pro-authoritarian justifications and anti-authoritarian counter-claims. Across themes and countries, researchers identified more anti-authoritarian than pro-authoritarian narrative frames, at a ratio of 2:1. This is consistent with findings from other Civic Media Observatory projects. Master narratives coming from states are often consistent across time and media sources, and frequently guided or encouraged by stage agents. In response, however, we often see a diversity of narratives coming from civil society seeking to resist authoritarian master narratives.[17]

Interestingly, a small number of narrative frames are used by both pro- and anti-authoritarian groups; this signals the importance of context when evaluating their meaning. For example, the narrative frame "The judiciary should not abuse its powers" is used both by pro-democracy groups in Hong Kong related to the closure of the media outlet Stand News, and also in Brazil by Bolsonaro supporters seeking to curb the authority of the courts.[18]

Our researchers found that pro-freedom of expression narratives are mostly used by pro-democratic groups pursuing freedoms, especially in the context of access and speech issues. Yet the inverse was sometimes true with regard to the theme of information. We see freedom of speech arguments used by regimes that are formally democratic, such as Bolsonaro's government in Brazil, which employed information operations and disinformation units to discredit opponents and consolidate power, perhaps as a precursor to efforts to restrict democratic participation.

PRO-AUTHORITARIAN NARRATIVE FRAMES

Researchers identified a relatively small number of pro-authoritarian narrative frames recurring across many incidents. This result emerged empirically out of the selection of incidents on which each researcher chose to focus, and does correspond to researchers' focus on speech freedoms. The most frequently occurring narrative frame in the dataset is "Freedom of expression is not an absolute right."[19]

The research also shows commonalities underlying the claims made by different narrative frames. For example, authoritarian claims frequently privilege national interests and state control over the freedoms and rights of citizens, and over universal rights. Pro-authoritarian claims that the right to freedom of expression and internet access are not absolute compete with pro-freedom aspirations for universal rights. Arguments in favour of limiting free expression and access are also well established in democratic contexts. This requires us to examine the claims of states carefully in order to understand whether an effort to delimit rights passes the tests for democratic governance, such as transparency, accountability, proportionality and citizen oversight.

Several popular pro-authoritarian frames attempt to justify freedom restrictions as being beneficial to citizens. These narratives focus on topics such as national security, public safety and health, public morals, and equality under law. For example, the second most

17. Ivan Sigal, "New report: Framing China's Belt and Road Initiative," Global Voices, December 5, 2022, https://globalvoices.org/2022/12/05/new-report-framing-chinas-belt-and-road-initiative/.

18. UM_NarrativeFrame_172. UM_MediaItem_1005. UM_MediaItem_973.

19. UM_NarrativeFrame_158.

common narrative frame in the dataset is "Governments must monitor media and social media to ensure political stability and public safety," which researchers found in Myanmar, Venezuela, India, Zimbabwe, Russia, Iran, Kyrgyzstan, and Rwanda.[20]

Other popular pro-authoritarian frames focus on vilifying and dehumanising opponents. Such claims use fear to legitimise repression and sometimes violence. For example, the narrative "Journalists who criticise the government are enemies of the state," found by researchers in Zimbabwe, Hungary, El Salvador, India, China (and Hong Kong), Cameroon, Philippines, Rwanda, and Iran, is tied to media shutdowns, arrests of journalists, justifications for surveillance, and restrictive media regulation.[21] Likewise, the populist narrative frame "Foreign-funded NGOs and media outlets are a threat to the country," found in Zimbabwe, Hungary, El Salvador, China (and Hong Kong), Russia, Kyrgyzstan, Iran, and Cameroon, is used to delegitimise civil society organisations with international ties, expel or restrict foreign journalists, and weaken claims to rights protected under international charters.[22]

Authoritarians take a variety of approaches to narrative construction and framing in response to threats to their authority. Analysing the choice of approach may illuminate the nature of regimes, and triggers useful questions for researchers seeking to understand the pacing and frequency of narrative frames, such as:

- Are there narratives that reliably prefigure an authoritarian turn?
- Are states devoting resources to creating and propagating narratives, such as state broadcasters, information operations units, and administrative processes for coordinating messaging?
- In which circumstances do governments perceive the need to propagate justifications for authoritarian actions?
- Are specific narratives more common in certain types of regime?
- Is there an inflection point on the spectrum of authoritarian rule beyond which authoritarian regimes no longer need to justify their actions?

20. UM_NarrativeFrame_71.

21. UM_NarrativeFrame_128.

22. UM_NarrativeFrame_157.

Narrative frames	Number of incidents asserting narrative
Freedom of expression is not an absolute right	**25**
Governments must monitor media and social media to ensure political stability and public safety	**13**
Journalists who criticise the government are enemies of the state	**13**
Blocking apps, websites and other forms of access to sensitive information is justified by national security reasons	**11**
Foreign-funded NGOs and media outlets are a threat to the country	**10**
Access to the internet is not an absolute right and it rightly has limits	**9**
The state respects press freedom	**7**
States' use of surveillance technology makes the country safer	**6**
Anybody critical of the state is the state's enemy	**5**
Social media should comply with state regulations to ensure content and activity online are in line with the law	**5**

Table 09: Top ranked pro-authoritarian narrative frames

ANTI-AUTHORITARIAN NARRATIVE FRAMES

As with pro-authoritarian frames, researchers also identified a relatively small number of anti-authoritarian narrative frames recurring across many incidents. This result emerged empirically out of the selection of incidents chosen by each researcher, and the findings correspond to researchers' focus on speech freedoms.

One of the most frequently occurring narrative frames is "Freedom of expression is a fundamental right," which appears in many contexts and countries, including Zimbabwe, Venezuela, India, Myanmar, Iran, Ethiopia, Egypt, Hungary, El Salvador, Tanzania, Brazil, Turkey, China (and Hong Kong), Kyrgyzstan, Sudan, Kenya, Cameroon, Philippines, Russia, and Rwanda.[23] This appeal to universal rights is foundational to many efforts to push back against speech and access restrictions. Notably, it is challenged by an array of positions from authoritarian states, which seek to diminish its impact by noting that fundamental rights are not absolute, and perhaps more effectively, with appeals to contextual and often paternalistic claims about safeguarding the well-being of citizens by protecting them from certain kinds of speech. Here again, details matter, as this narrative frame usually functions as a justification for pushing against speech restrictions that target perceived threats to regime power, are disproportionate, or do not accord with widely acknowledged international standards.

23. UM_NarrativeFrame_160.

Many of the other most widely used anti-authoritarian narrative frames also argue in favour of open expression, media rights, and the ability of journalists to work without hindrance, with appeals to universal rights.[24] Other key narrative frames likewise argue that surveillance and access restrictions such as internet shutdowns are breaches of universally protected, fundamental rights.[25]

Other anti-authoritarian narrative frames make values-based claims, citing the protection of democracy, and the societal benefits of transparency, proportionate and justified regulation, and the equal protection of existing law. Many of these are context-specific, and fall under meta-categories such as "Frames against surveillance by the state," "Arguments against internet controls and access blocking," and "Frames upholding data protection."

Analysing anti-authoritarian narrative frames may illuminate the choices and effectiveness of opposition, and triggers useful questions for researchers seeking to understand the process of anti-authoritarian narrative-making, such as:

- Are appeals to universal rights effective? And if so, in what contexts do claims that rely on fundamental and democratic rights have influence?
- When do local, contextual claims and arguments have influence?
- Which social media platforms support speech rights in practice?
- Under what conditions are arguments for speech rights actually detrimental for democracies?

Narrative frames	Number of incidents asserting narrative
States should not crack down on dissent and criticism	**24**
Freedom of expression is a fundamental right	**24**
The country's press freedom is in decline	**18**
Journalists should be able to report on abuses of power without being surveilled or harmed in other ways	**15**
Surveillance of citizens violates their fundamental rights	**13**
It is never acceptable for governments to block websites and other online content	**13**
Internet shutdowns and disruptions are hugely detrimental to society	**12**
States must not engage in censorship	**11**
It is never acceptable for governments to shut down the internet	**9**
Government and state-owned media should not sponsor mis/disinformation and defamation campaigns	**8**

Table 10: Top ranked counter narrative frames

24. UM_NarrativeFrame_163, UM_NarrativeFrame_44.

25. UM_NarrativeFrame_36, UM_NarrativeFrame_147.

PARENT FRAMES

Parent Frames are groupings of narrative frames that share commonalities. The table below shows both the number of detailed narrative frames within each Parent Frame, and the number of incidents that cite it. Given the dataset's focus on freedom of expression, it is no surprise that the Parent Frame in support of freedom of expression appears in the highest number of incidents, followed by those that support press freedom and those that oppose internet controls and access blocking.

Interestingly, the number of Parent Frames with the largest number of narrative frames is "Frames that support the Russian state's claims." This makes sense considering the Russian war on Ukraine, and the energies the Russian state puts into churning narratives as a misdirection tactic to drive indifference and confusion. Russia invests in technologies and media and builds sophisticated and expensive state media outlets and administrative systems for propagating and policing narrative frames, combined with messaging protocols from governmental ministries, proxy troll armies working social media networks, and the policing of counter-narratives by regulators.[26]

In the dataset, Parent Frames are organised using the "group" function of Airtable, and can be found as headings in the Narrative Frames table.[27]

Parent Frames	Number of detailed narratives	Number of incidents asserting it
Frames that oppose coordinated inauthentic behaviour and disinformation	9	25
Frames that oppose the Chinese state's claims	1	2
Frames that oppose the Russian state's claims	8	23
Frames that oppose internet controls and access blocking	6	49
Frames that oppose the regulation of social media and influence campaigns	2	2
Frames that support the Russian state's claims	17	22
Frames that support press freedom	6	58
Frames that support freedom of expression	11	85
Frames that support regulating tech companies	3	7
Frames that defend surveillance	2	13
Frames that defend the independence of tech platforms	2	8
Frames that uphold privacy as a fundamental right	4	5

26. UM_NarrativeFrame_37. Peter Pomerantsev, "Nothing Is and Everything Is Possible," (New York, Public Affairs, 2014.

27. UM_NarrativeFrames.

Parent Frames	Number of detailed narratives	Number of incidents asserting it
Frames arguing that Western countries are acting against the interests of non-Western states	3	14
Frames that deny the existence of technology controls in authoritarian states	8	24
Frames that oppose state-sanctioned authoritarianism	6	10
Frames that oppose surveillance by states	13	43
Frames that oppose technology exports that further authoritarianism	4	8
Frames that support limitations on freedom of expression	2	26
Frames arguing that platforms are biased	8	4
Frames arguing that platforms enable digital authoritarianism	8	12
Frames that support anti-minority discrimination	3	1
Frames that oppose anti-minority discrimination	3	5
Frames that support data protection	5	6
General, pro-regime frames	1	1
Frames that justify digital authoritarianism by the state	7	17
Frames that support internet controls and content blocking	4	30
Frames that justify state-sanctioned surveillance	4	9
Miscellaneous frames	4	3
Frames that oppose censorship	4	24
Frames arguing that states used COVID-19 as an excuse to restrict freedoms	2	8
Frames arguing that social media platforms are effective at curbing misuse of their platforms	4	5
Frames that oppose press freedom	4	17
Frames that demand accountability and transparency by states	5	7

Table 11: Parent frames

For a deeper explanation of the Civic Media Observatory methods and analysis of our dataset, see the methods section in the appendix.

FOUR CASES: DATA GOVERNANCE, SPEECH, ACCESS, INFORMATION

All authoritarian acts analysed in the dataset share an underlying logic that seeks not only to control or punish specific groups or individuals, but to reinforce a system of power. For example, one incident in the Turkey dataset involves the arrest of three men for running a YouTube channel that analyses Turkey's economy. The men were targeted for "denigrating the state and government." Their detention, according to our analysis, is illustrative of the Turkish government's efforts to "silence independent voices but also mute people's growing discontent with the government policies." The nature of their arrest also points to the government's use of digital public surveillance, using a range of technologies and monitoring of online environments.[28]

There are times when authoritarian acts are overt, highly visible and aggressively telegraphed by the state and its agents. For example, Russia's expansion of its invasion of Ukraine on February 24, 2022 triggered an array of authoritarian acts:

> *To police real coverage of the war in Russia, Russian officials cracked down on the remaining independent media and social media platforms, passing a new law that criminalised any coverage of the war not aligned with state rules (e.g., calling it a "war") and blocking a number of major social media platforms and independent media, including Facebook, Instagram and Twitter.*[29]

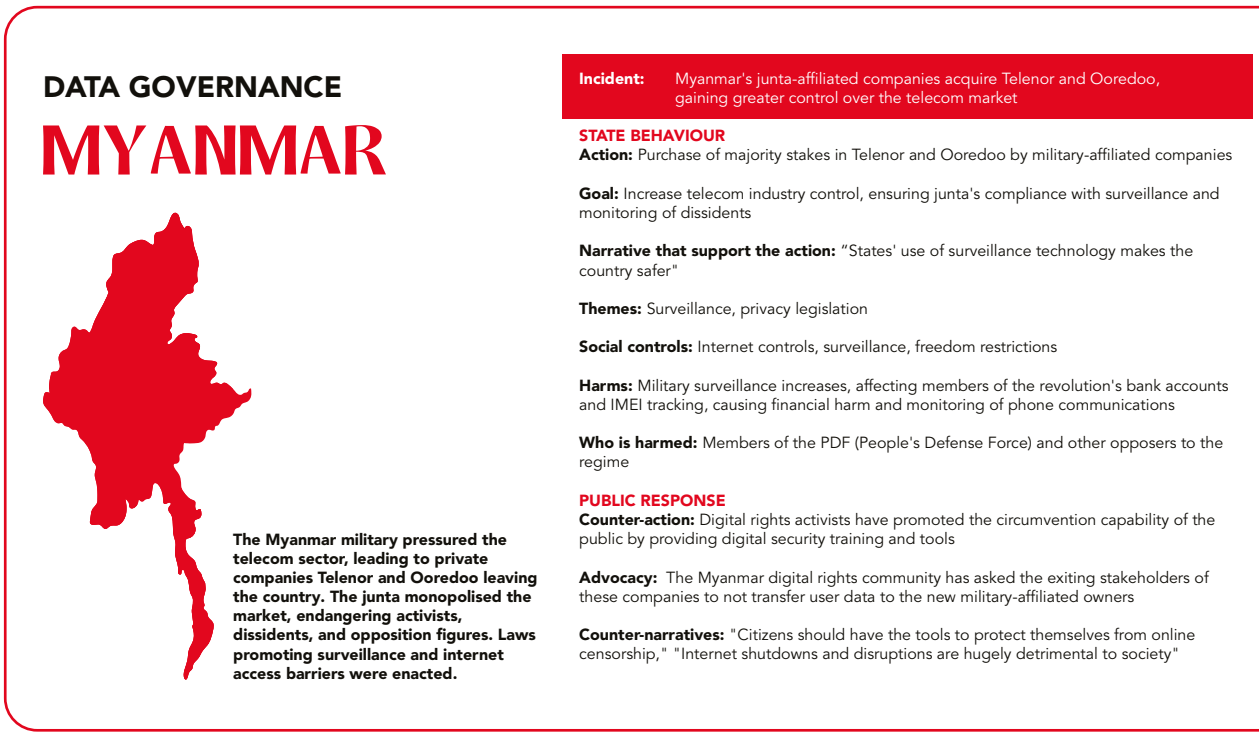
The decision to include Russia's invasion of Ukraine as an incident is, it should be noted, unusual in the dataset, just as the invasion itself is unusual. But, despite the vast difference in scale, we can draw parallels between Russia's actions and the one carried out by Turkey described above. In both cases authoritarian acts are justified as necessary to preserve the power of the state. Both also repress speech that threatens state narratives using technological means.

In the following four cases we select one incident to illustrate each theme, to unpack how authoritarian practices have played out in different contexts.

28. Unfreedom Monitor dataset, "Three YouTubers in Turkey are handed house arrests," UM_Incident_11.

29. Unfreedom Monitor dataset, "Russia's invasion of Ukraine," UM_Incident_17.

DATA GOVERNANCE



Incident: Myanmar's junta-affiliated companies acquire telecom operators Telenor and Ooredoo, gaining greater control over the telecom market.[30]

Country: Myanmar

Tagline: The sale of foreign telecom companies operating in Myanmar to entities friendly to or owned by the regime puts users at risk, as user data are among the companies' key assets. All four of Myanmar's telecom companies are now controlled by the government, allowing it to surveil networks and access user data at will.

Themes: This incident concerns control over communications networks and, by extension, data governance, including both surveillance on networks and privacy violations of users. Control over data enables the state to exercise other restrictions through the implementation of surveillance technologies, such as fine-grained control over internet access, monitoring of individual accounts, restrictions on speech, and mandatory registration of SIM and IMEI numbers.[31]

30. UM_Incident_50.

31. Global Voices Civic Media Observatory analysed 247 media items in Myanmar from November 2021 to January 2023, including many instances of hateful, disinformation and misleading expression by the military regime and its supporters. Civic Media Observatory 2021-2022: Myanmar.

Summary of the incident: The purchase by state-affiliated entities of foreign-owned telecommunications networks helps Myanmar's government gain control of the telecom industry, which ensures that all they have access to user data in telecommunications networks, and that companies will abide by state requests to facilitate surveillance and monitoring of Myanmar's population. This consolidation of control threatens opposition party activists and leaders, journalists and other dissenting voices the state might wish to target.

The Myanmar military pressured two private companies, Telenor (Norwegian) and Ooredoo (Qatari) into selling their Myanmar operations. Telenor acknowledged that pressure from the junta to enable intercept surveillance was a key reason for the sale, as was avoiding EU sanctions.[32] The companies were purchased by military-backed and affiliated companies, leading to concern that the telecom market would be fully monopolised by the junta, endangering the lives of activists, dissidents and opposition figures.[33]

The junta simultaneously enacted laws that encourage surveillance and create barriers to internet and phone access, such as mandatory IMEI registration and increased taxation of SIMs.[34] There are four telecom operators in Myanmar: MPT, MyTel, Telenor and Ooredoo. MPT and MyTel are owned by military affiliates. By acquiring Telenor and Ooredoo, the junta gains full control of the telecom market.

Telenor completed its sale to the Lebanese firm M1 and the Myanmar company Shwe Byain Phyu in March 2022.[35] In September 2022, the Ooredoo Group announced the sale of its Myanmar telecom business to Nine Communications Pte. Ltd., which is incorporated in Singapore and reportedly owned by the Link Family Office and Mu Nyan Win.[36]

Social controls: The purchase of the two telecommunications firms by regime-friendly businesses facilitates numerous types of controls, including digital public surveillance, online tracking, and access to user data. It also facilitates the state's ability to increase barriers to online access through price increases and punitive taxes for online access.[37] Phone numbers of pro-democracy political leaders have been cloned and monitored. The military is also monitoring activity on phone numbers and watching mobile banking services for financial flows to opposition figures.

Narrative frames: While the Myanmar government does not always justify its actions with narratives, when it does, it uses narratives that focus on public order and safety, national security, and peace.

---

32. "Qatari Telecom Operator Ooredoo Exits Military-Ruled Myanmar," The Irrawaddy, September 8, 2022, https://www.irrawaddy.com/news/burma/qatari-telecom-operator-ooredoo-exits-military-ruled-myanmar.html.

33. "As Myanmar junta extends control over telcos, surveillance and privacy risks increase," Access Now, February 24, 2022, https://www.accessnow.org/myanmar-junta-surveillance-telcos/.

34 "Myanmar IMEI FAQ: how the junta could disconnect the resistance," Access Now, July 7, 2022, https://www.accessnow.org/myanmar-imei/.

35. "Telenor completes Myanmar business sale, to be paid over 5 years," Reuters, March 25, 2022, https://www.reuters.com/business/media-telecom/telenor-completes-myanmar-business-sale-be-paid-over-5-years-2022-03-25/.

36. UM_Synthesis_38.

37. UM_MediaItem_252.

"States' use of surveillance technology makes the country safer."[38] This argument is made by governments and technology companies that have manufactured and implemented surveillance technology, who contend that doing so makes populations safer by helping fight crime, including financial fraud, and make cities safer. Activists argue that the measures violate citizens' privacy and create the potential for the insidious abuse of the large volumes of citizen data that is gathered as a result of this surveillance. Researchers also found this narrative in Egypt, Tanzania, Hungary, Ukraine, Zimbabwe, and Kenya.

Counter-narrative frames: Several of the counter-claims made here focus specifically on data governance and control of the telecoms industry. Others appeal to the universal rights and values that underpin claims in favour of privacy, access to information, and access to technologies.

"The government is consolidating its dictatorship by seeking control of the telecom industry."[39] The claim states that regimes such as the Myanmar junta are trying to monopolise the telecom market to consolidate their total control over communications, to clamp down on dissent and freedom of expression. Researchers also found this narrative in Sudan.

"Citizens should have the tools to protect themselves from online censorship."[40] This assertion, made by media, activists and NGOs, supports the idea that citizens living in countries with online censorship need to have access to the tools to evade it. Proponents of this frame argue that the goal is to promote access to information through tools that will keep citizens safe. This narrative has been promoted as a citizen solution to evade censorship, especially during elections and times of political and social crisis. Researchers also found this narrative in Venezuela.

"Surveillance of citizens violates their fundamental rights."[41] This narrative claims that carrying out surveillance on citizens and collecting their data without their consent is authoritarian. Authoritarian regimes have long feared mass uprisings, and implement political repression to target and harass opposition. Researchers also found this narrative in Zimbabwe, Hungary, China (and Hong Kong), Egypt, Brazil, Russia, Morocco, Tanzania, Sudan, Kenya, Cameroon, El Salvador, Iran, and India.

"The government should not be able to access citizen data without legal justification."[42] This narrative frame argues that governments should be required to provide legal justification to obtain access to citizen data, and that such requests should be necessary, proportionate and made in a transparent manner. This frame is asserted in contexts where there is fear of abuse of power and governmental overreach. Researchers also found this narrative in Brazil, Egypt, Hungary, Tanzania, and India.

38. UM_NarrativeFrame_171.
39. UM_NarrativeFrame_77.
40. UM_NarrativeFrame_136.
41. UM_NarrativeFrame_36.
42. UM_NarrativeFrame_37.

"The government's taxing of internet use is an infringement of citizens' rights."[43] This narrative frame argues that restricting citizens' access to the internet by imposing high taxes is undemocratic and an infringement of digital rights. In the case of Myanmar, the state imposed both a commercial tax on SIM cards and a tax on ISP income, which raises the cost of access. Knowledgeable observers claim that the state is increasing barriers to access in order to restrict use.[44] Researchers also found this narrative in Zimbabwe, Tanzania, Sudan, Kenya, Cameroon, and Egypt.

"Internet access is a human right."[45] This narrative frame asserts that everyone must be able to access the internet in order to exercise their rights to freedom of expression, press, opinion and other fundamental human rights. The frame also asserts that states have a responsibility to ensure internet access and that governments may not unreasonably restrict access to the internet. Some countries have laws that require the state to ensure that internet access is broadly available, and regulations that prevent the state from unreasonably restricting the access to information and the internet. Many activists in authoritarian countries use this claim to protest internet restrictions, and to promote the idea that internet access is a human right or a human rights enabler. Researchers also found this narrative in Venezuela, India, Tanzania, China (and Hong Kong), Egypt, Iran and Sudan.

Counter-action: Telenor publicised the pressure placed on them by the military, including orders that they remove IP addresses, block certain websites and platforms, and participate in a nationwide shutdown of mobile communications, and a requirement that it stop sharing those orders with the public.[46]

Digital rights activists have been promoting circumvention capability for internet users by providing digital security training and tools, and information about VPNs and encrypted messaging applications, while claiming their right to do so as part of a broader argument about universal expression rights.

Advocacy: The Myanmar digital rights community has asked the exiting companies to not transfer user data to the new military-affiliated owners.[47] Numerous groups have noted their displeasure with the Telenor sale with the OECD representative for Norway — noting that the Norwegian state is the majority shareholder in Telenor.[48]

Before the sale of Telenor, a data protection complaint was filed by Myanmar activists against the Norwegian company and 694 civil society organisations signed a petition asking for transparency on how Telenor will handle the transfer of the data of 18 million users.[49]

---

43. UM_NarrativeFrame_57.

44. "Myanmar Junta Raises SIM and Internet Taxes to Silence Opposition," Irrawaddy, January 12, 2022, https://www.irrawaddy.com/news/burma/myanmar-junta-raises-sim-and-internet-taxes-to-silence-opposition.html. UM_MediaItem_252.

45. UM_NarrativeFrame_53.

46. "Updates on Telenor in Myanmar," last updated February 28, 2022, https://www.telenor.com/sustainability/responsible-business/human-rights/human-rights-in-myanmar/directives-from-authorities-in-myanmar-february-2021/.

47. UM_NarrativeFrame_50.

48. Stein Tønnesson, "Telenor's Exit from Myanmar: An External Review Is Needed," PRIO Blogs, May 29, 2022, https://blogs.prio.org/2022/05/telenors-exit-from-myanmar-an-external-review-is-needed/.

49. UM_NarrativeFrame_77.

Both international and Myanmar civil society advocates argued that Telenor and Oredoo are obliged to uphold human rights, and made their case through press releases, public letters, social media posts, interviews with media and think tanks,and interventions in international forums.

These efforts ultimately had little effect on the outcome of the sales. Access Now, in a press release, noted for instance that Ooredoo "has not responded to, or acknowledged" communications that encourage the communications firm to meaningfully engage with civil society.[50] They had asked that Ooredoo "immediately conduct human rights due diligence, and urgently engage w/ civil society + key stakeholders to ensure people's rights are protected."[51]

Other civil society groups, such as ANFREL (Asian Network for Free Elections) and the Chin Human Rights Organization, also regularly advocate via social media, such as in the Facebook public group Burma Nationalities Human Rights, and in a range of independent media and international forums.[52]

These efforts have served to document details and a timeline of events in Myanmar, and register objections in a variety of forums. While they have had less success in changing short-term outcomes, such efforts do have influence over time, at least with international bodies and multinational initiatives. Whether they will ultimately influence the situation in Myanmar remains to be seen.

50. "Ooredoo's plans to leave Myanmar hands military full control of nation's telco sector — it must mitigate the human rights risks," Access Now, September 15, 2022, https://www.accessnow.org/press-release/ooredoo-myanmar-sale/.

51. UM_MediaItem_432.

52. UM_MediaItem_406.

SPEECH

SPEECH

KYRGYZSTAN

A series of detentions occurred in Kyrgyzstan against civil society activists, ex-politicians, and acting politicians between October 23 and 27, 2022. In total, 27 people were arrested and detained for two months before their trial, including six women, some with minor children. They publicly spoke against the handover of the Kempir-Abad water reservoir to Uzbekistan.

Incident: Mass detention of critics who protested on social media against the controversial border deal with Uzbekistan

STATE BEHAVIOUR

Action: Censorship of social media users and punishment of critics

Goal: Repression of dissonant voices

Political and legal justification: The state base its actions in the law against the spread of fake news, adopted in August 2021

Narrative that support the action: "Foreign-funded NGOs and media outlets are a threat to the country," "Civil society activists and pro-Western media are fomenting political instability"

Themes: Freedom of expression, freedom of opinion, surveillance, legislation

Technology applied: Hacking of social media

Social controls: Surveillance, freedom restrictions, technology controls, information manipulation

Harms: Surveilled, intimidated, harassed online, harassed in real life, home or office raided, interrogated

Who is harmed: Social media users, bloggers, journalists, and any political regime critics

PUBLIC RESPONSE

Counter-action: Protests were held against the transfer of the Kempir-Abad reservoir and political pressure against activists. Pushback was also recorded within civil society organisations and the Parliament

Advocacy: More than 80 representatives of civil society and human rights activists in Kyrgyzstan appealed to the government to release female activists

Counter-narratives: "Citizens should be able to access information on state projects," "Surveillance of citizens violates their fundamental rights"

Incident: Mass detention of critics who protested on social media against the controversial border deal with Uzbekistan.[53]

Country: Kyrgyzstan

Tagline: The incident features a combustible mix of regime populism plus an array of legal, extralegal and technological approaches to restrict expression and civic participation, as well as narratives that demonise civic activists as agents of foreign powers.

Themes: This incident primarily concerns the restriction of freedom of speech and freedom of opinion. Other themes in play include the use of surveillance, legislation to create repressive regulation, and disinformation and misinformation.

Summary of the incident: Numerous civil society activists and politicians in Kyrgyzstan were detained during the period October 23-27, 2022. Twenty-seven people were arrested and held in pre-trial detention for two months, with the detention of many extended further. They opposed the handover of Kyrgyzstan's Kempir-Abad water reservoir to Uzbekistan as part of a deal to settle disputes over their shared border. They voiced their opposition on social media channels and during a public assembly (Kurultai) organised in Özgön on October 15, 2022.

53. Unfreedom Monitor dataset, "Mass detention of critics who protested on social media against the controversial border deal with Uzbekistan," UM_Incident_56.

Most of the detained activists were members of the Committee to Save Kempir-Abad, an initiative formed after the Özgön public assembly. The committee sought to hold a nationwide public meeting on October 26 in Bishkek on the issue of the water reservoir.

The regime engaged in digital and in-person surveillance and wiretapping of the activists, monitoring of their social media activities, and both digital and in-person harassment. According to Human Rights Watch, the state "conducted warrantless searches of activists' houses and seized personal property."[54]

The incident turned on a claim by the government that the civic activists aimed to create protests that would trigger the overthrow of the current government, and that their opposition to the transfer of the Kempir-Abad water reservoir was merely a pretext for regime change.

This claim is bolstered by an act of information manipulation: Kyrgyzstan's security forces published three audio conversations on social media recorded using a wiretap, and edited to make it appear that the activists were planning an attempt to overthrow the government. The detainees are accused of attempting to organise a mass riot, which, under Kyrgyzstan's Criminal Code, can be punished by up to 10 years of imprisonment.

Social controls: The current government of President Sadyr Japarov has an increasingly populist and authoritarian character. Japarov's government uses social media platforms to create an impression of public support and to discredit non-state media, NGOs, and opposition politicians.[55]

Kyrgyz authorities, in turn, are creating an enabling environment to support authoritarian acts. They are amending existing laws and introducing new ones to limit and control the freedoms of expression, opinion and information production of non-state media, bloggers and civil society. The government passed the "Law on Protection from False Information" in 2021, which has been used to justify its surveilling and censoring of social media users and has been punishing them for posting or reposting any information critical of the state.[56] The government is also pursuing the establishment of registration requirements for online media outlets and bloggers, modelled on Russia's regulation of bloggers and independent media outlets.[57]

The state blocks the websites of critical media, such as RFE/RL's Azattyk.[58] While there is no openly available information about the technologies used to block sites, DNS blocking and IP blocking of websites is common in Kyrgyzstan.

---

54. Syinat Sultanalieva, "Kyrgyzstan Arrests Activists en Masse," Human Rights Watch, June 21, 2023, https://www.hrw.org/news/2022/10/25/kyrgyzstan-arrests-activists-en-masse.

55. Arzuu Sheranova, "Social media censorship and information manipulation after Sadyr Zhaparov's rise in Kyrgyzstan," Global Voices, May 3, 2023, https://www.president.kg/ru/sobytiya/20377_podpisan_zakon_kirgizskoy_respubliki_zakon_krozashite_otnedostovernoy_loghnoy_informacii.

56. Website of the Office of the President of the Kyrgyz Republic, Подписан Закон Кыргызской Республики Закон КР «О защите от недостоверной (ложной) информации», August 23, 2021, https://www.president.kg/ru/sobytiya/20377_podpisan_zakon_kirgizskoy_respubliki_zakon_krozashite_otnedostovernoy_loghnoy_informacii.

57. "Importing illiberal practices: The Kyrgyz state's attack on media, journalists and bloggers," Global Voices Advox, May 20, 2023, https://advox.globalvoices.org/2023/05/20/importing-illiberal-practices-the-kyrgyz-states-attack-on-media-journalists-and-bloggers/.

58. Unfreedom Monitor dataset, "Kyrgyzstan: Mass detention of critics who protested on social media against the controversial border deal with Uzbekistan," UM_Incident_62.

Narrative frames: Japarov's government pushes narratives that depict civic activists and civil society and journalists as agents of foreign powers, claiming that the issue is one of state sovereignty.

"Civil society activists and pro-Western media are fomenting political instability."[59] This narrative asserts that civil society activists, NGOs, and other regime critics are "nation spoilers" or destabilisers/provocateurs who seek to create political instability in the country. This is a central narrative promoted by state authorities in some countries and is used to oppress and limit civil society, open media, critics and political opponents. Researchers also found this frame in Kazakhstan and China (Hong Kong).

"Foreign-funded NGOs and media outlets are a threat to the country."[60] This narrative asserts that NGOs and media outlets that receive funding from abroad are able to influence public life without any democratic legitimacy. This narrative frame is used by states to justify clamping down on organisations and media outlets that do not conform to their values and comply with their demands. Researchers also found this frame in numerous countries in the dataset, including Zimbabwe, Hungary, El Salvador, China (and Hong Kong), Russia, Iran, and Cameroon.

Secondarily, the government's position aligns with a narrative frame that many states use to justify crackdowns on civic expression, opinion and information.

"Freedom of expression is not an absolute right."[61] This argument states that freedom of expression is not absolute and that it is justifiable to place limits on it. This narrative frame helps shed light on how the "anti-hateful speech" argument is used to crack down on dissent and opposing voices. Researchers found this frame in Brazil, India, Zimbabwe, Hungary, Tanzania, Myanmar, China (and Hong Kong), Turkey, Cameroon, Kazakhstan, Iran, Philippines, and Rwanda.

Counter-narrative frames: Opposition narratives in Kyrgyzstan have focused on fundamental and universal rights, on the transparency of governmental information, and on an explicit counter-narrative that seeks to discredit a governmental position.

"Freedom of expression is a fundamental right."[62] This narrative argues that freedom of expression, both online and offline, is reflective of a vibrant democratic system that respects the rule of law and the human and digital rights of people. This frame provides nuance and context about how autocratic governments violate fundamental rights such as freedom of expression. This narrative is one of the most frequently used by democracy activists in the dataset. We also found it in media items from many countries, including: Zimbabwe, Venezuela, Sudan, India, Myanmar, Venezuela, Egypt, Hungary, El Salvador, Tanzania, Brazil, Turkey, China (and Hong Kong), Kenya, Cameroon, Philippines, Russia, Rwanda.

59. UM_NarrativeFrame_157.
60. UM_NarrativeFrame_158.
61. UM_NarrativeFrame_159.
62. UM_NarrrativeFrame_161.

"Under no circumstances should the state be able to jail journalists."[63] This narrative, promoted by media rights activists and journalists, asserts that state authorities that level fabricated and trumped-up charges should not imprison journalists under any circumstances. It highlights how states persecute journalists unfairly and unlawfully. In the dataset this narrative is seen in Egypt, Zimbabwe, Myanmar, China (and Hong Kong), Russia, Egypt, Turkey, India, Tanzania, Sudan, Cameroon, and Russia.

Surveillance of citizens violates their fundamental rights."[64] This frame is important for the preservation of fundamental rights and makes a case for ending the surveillance of citizens. It is ubiquitous in the dataset, and has been found in media items that discuss Zimbabwe, Hungary, China (and Hong Kong), Egypt, Brazil, Iran, Russia, Rwanda, Tanzania, Sudan, Kenya, Cameroon, Myanmar, El Salvador, India, and Ecuador.

"Citizens should be able to access information on state projects."[65] In the dataset, this frame appears in the context of the specific concerns of Kyrgyzstani activists, because the Kyrgyzstani government has kept details of its negotiations with Uzbekistan secret. The narrative serves as a foundation for exerting civic pressure on Kyrgyz authorities to be more transparent in decision-making, and draws the attention of the international community to the violation of human rights by the Kyrgyz authorities.

"The state uses the label 'foreign agent' to discredit independent media outlets."[66] This narrative is promoted by independent media, opposition actors and NGOs, and explicitly opposes a state narrative. It claims that the foreign agent label is designed to legitimise the persecution of those who oppose state narratives and policies, and targets mostly independent journalists, human rights activists and citizens critical of the regime. Since the passing of foreign agent laws, many independent media, NGOs and individuals have been targeted, which has led to organisations and individuals shutting down their operations in places such as Russia, and the blocking of their websites. This also puts pressure on remaining independent voices, including those operating online. In the dataset, Russian and Kyrgyzstani activists use this frame.

Counter-action: Kyrgyzstan has a robust civil society sector and has been able to muster a substantial response in this case. Following is a summary of advocacy efforts, most of which was originally published in the Unfreedom Monitor's Kyrgyzstan Country Report.[67]

On October 24, in Bishkek and Osh, protests were held against the transfer of the Kempir-Abad reservoir and the political pressure being exercised against activists.[68] The participants urged the government to halt the prosecution of detained civic activists and demanded their release. Three hundred participants took part in the protest in Bishkek, 10 in Osh, and around 100 in Uzgen. The Ombudsman Institute of the Kyrgyz Republic

63. UM_NarrativeFrame_156.

64. UM_NarrativeFrame_34.

65. "Citizens should be able to access records to state projects," UM_NarrativeFrame_133.

66. UM_NarrativeFrame_52.

67. "The Unfreedom Monitor: Kyrgyzstan Country Report," Global Voices Advox, June 2023, pp. 18-20, https://globalvoices.org/wp-content/uploads/2023/08/Unfreedom_Monitor_Kyrgyzstan_Country_Report_2023_updated.pdf.

68. "В Кыргызстане прошли акции протеста против передачи Кемпир-Абада," Kloop, shared on YouTube, last accessed June 28, 2023, https://www.youtube.com/watch?v=REh0_q7pPYo.

led by Atyr Abdrahmatova, publicly expressed their concern about the mass detention of activists, and called on the government to ensure the implementation of international Human Rights regulations and ensure the independence of the Ombudsman Institute.[69]Some members of the Kyrgyz parliament, including Zhanar Akaev and Dastan Bekeshev, also publicly demanded the release of detained activists during a parliamentary sitting. Following a December 2022 court decision to extend the activists' arrest until February 20, 2023, relatives of the detained activists held a protest requesting a house arrest.[70]

On October 27, 2022, the Media Policy Institute, an NGO working for press freedom in Kyrgyzstan, published a letter calling on the government to stop attacking the freedom of the media and expression in the country, to stop pressuring journalists and media outlets, and to reconsider the law on the spread of false information that was passed in 2021. The letter was signed by representatives of independent media outlets, bloggers, independent journalists and activists.

Another letter was published by representatives of independent media and civil activists calling on President Zhaparov, the Kyrgyz Parliament, and the government to stop blocking Azattyk and other media outlets, to stop prosecution against journalists, to withdraw the draft of a law on media in Kyrgyzstan, to establish a working group to participate in discussions on legislative amendments concerning media, and to cancel the law on false information. The undersigned also requested a personal meeting with President Zhaparov.

On October 28, 2022, a solidarity protest against state censorship and pressure on media was staged by independent media, journalists and activists in Kyrgyzstan by posting a blacked-out page on their websites or social media with the words: "No News Today. Media Under Pressure in Kyrgyzstan." Independent media outlets such as Kaktus.media, Kloop.kg, 24.kg, T-Media, TV1, NEXT TV, 3rd channel, April TV, Bulak.kg, Politklinika.kg, TemirovLive, and MediaHub halted their news coverage for three hours on that day as a sign of protest.

On November 7, 2022, in Bishkek, on the occasion of the Day of Information and Press, representatives of the media held an event called "Plant trees, don't arrest journalists," where journalists and activists planted trees in the city park.

More than 80 representatives of civil society and human rights activists in Kyrgyzstan, including the Legal Clinic Adilet, appealed to the government to release female activists, but they received no official response.

69. Atyr Abdrakhmatova, Facebook post, October 23, 2022, https://www.facebook.com/permalink.php?story_fbid=pfbid02qg1SBidUNCaEPoV8yAs72cotuPHMGqy57ajXQzbCKBM3oqpfrJGgSpvLiTD7DHRhl&id=676656558.

70. "The Unfreedom Monitor: Kyrgyzstan Country Report," Global Voices Advox, June 2023, pp. 18-20, https://globalvoices.org/wp-content/uploads/2023/08/Unfreedom_Monitor_Kyrgyzstan_Country_Report_2023_updated.pdf.

International organisations such as Human Rights Watch, the International Partnership for Human Rights (IPHR), Civil Rights Defenders (CRD), Norwegian Helsinki Committee, and the International Federation for Human Rights (FIDH), expressed their concerns about 20 mass detentions, called the Kyrgyz government to release detained activists and to observe international human rights law. Embassies of the US, the UK, Germany, France and the EU representative office in Kyrgyzstan also released a joint statement on the International Day to End Impunity for Crimes against Journalists. The statement called on the Kyrgyz government to ensure freedom of media and freedom of expression.

Advocacy: Kyrgyzstan has a relatively robust and experienced civil society and political opposition. While the current government may be working to diminish activist power and effectiveness, they are currently at relatively early stages of repression. Consequently, there have been significant efforts on the part of both domestic and international advocates to document, resist, and protest against state repression related to this incident.

Advocacy efforts in Kyrgyzstan cut across a range of legal and technological concerns. They involve several proposed and recently passed laws, including on information, on media registration, and on "foreign agents," all of which focus on national legislation. They also involve efforts to get governments to follow existing laws; the incident, for example, includes a warrantless wiretap.

There are also numerous points of advocacy around governmental transparency, including state methods used to block websites, transparency of the process by which blocks are applied, and transparency about the both online and real-world surveillance practices. These issues are not only about the laws themselves, but the rules by which laws are administered and overseen, and about processes for state accountability.

Additionally, the state is using social media platforms for information operations, disinformation and smear campaigns, and populist mobilisation. These actions suggest the need for advocacy with social media companies, especially as the government is unlikely to create any conditions that constrain its own behaviour.

Advocacy to support fundamental rights — in this case, freedom of expression and the press — as asserted through numerous international and regional agreements and entities, remains an important, though infrequently successful, approach to securing national rights. Kyrgyzstan is a signatory to numerous key agreements and in theory is obligated to respect fundamental rights. However, international pressure can backfire, as populist authoritarians who espouse nativist narratives can use foreign advocacy to paint local activists as agents of foreign powers.

ACCESS

ACCESS

TURKEY

In December 2021, an article added to law No. 5894 (Law on the Establishment and Duties of the Turkish Football Federation) granted the Turkish Football Federation the authority to block access to broadcasts and URLs in case the federation determines the broadcasts to be illegal.

Incident: Turkish state grants the Turkish Football Federation the right to block websites

STATE BEHAVIOUR

Action: An article added to law No. 5894 granted the Turkish Football Federation the authority to block access to broadcasts and URLs

Goal: Expands censorship authority to other governmental institutions without court involvement

Political and legal justification: Although opposition legal experts call this "clearly unconstitutional," it is justified based on stopping piracy

Narrative that support the action: "Blocking apps, websites and other forms of access to sensitive information is justified by national security reasons," and "Freedom of expression is not an absolute right"

Technology applied: Website and URL blocking

Themes: Legislation

Social controls: Internet controls, surveillance, technology controls, freedom restrictions

Harms: Creates a precedent to allow more entities to censor online content they dislike

Who is harmed: IP pirates, but, more broadly, this implicates the rights of all citizens

PUBLIC RESPONSE

Counter-action: The Constitutional Court ruled that access blocks on some of the news stories published in 2021 violated their rights and that the relevant authorities should pay the non-pecuniary damages and court expenses.

Advocacy: Human rights lawyer Kerem Altiparmak called the decision 'completely unconstitutional'

Counter-narratives: "States must not engage in censorship," The press freedom crisis is being compounded by increasing digital censorship"

Incident: Turkish state grants the Turkish Football Federation the right to block websites.[71]

Country: Turkey

Tagline: Normalisation of authoritarian practices by extending the authority to censor to multiple entities.

Themes: This incident concerns internet access, and focuses on the use of legislation to restrict freedom of information and freedom of expression.

Summary of the incident: In December 2021, an article added to Law No. 5894, the Law on the Establishment and Duties of the Turkish Football Federation, granted the Federation the authority to block access to broadcasts and URLs whenever the federation determines them to be illegal.

This incident, narrowly construed, focuses on granting the federation the power to restrict the illegal sharing and broadcast of football matches. However, this power also grants the federation the right to censor the internet without a court order, and without notification, and the possibility of applying arbitrary judgments without oversight. The regulation gives the board of directors of the federation the authority to block URLs and entire websites without oversight from the courts. The federation shares its decision with the Access Providers Union, which enforces the block. Once blocked, the decision can be appealed at the Criminal Court of Peace. By February 2022, the federation had blocked access to 866 websites.[72]

71. UM_Incident_36.

72. "TFF harekete geçmişti: 866 siteye erişim engeli," Cumhuriyet, February 2, 2022, https://www.cumhuriyet.com.tr/spor/tff-harekete-gecmisti-866-siteye-erisim-engeli-1910068.

Similar powers were granted to the National Lottery in the past. Seen in context, granting censorship authority to other agencies expands the already robust idea in Turkey that censorship is an accepted practice.[73]

According to a 2021 Media Research Association report, censors remove at least three news items daily. These stories often focus on corruption or due process irregularities, and are often related to President Recep Tayyip Erdoğan, his family or AKP officials.[74] Turkey had blocked access to over 574,000 internet domains by December 2021.[75]

Social controls: The origins of legislation that restricts expression online have a long history, rooted in the 1991 "Informatics Bill," which set the stage for criminal prosecution for online expression, and the government has been blocking websites since at least 2007.[76] Since Erdoğan's ascendance to power, Turkey has passed progressively harsher legislation that supports a range of powers to censor expression and restrict access to information. Most power to regulate is presently assigned to the Information and Communication Technology Authority (BTK), while the Radio and Television High Council (RTÜK) has the authority to monitor online broadcasting.[77]

As such, the enabling environment for restrictions of rights by legal, extra-legal, and technological means is in full bloom in Turkey. The state has robust surveillance, internet blocking, and state repression capacity to control online communications and broadcasting activities. As stated in the Unfreedom Monitor Turkey Country Report, the Turkish state mutes critical public discussion through a "combination of traditional forms of censorship such as arrests, detentions, intimidation, and critical legal amendments combined with a crackdown on the internet using high level opaque administrative and judicial decisions blocking, banning, withholding online content."[78]

Narrative frames: Turkey's government justifies its access restrictions through appeals to national security, sovereignty, public morals and health, and as rejoinders to claims by rights defenders that blocking internet access harms the fundamental rights of expression and access to information.

"Blocking apps, websites and other forms of access to sensitive information is justified for national security reasons."[79] This narrative argues that website takedowns and blocking of social media content, apps and websites are justified for national security reasons. In Turkey, where cases of censorship are rampant and violations of rights and freedoms are common, citizens are left with government-approved media whose reporting may be biased, unverified, or simply a continuation of government rhetoric.

---

73. Arzu Gebullayeva, "Trace Turkey's path to normalizing the practice of blocking news websites," Global Voices, June 3, 2022, https://advox.globalvoices.org/2022/06/03/trace-turkeys-path-to-normalizing-the-practice-of-blocking-news-websites/

74. "Impact of Social Media Law on Media Freedom in Turkey Monitoring Report," Media Research Association, September 2021, https://medarder.org/wp-content/uploads/2021/09/Impact-of-Social-MediaLaw-on-Media-Freedom-in-Turkey-Monitoring-Report.pdf. Gebullayeva, Ibid.

75. Engelliweb, accessed June 2023, https://ifade.org.tr/en/publications/reports-books/.

76. Unfreedom Monitor Turkey Country Report, Global Voices Advox, August 2022, p.6, https://globalvoices.org/wp-content/uploads/2023/08/Unfreedom_Monitor_Turkey_Country_Report_2022_updated.pdf.

77. Gebullayeva, "Trace Turkey's path to normalizing the practice of blocking news websites."

78. Unfreedom Monitor Turkey Country Report, p. 6.

79. UM_NarrativeFrame_153.

Authorities also use national security as grounds for enacting legislation governing the internet. Examining this narrative frame allows us to understand the nuances and cases of possible misuse. Researchers also found this narrative in India, Philippines, Russia, and Iran.

"Freedom of expression is not an absolute right."[80] This argument in favour of restrictions on freedom of expression is used by governments not only to persecute people for acts of expression, but to restrict access. This narrative frame has been a catch-all to restrict dissent and opposing voices in numerous contexts, and functions as a rejoinder to arguments for robust protections of rights universally acknowledged in numerous international agreements. Researchers found this frame in Brazil, India, Zimbabwe, Hungary, Tanzania, Myanmar, China (and Hong Kong), Turkey, Cameroon, Kazakhstan, Iran, Philippines, Rwanda, Kyrgyzstan.

Counter-narrative frames: Turkish political opposition, journalists and rights activists have put forward numerous arguments against the normalisation of restrictions on internet access, including both narratives that support universal rights and claims specific to Turkey. Following is a subset of those frames.

"States must not engage in censorship."[81] This narrative asserts that states should not censor the media and citizens' expression. This narrative relates to the overall state of censorship and specifically the state's crackdown on media and internet freedoms while deploying various tools at its disposal, including legislative amendments, punitive measures, bogus charges, and surveillance tools. In July of 2021, the Turkish government announced plans to regulate foreign-funded media and misinformation. In 2022, a new social media law came into effect that will have a lasting impact on digital rights and freedom of expression in Turkey. Researchers also found this argument in Egypt, India, Russia, Tanzania, and Sudan.

"The judiciary is helping to censor online activity."[82] This narrative, asserted by activists and opposition members in Turkey, claims that the judiciary is not independent and uses its powers to censor online activity. The judiciary is supposed to play an important role in guaranteeing basic freedoms such as expression, information, opinion, and access. When they fail to do so, it is important that there is robust acknowledgement of, and discussion about, this failure in the media discourse. Turkish criminal peace judgeships were established in 2014, replacing previous criminal courts of peace without retaining their prerogatives. Since then, they, as the frontline courts that authorise decisions restricting rights to liberty and other rights, have often been criticised for violating human rights.[83] The decisions reviewed for the purpose of this research indicate that these courts authorise access blocks for news items that cover corruption allegations, fraud, governance issues, and LBGTQ+ rights and freedoms.

80. UM_NarrativeFrame_159.

81. UM_NarrativeFrame_118.

82. UM_NarrativeFrame_119.

83. "The Turkish Criminal Peace Judgeships and International Law," International Commission of Jurists, 2018, https://www.icj.org/wp-content/uploads/2019/02/Turkey-Judgeship-Advocacy-Analysis-brief-2018-ENG.pdf.

"The press freedom crisis is being compounded by increasing digital censorship."[84] This narrative expresses the belief that the deterioration of press freedom in many countries is being exacerbated by increased digital censorship. The narrative frame asserts that digital censorship and press freedom are intricately linked — that even though digital censorship applies to everyday citizens and not media outlets, it affects media freedom disproportionately and leads to a culture of self-censorship that worsens press freedom indirectly. Researchers also found this narrative in Egypt and Venezuela.

"The state is using national legislation to silence online dissent."[85] The assertion is that the state is using legislation, including vague hate speech laws, to punish any form of online dissent. Some countries justify the criminalisation of dissident voices through these vague regulations, so it is important to analyse detentions, arrests, exiles and other types of legal procedures within authoritarian regimes.

Countries around the world endorse regulatory systems to deal with speech that could be branded as hateful, most of which is framed in conventional speech law. However, some governments may take advantage of "hate laws" to persecute criticism and crack dissident voices. Since each country has a different regulatory system, they also apply different strategies in their individual contexts. Researchers also found this narrative in Turkey, Venezuela, Philippines, Kenya, Russia, Egypt, Zimbabwe, and Tanzania.

"It is never acceptable for governments to block websites and other online content."[86] Closely related to arguments that internet shutdowns are never acceptable, this narrative makes the claim that there are almost no circumstances under which governments can reasonably block websites and infringe on the right to freedom of expression. This narrative raises concerns about the use of digital tactics to enforce censorship. Researchers also found this narrative in Egypt, Venezuela, India, Myanmar, China (and Hong Kong), Tanzania, Sudan, Philippines, Russia, and Ecuador.

Counter-action: The Turkish human rights lawyer Kerem Altiparmak called the decision to empower the Turkish Football Federation with authority to censor "completely unconstitutional."[87] Yet constitutional redress appears to be slow and perhaps unworkable.

A pilot ruling by the Constitutional Court in October 2021, which predates the regulation that grants the federation the authority to censor, ruled that access blocks on some of the news stories published in 2021 were in violation of their rights and that the relevant authorities should pay non-pecuniary damages as well as court expenses. If sustained, this ruling has the potential to lessen censorship and blocking of internet access.[88]

84. UM_NarrativeFrame_120.

85. UM_NarrativeFrame_51.

86. UM_NarrativeFrame_148.

87. UM_Incident_36.

88. "Turkey's top court urges Parliament to eliminate structural problems within a year," Bianet English, January 7, 2022, https://bianet.org/english/law/255916-turkey-s-top-court-urges-parliament-to-eliminate-structural-problems-within-a-year.

Advocacy: Turkey has a substantial network of citizen's rights supporters, activists, journalists and lawyers working to document threats to fundamental rights. Research and reporting networks such as the Free Web Turkey and the Freedom of Expression Association, and the Initiative for Free Expression maintain projects that track internet controls, legislation, extra-legal activities, applied technologies, and other social controls.[89] Regardless, internet censorship, together with information access restrictions, has grown steadily. Today the state can block any content it deems critical, or that allegedly threatens national security interests. Critics can end up behind bars for what the state perceives as an "insult" to ruling party members or government institutions.[90] Advocates for the reinstatement of fundamental rights, and for policies that restrict governmental use of technologies for authoritarian purposes, may well end up being targeted by the state for their efforts.

Advocacy efforts to reverse Turkey's authoritarian practices face a daunting array of existing laws and a thicket of technological applications used by the state, with little to no transparency about their extent, capabilities, and function. Turkey stopped publishing data about the number of websites it blocks in May 2009, without explanation.[91] The Turkish government is known to employ spyware to hack and track activists, journalists and opposition political groups, including products made by Finfisher, Hacking Team, and the NSO Group. They also use facial recognition software linked to CCTV cameras, and employ public digital surveillance tools such as deep packet inspection and middleboxes.[92] Evidence for these claims usually comes from internet monitoring by activist groups and leaked documents, rather than through the government's acknowledgement of its methods.

In the absence of transparency, The Freedom of Expression Association and its EngelliWeb (Disabled Web) have taken on the task of tracking web blocks, and others such as Citizen Lab document internet throttling, press restrictions, and other forms of information and speech suppression, as well as the targeting, detention and arrest of individuals.[93] International freedom of expression and information access groups as well as international organisations, such as the Organization for Security and Co-operation in Europe (OSCE), also document Turkey's offences against freedoms, and issue statements of concern. Documentation and related advocacy, however, rarely affect the decisions of Erdoğan's government, which operates with a great deal of impunity.

89. Free Web Turkey: https://www.freewebturkey.com/index.php. Freedom of Expression Association: https://ifade.org.tr/en/. Initiative for Freedom of Expression: http://www.dusun-think.net/.

90. UM_NarrativeFrame_120.

91. Unfreedom Monitor Turkey Country Report, Global Voices Advox, p. 6.

92. Steven Feldstein, "Governments Are Using Spyware On Citizens. Can They Be Stopped?" Carnegie Endowment for International Peace, July 21, 2021, https://carnegieendowment.org/2021/07/21/governments-are-using-spyware-on-citizens.-can-they-be-stopped-pub-85019. Abdullah Bozkurt, "Turkey uses facial recognition to spy on millions, secretly investigates unsuspecting citizens," Nordic Monitor, September 20, 2021, https://nordicmonitor.com/2021/09/turkey-uses-facial-recognition-to-spy-on-millions-secretly-investigates-unsuspecting-citizens/. Thomas Brewster, "Is An American Company's Technology Helping Turkey To Spy On Its Citizens?" Forbes, October 25, 2016, https://www.forbes.com/sites/thomasbrewster/2016/10/25/procera-francisco-partners-turkey-surveillance-erdogan/?sh=a0e998444345

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

INFORMATION

INFORMATION

BRAZIL

The Brazilian Federal Police told the Supreme Court that a "digital militia" operates to attack institutions and democracy, using the structure of presidential aides and allies that operate from within the presidential palace. This information was part of a preliminary report the Federal Police delivered to the Supreme Court, where a probe related to the digital militias is also ongoing.

Incident: Brazilian Federal Police tells Supreme Court that "digital militia" is behind attacks on democracy

STATE BEHAVIOUR

Action: Use of misinformation techniques to attack and target political opposers

Goal: Ensuring financial and/or partisan benefits to the people involved

Political and legal justification: Bolsonaro and his allies have mostly denied that they are involved in falsifying information and spreading false news. 2021

Narrative that support the action: "Disinformation is not only a right-wing problem," "Bolsanaro's supporters are being unfairly targeted for their online activities," and two more.

Themes: Disinformation and misinformation, coordinated inauthentic behaviour and influence campaigns

Social controls: Information manipulation

Harms: Targeted with false rumors, targeted with character assassination

Who is harmed: Political opponents, Supreme Court justices, members of the government itself, political dissidents, journalists

PUBLIC RESPONSE

Counter-action: A police investigation is ongoing and should be the topic of discussion in the Senate in the near future

Counter-narratives: "Digital militias are forcing democratic institutions into positions that undermine democracy," "Private citizens and businesspeople should not sponsor disinformation and defamation campaigns"

Incident: Brazilian Federal Police tells Supreme Court that a "digital militia" is behind attacks on democracy.[94]

Country: Brazil

Tagline: This incident discusses political influence operations run by the Bolsonaro administration in the years 2019–2022 that are alleged to have illegally used state resources, and ongoing investigations of the matter by the Federal Police and the Supreme Court.

Themes: This incident concerns misinformation and disinformation, and influence campaigns.

Summary of the incident: In February 2022, Brazil's Supreme Court authorised public access to a report written by the Federal Police that concluded that the Bolsonaro administration had "orchestrated action" to identify targets, and create and spread disinformation for "ideological, party-political and financial gains." The report alleged that the administration had worked with a shadowy group of government advisors and media influencers popularly known as the "Hate Cabinet" or "digital militia." This group created campaigns on social media platforms such as Twitter, Telegram and WhatsApp.

The report originated in Supreme Court Justice Alexandre de Moraes' investigation of Bolsonaro's information operations, popularly known as the "Digital Militias Investigation."

94. UM_Incident_21.

The digital militia gained influence by disseminating misinformation, promoting hate speech, and launching coordinated attacks on political opponents. These tactics were aimed at shaping public opinion, sowing division, and undermining democratic institutions.

The use of influence campaigns in Brazilian politics is not new. Long before Jair Bolsonaro took office, politicians across the political spectrum had worked legally with media influencers to promote their agendas online. However, using state infrastructure and funds to promote the president's agenda through information operations and campaigns is unprecedented in the history of Brazilian politics.

The investigation was initiated based on a request from the President of the Parliamentary Commission of Inquiry (CPI) into the COVID-19 pandemic in the Federal Senate that President Bolsonaro be investigated in relation to the crimes identified in the final report of the CPI. In his decision, Justice de Moraes stated that "there is no doubt that the reported conduct of the President of the Republic, in the sense of spreading fraudulent news about vaccination against Covid-19, use the modus operandi of mass dissemination schemes on social networks."[95]

As noted in the Unfreedom Monitor Brazil Country Report,[96] the group behind the operation is alleged to consist of government aides operating from within the former presidential compound in Brasília. Details regarding how the group operates were made public through either material leaked from the judicial and police investigations or by former Bolsonaro loyalists who have since left the administration. The three key persons named in the investigations are presidential aides who are also close to Carlos Bolsonaro, one of the president's sons.

Social controls: Key to understanding this phenomenon is acknowledging that information manipulation generally thrives in Brazil, even in the absence of regulatory support or technical changes in the communications infrastructure. Unlike authoritarian regimes that rely on force and coercion, the digital militia achieves its objectives by exploiting existing vulnerabilities in modern communication technologies and infrastructures. A combination of low digital literacy among segments of the population and the widespread availability of social media platforms has also provided fertile ground for propaganda campaigns.

The digital militia's success is further bolstered by its close ties to the government and government-aligned media. The Hate Cabinet Investigation revealed disturbing connections between high-ranking officials and the network of individuals involved in spreading misinformation and hate speech. This symbiotic relationship facilitated the dissemination of a distorted narrative that amplified the government's agenda, while discrediting dissenting voices and the press. The consequences of this manipulation of information cannot be understated: by exploiting existing societal divisions and stoking hatred, the digital militia undermined social cohesion and eroded trust in democratic institutions. Moreover, it created an environment in which critical thinking and open dialogue are stifled, making it increasingly difficult for citizens to distinguish fact from fiction.

---

95. Decision note written by Minister Alexandre de Moraes.

96. Laís Martins, The Unfreedom Monitor: Brazil Country Report, April 2022, https://globalvoices.org/wp-content/uploads/2023/08/Unfreedom_Monitor_Brazil_Country_Report_2022_updated.pdf.

Narrative frames: Attempts by the judiciary to curb disinformation and misinformation and influence operations on both social media and mass media are often vilified by sectors of society aligned with Bolsonaro as "censorship." Bolsonaro allies who justify these practices also claim that the Supreme Court supports censorship. The use of pro-freedom narratives to support authoritarian practices is highly disingenuous in its pretence that hate speech, trolling, doxxing, and threats of violence are innocent in their effects, and do not shut down the speech of others.

"Disinformation is not only a right-wing problem."[97] This narrative argues that left-wing parties and groups are also involved in promoting disinformation and conducting influence campaigns, either by producing, coordinating, or sponsoring them. This narrative frame is based on false equivalence, acknowledging disinformation as a hypothetical problem, but justifying its use as part of a response to alleged left-wing activities. It attacks the idea that coordinated influence campaigns, or the coordination of the digital militia, are primarily the practice of centre-right and far-right groups. A key figure linked in the dataset is Carlos Bolsonaro,[98] one of President Jair Bolsonaro's sons and reportedly responsible for his father's social media, as a major proponent of this view. In the dataset, this argument was specific to Brazil, but it is also found in other national contexts.

"Investigations into coordinated behaviour on social media are an effort to regulate the internet and curb free speech."[99] This narrative argues that investigations into online coordinated behaviour such as influence campaigns or mis/disinformation are an excuse to pass legislation that regulates the internet and curbs free speech. Some segments of society assert that investigations into influence operations are just a pretext to clamp down on rights. This inversion of the causal chain creates a false narrative about internet regulation. In Brazil, this argument is put forward by right-wing actors who are themselves targeted, or have political allies being targeted, by police and court investigations for engaging in allegedly malicious coordinated behaviour, including attacks against democratic institutions. In the dataset, this narrative frame is specific to Brazil.

"The judiciary should not abuse its powers."[100] This narrative argues that judicial authorities, such as the Supreme Court, should not overstep their legitimate authority, as this creates an imbalance in democracy. This assertion has been used by right and far-right groups in Brazil to characterise investigations into the behaviour of political leaders aligned with their beliefs as political persecution and censorship.

"Bolsanaro's supporters are being unfairly targeted for their online activities."[101] This narrative makes the claim that supporters of former President Jair Bolsanaro are facing an unreasonable degree of persecution for their online activities. Federal Police and Supreme Court investigations into Bolsonaro-affiliated influence campaigns have prompted Bolsonaro and his associates to claim that their supporters are being targeted only because they support him, and are harmed by the Supreme Court and by the big tech platforms that

97. UM_NarrativeFrame_22.

98. UM_PeopleEntities_32.

99. UM_NarrativeFrame_97.

100. UM_Incident_21.

101. UM_NarrativeFrame_12.

enforce court rulings. This narrative of political persecution and denial of fundamental rights inverts the argument often put forward by authoritarian governments seeking to restrict expression and internet access. The narrative elides the distinction between expression and coordinated influence campaigns that function to silence others through hate, threats of violence, and disinformation. In the dataset, this narrative frame is specific to Brazil.

Counter-narrative frames: Opponents of the Bolsonaro administration's use of state resources to run influence and disinformation campaigns make the highly context-specific claim that specific individuals and groups benefit from these practices. They also, more significantly, emphasise that the use of freedom of expression claims has the potential to undermine trust in Brazilian democracy and its ability to defend fundamental freedoms, leading courts and regulators to restrict some speech rights in an effort to shut down hateful and disinforming expression.

"Private citizens and businesspeople should not sponsor disinformation and defamation campaigns."[102] This narrative asserts that private citizens, businesses, or businesspeople should not sponsor disinformation and defamation campaigns. At the core of this narrative is a call for transparency and clear boundaries between the private and public spheres, as coordinated disinformation or hate campaigns work for the benefit of those who orchestrate them. Several business leaders in Brazil are under investigation[103] for their alleged support of pro-Bolsonaro misinformation operations, on the premise that, by keeping Bolsonaro in power, they will benefit from tax breaks and more corporate freedom. These efforts go beyond the usual business influence in politics; They degrade the information environment in the name of business interests. Researchers also found this narrative in Zimbabwe and Iran.

"Digital militias are forcing democratic institutions into positions that undermine democracy."[104] This narrative argues that democratic institutions such as the Supreme Court and Congress are being forced into a position where they must take extreme measures that may undermine democracy in order to combat the destabilising activities of digital militias.

The work of the digital militia includes coordinated online smear campaigns, libel, disinformation, and targeted attacks against specific figures. Many of these actions are justified with narrative frames that support "freedom of expression." This claim provokes responses from democratic institutions, especially the Supreme Court, that opponents call disproportionate and authoritarian. The judiciary finds itself in a complicated position where it becomes both the target and judge of the attacks emanating from the right. In the dataset, this narrative frame is found only in Brazil.

Counter-action: The Federal Police investigation brought clarity to how the digital militias and the Hate Cabinet operate, but it wasn't the first time those practices became known in Brazilian society. News outlets have been covering the use of political coordinated campaigns on social media since the start of the Bolsonaro administration.

102. UM_NarrativeFrame_120.

103. UM_Incident_21.

104. UM_Incident_21.

Journalistic coverage is a key aspect of this incident. Out of 26 records in the dataset showcasing how the issue reverberated in society, 14 come from editorial media. The incident was a part of the media discussion throughout the presidential campaign before the election in October of 2022.

Advocacy: In Brazil, advocacy efforts are actively working to preserve digital rights and build fair and inclusive information ecosystems. Civil society organisations, universities, media, and journalism initiatives, legal and policy measures, international collaboration, and education and media literacy activities are part of these efforts.

The Institute for Technology and Society of Rio de Janeiro (ITS-Rio) is an example of an organisation carrying out research and innovation. Observing the growth of inauthentic behaviour in social networks, the institute has developed tools such as the so-called PegaBot to identify real or false accounts.[105] Research groups have used the tool in their investigations on digital militias in Brazil.[106]

At the beginning of investigations into the Hate Cabinet there was little public advocacy, mostly due to the ongoing status of the investigations.[107] However, Brazilian news organisations and media outlets played a critical role in reporting on the Hate Cabinet and its operations. Through investigative reports, fact-checking, and reporting on the strategies and repercussions of digital misinformation, civil society gained access to details that are key to understanding this entity.

105. https://pegabot.com.br/.

106. Joao Guilherme Bastos dos Santos et. al., "Das milıcias digitais ao comportamento coordenado: metodos interdisciplinares de analise e identificac¸ ao de bots nas eleicoes brasileiras," Instituto Nacional de Ciencia e Tecnologia em Democracia Digital, August 2021, https://itsrio.org/wp-content/uploads/2021/08/16138-553-12848-1-10-20210709.pdf

107. Márcio Falcão, "Moraes prorroga investigações sobre omissão nos ataques de 8 de janeiro e milícias digitais no STF", published on February 27, 2021 at G1: https://g1.globo.com/politica/noticia/2023/02/27/moraes-prorroga-investigacoes-sobre-omissao-nos-ataques-de-8-de-janeiro-e-milicias-digitais-no-supremo.ghtml

appendix

A

GLOSSARY

INCIDENTS - CONTROLS

(NOTE: definitions are written to make sense regardless of whether the controls are employed in the service of legitimate governance or authoritarian practice. What makes surveillance authoritarian, for example, is a lack of transparency, proportionality, and accountability.)

B

Bandwidth throttling

Intentional slowing of internet speeds to restrict access

C

Coordinated inauthentic behaviour

A definition that originates with Facebook, and describes multiple users, including bots, who misrepresent themselves and collaborate in the service of an agreed goal, such as spreading misinformation or engage in behaviours designed to enable other violations under the platform's community standards, and where the use of fake accounts is central to the operation (The Media Manipulation Casebook)

D

Data

Restrictions on user control of or rights over personal data

DDOS

Flooding a network with internet traffic, thereby preventing access for users

Device-based surveillance

Using devices such as phones and laptops to spy on the activities of people

appendix

Disinformation

Intentionally false information shared for the purpose of deception

For example, a government's propaganda narrative that cites false statistics to boost its own image

E

Expression

Restricting the right to freedom of expression, such as public speech, media freedoms, and interpersonal communications, as defined in Article 19 of the Universal Declaration of Human Rights

F

Freedom Restrictions

Restrictions on a range of fundamental and widely supported international rights, using a variety of technological and regulatory approaches

I

Import restrictions

Government restrictions on imports of technology, goods and services

Influence campaign

Propaganda efforts that aim to shift or create public opinion and awareness about a subject

Information manipulation

The shaping of information ecosystems to restrict information access, encourage engagement with state information sources and narratives, and discredit or diminish legitimate, accurate information

Informants

Individuals with access to restricted or secret information who share details about persons of interest to authorities

Information ecosystem shaping

Creating information resources that have widespread influence over what information people consume, such as creating media outlets, social media platforms, or providing preferential information services

Examples include the Sputnik or RT networks, TruthSocial, false news outlets on YouTube.

Internet controls

A class of restrictions on internet access, from complete shutdowns to blocking of specific websites to filtering systems that censor terms, ideas, and names

Internet access restrictions

Blocking websites and applications, using filtering systems and similar technologies to control what information is accessible

Internet controls are about restrictions on the network side — ISPs, blacklists, throttling, keyword blocks, etc., rather than targeted attacks on the user side (DDOS etc.)

Internet of things

Surveillance and activity monitoring capabilities embedded in goods, such as CCTV cameras containing facial recognition software, smart doorbells, e-readers that track reading habits, and GPS systems

For example, surveillance cameras that are connected to systems and databases that allow information to travel quickly and widely

appendix

Internet shutdown

Blocking full access to the internet and digital communications, on the basis of technical infrastructure

We define a shutdown as a full restriction on all internet services, in order to differentiate between shutdowns and targeted restrictions on particular services, platforms, or websites, bandwidth throttling, and other partial restrictions

I

ISP controls

Blocking access to aspects of the internet, from individual websites, to keyword blocks on search terms, to geographic controls at the ISP level

M

Media

Restrictions on media rights and freedoms such as publication and dissemination, freedom from censorship, and from burdensome regulation

Misinformation

Unintentionally false or inaccurate information

Movement

Restricting the right to international and intrastate movement and residence as defined in Article 13 of the Universal Declaration of Human Rights

O

Online tracking

Tracking behaviour on the internet and telecommunications services using a range of technologies, from cookies embedded in websites to spyware

P

Phishing

Deceiving users into disclosing critical information

Physical surveillance

Directly monitoring activities by any means not involving electronic surveillance

Privacy

Freedom from arbitrary or unlawful interference with individual privacy as defined in Article 12 of the Universal Declaration of Human Rights

Public digital surveillance

Tracking the activity of people in public spaces and publicly available internet and communications spaces, through a variety of digital surveillance techniques

Techniques include ISP-level surveillance, data requests from websites and applications, tagging and monitoring malware, website scraping and content parsing, and other mass surveillance approaches

Punitive internet taxes

Taxes and fees that increase the cost of the internet or telecommunications in order to limit access

S

Social media access restrictions

Preventing access to some kinds of content on social media platforms

Access restrictions applied by social media platforms, either to users or to certain types of content (e.g. content removal requests)

Social media shutdown

Blocking access to social media platform(s)

Blocking occurs through regulation, infrastructure controls, or ISPs. For example, India's ban on access to TikTok

T

Surveillance

Persistent observation of populations in a variety of ways, such as monitoring video in person, monitoring online behaviours, or closely surveilling individuals digitally using spyware

System attacks

The use of technological and informational methods to shut down, damage, or restrict access to technologies for information access and communication

Technology controls

A class of restrictions on access to technologies, import/export licenses, registration requirements for technology services, network interference, or the use of spyware

Spyware is a piece of software that gathers and sends information about the computer it is installed on without the owner's consent or knowledge

appendix

B CIVIC MEDIA OBSERVATORY METHODS

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 Civic Media Observatory (CMO) offers a research method deployable in relation to key events and trends to find, assess, describe and analyse information. The approach is primarily qualitative and looks beyond socio-technical causes to consider power analysis, offer a way to discuss effects, and emphasise what works, as well as what is negative. It is a framework that can be consistently applied across a range of settings 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.

The research is grounded in the following:

LOCAL KNOWLEDGE — clarifies subtext and context

EDITORIAL RIGOUR — serves as a method to ensure that research analysis is impartial

CIVIC IMPACT SCORE — evaluates material based on potential benefit or harm to civic discourse, in accordance with international human rights norms

SUGGESTED ACTIONS — recommends a range of tactics to inform journalistic coverage, support content moderation and platform governance strategies, and help frame research, to promote the protection of human rights within the media environment

The core of the Civic Media Observatory is the INVESTIGATION — the focus of the research in a given instance. Investigations focus on THEMES — events, trends or phenomena.

appendix

Themes:
What people talk about

Frames:
How they talk about it

The researchers working on an Investigation classify, analyse and assign a measure of civic impact to MEDIA ITEMS — social and other online media, mainstream media and offline content — and suggest further ACTIONS to be taken.

Researchers also identify NARRATIVE FRAMES — the dominant narratives used to debate themes. This is an iterative process in which an initial set of narratives are identified and defined at the beginning of the research, and then refined in response to events.

Researchers work in AIRTABLE, a relational database, which allows for rich interlinking of media sources, themes, narrative frames, media items, and languages, as well as granular analysis of dozens of metadata fields we use to describe media items. This approach helps us to build consistent responses to questions about the accuracy, truthfulness, verifiability, and ideological leaning underlying media items, as well as deeper analysis of context, subtext, when warranted.

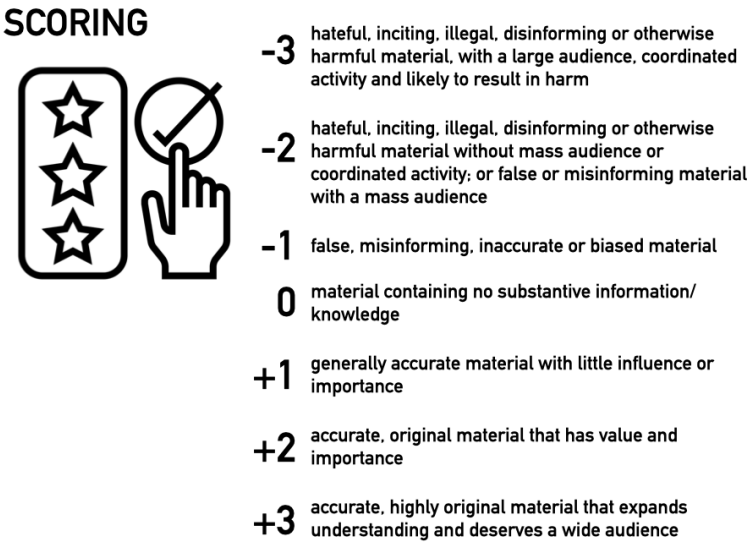
Researchers work together to discuss and edit their analysis, and every item is reviewed by at least two researchers.

The Civic Impact Score is a normative evaluation to categorise media items by potential benefit or harm to civic discourse, in accordance with international human rights norms. It is supported by analysis based on methodology questions.

This study employs research methods based on qualitative analysis of narrative themes and trends in mainstream media, social media, other online media, and other offline media. The research does not employ statistical methods and is not meant as a representative sample; all quantitative statements about the data refer only to the material in the set. For example, relatively few items in the dataset focus on surveillance. That lack is not meant as a reflection of the relative importance of surveillance, but a decision by the research team to focus on a relatively narrow set of themes and frames that, during the research period and due to the countries in focus, were sources of contention, national importance and provided story angles that are less prominent in mainstream media.

CIVIC IMPACT SCORE

The Civic Impact Score is a mechanism to help researchers evaluate the possible effects of a media item on civic discourse. The score serves as an indicator or guide based on researcher knowledge rather than as a calculated score based on a summation of other factors. Scores need to be supported by analysis and recommended actions. To guide the assignment of the civic impact score, researchers answer all CMO method questions that are relevant to a particular item and discuss why they assigned that particular civic impact score.[108]



The dataset offers numerous points of entry for curious readers and researchers interested in exploring relationships within the data.

To begin, note that the Airtable has interrelated tables: Incidents, Items, Media Sources, Themes, Narrative Frames, Synthesis Table, Stories, and Locations. Any of these tables can be a starting point for inquiry. It is useful to begin with an overview of the data in order to familiarise yourself with the possibilities for search. Themes and Narrative Frames are excellent starting points.

108. A coordinating editor (who is usually not part of the local research team), will check the analysis for logical consistency and will question a score that does not accord with the logic of the other questions. For example, if a researcher applies a positive civic score to an item that makes claims unsupported by evidence (an objective measure), that score will be questioned by the reviewer.

FILTERS

Airtable has a filter function, a flexible and powerful tool that allows users to sort the data according to their varied interests. Filters may be applied to any of the tables. Importantly, users may apply multiple filters in order to refine results.

ADVANCED TOOLS

Airtable offers other, powerful tools for sorting and comparing data. These include:

- **Views**, which allow users to create multiple selections of the data, in order to compare results or to present the data in other forms such as Gantt charts or Kanban boards, groups, field sorting, and colour codes.

- **Groups**, which allow users to, within a view, organise media items by specific fields. Like filters, users can add multiple nested groupings to view data in different ways.

Users can also download the data as a CSV file.


GlobalVoices
advox


The
Unfreedom
Monitor