# Digital Authoritarianism: ICT-enabled Repression Across Regime Types*

Lucaccini Martina[1,2,*]

[1]Sapienza Università di Roma
[2]Luiss Guido Carli

**Abstract**

Digital authoritarianism uses Information and Communication Technologies (ICTs) to sustain autocratic stability through surveillance, censorship, cyberattacks and social manipulation. While this phenomenon is central to modern autocracies, the borderless nature of cyberspace has enabled democratically elected states to adopt similar practices under certain conditions. Drawing on data from the Digital Society Project (DSP) and cross-national time-series analysis on the Digital Repression Index (DRI), this study reveals significant differences in the digital authoritarian toolkit across regime types. Closed regimes predominantly utilize tactics such as surveillance, social manipulation, and internet shutdowns, whereas democracies, despite possessing greater digital repression capacities, generally exercise restraint. However, when governed by illiberal leaders, democracies exhibit patterns of digital repression similar to their autocratic counterparts, challenging assumptions about the normative divide between regime types.

**Keywords**

cyber politics, geopolitics, authoritarianism, technologies

## 1. Introduction

In the 1990s and early 2000s, scholars defined the World Wide Web as a virtual Habermasian public sphere fostering democratisation [1, 2, 3]. Today, the Internet has not brought the hoped-for liberalization, and authoritarian regimes are instrumentalizing it to serve state-defined interests [4, 5]. Recent research suggests that digital authoritarian practices—such as internet censorship, shutdowns, government disinformation on social media, and social media surveillance—are now fundamental characteristics of modern autocracies [6, 4, 7]. However, some of these practices are also utilized in democracies exceptionally [8, 9] or inherently [10, 11, 12]. This article defines *digital authoritarianism* as a broad term that includes tactics to manipulate, monitor, and control the online space. Similarly to offline authoritarianism practices, these online tactics can potentially reinforce the authoritarian pillar of stability and take hold in democracies. After theoretically conceptualizing its toolkit, the empirical section of the paper, based on the Digital Society Project [13] and Feldstein's Digital Repression Index (DRI) [14], sheds light on the diffusion of the digital authoritarian toolkit across regime types.

## 2. Defining Digital Authoritarianism

Despite the assumption that authoritarian rule systems [15] were incompatible with the media environment, regimes have swiftly shaped cyberspace [16] to their strategic advantage. Collecting the economic benefits of the Internet [17], they included technological breakthroughs in their authoritarian toolbox [18]. This process is defined as networking authoritarianism, data-driven authoritarianism, or digital authoritarianism. *Digital authoritarianism* refers to using digital information technology to surveil, repress, and manipulate domestic and foreign populations while retaining political control [19]. These governments have sought to manipulate and regulate citizens' engagement with these tools,

*Joint National Conference on Cybersecurity (ITASEC & SERICS 2025), February 03-8, 2025, Bologna, IT*
*Corresponding author.
martina.lucaccini@uniroma1.it (L. Martina)
0000-0002-0877-7063 (L. Martina)

| Challenges | Tools of Cooptation, Repression and Legitimation | | | | Tools of Great Power | |
|---|---|---|---|---|---|---|
| | *Surveillance* | *Censorship* | *Cyberattacks* | *Disinformation* | *Digital Infrastructure* | *Digital Sovereignity* |
| 1. Autocracies | | | | | | |
| 2. Transnational | | | | | | |
| 3. Export | | | | | | |
| 4. Democracies | | | | | | |

**Table 1**
A taxonomy of the digital authoritarian toolkit

as well as to leverage this technology for political gain. *First-generation controls* of the Internet were based on establishing national cyber-borders (e.g., examples include China, Iran, Pakistan, Saudi Arabia, Bahrain, Yemen, and Vietnam) and on filtering activities on keywords, servers, domains, and IP addresses to censor political and security-related content [20]. *Second-generation controls* extended through laws, regulations, and requirements imposed on privately owned networks (e.g., backdoor functionalities and deep packet inspections; banning anonymizing tools and VPNs). Often referred to as "just-in-time", they also granted dynamic Internet access management and plausible deniability [21]. *Third-generation controls* are offensive and undermine the networking advantages that civil society might otherwise gain from digital media by actively manipulating information (e.g., China's fifty-centers, Venezuela's communicational guerrillas, the Egyptian Cyber Army, the Syrian Electronic Army; the pro-Putin bloggers of Russia; Kenya's director of digital media, Saudi Arabia's ethical hackers) [22]. *Fourth generation controls* introduce an assertive international dimension of digital authoritarianism; in this context, the digital authoritarian toolkit is used for strategic competition among great powers.

## 2.1. Perpetual Agendas and Global Challenges

The stabilization strategies of authoritarian regimes have been convincingly theorized based on *legitimacy*, *repression*, and *cooptation* [23]. Authoritarian regimes adapt their perpetual agenda to the dynamics of cyberspace to *a)* obtain perfect information about their subjects and *b)* influence behaviour and beliefs so that their rule appears legitimate [8, 1]. Figure 1 illustrates how the three pillars of authoritarian stability are adapted in the digital age. *Digital repression* (i.e., influencing strategies for controlling the information environment) and *digital cooptation* (i.e., manipulation of potential sources of opposition) ensure citizens' compliant participation in society influencing their behaviors through positive incentives (e.g., social credit scores), sanctions (e.g., deplatforming, shadowbanning, hacking) or controlling the information environment (e.g., Denial of Service attacks and slowing access to the Internet) [20]. Regimes can also rely on covert practices when they attempt deception (i.e., through cooperation with Internet Service Providers to remove contents or use algorithms) or target specific individuals and organizations using spyware [24]. To control narratives and shape their subjects' beliefs, the autocrat's goal is to strengthen their *legitimation* and create a façade of participation and responsiveness to the dictators' rule. Dictators rely on information channelling (i.e., redirecting or influencing attention) and employ social media bots and trolls to spread pro-regime narratives (i.e., advanced by patriotic hackers or automated through bots and algorithms), disinformation (i.e., the dissemination of false, inaccurate, or misleading information) and flooding (i.e., promoting competing or distracting information that overwhelms legitimate information sources) [20, 10, 25].

Disaggregating Figure 1 to understand the *digital authoritarian toolkit* offers further insights. I defined a taxonomy that distinguishes between four practices reinforcing the classical pillars of authoritarian stability (i.e., surveillance, censorship, cyberattacks, disinformation) and two practices acting as tools of great power (i.e., digital infrastructure and sovereignty). Each of them draws from a unique set of tools to perform its objectives.

*Surveillance* has become faster to implement in the digital age. The availability of big data from both public and private sources, along with advances in algorithmic sophistication and artificial intelligence,

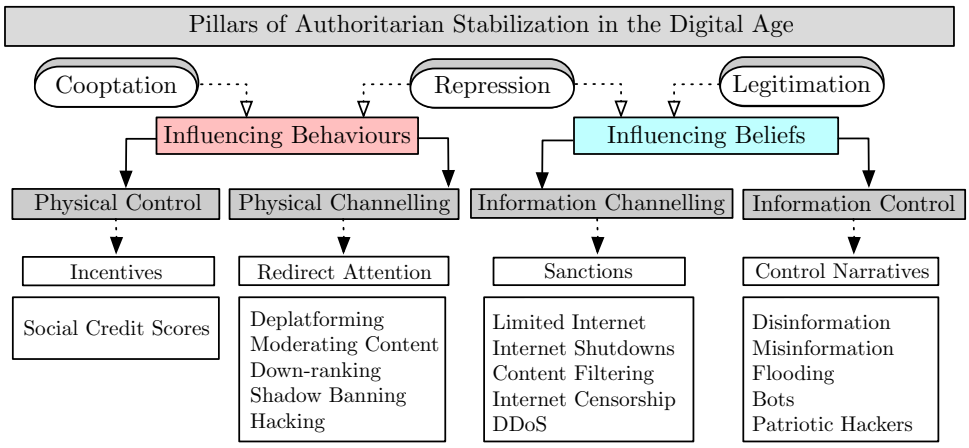


**Figure 1:** Theoretical framework: pillars of authoritarian stability in the digital age. Figure elaborated building on previous work by[20, 8].

has enabled enhanced data-gathering capabilities [26]. Surveillance helps predict the population's political preferences, as technology-driven incentives and punishment systems promote data sharing between tech companies and government agencies, impacting societal participation [27]. *Cyberattacks* such as DDoS, hacking, malware, and network intrusions enable covert data collection and suppress the voices of critics against regimes [28]. Some of these cyber-offensive capabilities, such as spyware, are available for purchase commercially [29]. *Censorship*, a long-standing authoritarian practice, continues to be a key component of the digital authoritarian toolkit. As repressors maintain centralized control of information [21], they regulate citizens' access to unwanted content through filtering mechanisms, Internet shutdowns and information control strategies [30]. *Disinformation* is a tool for social manipulation; for instance, autocrats can manipulate election processes using bot armies and defamation tools, create a fragmented information landscape, and strengthen their legitimacy [8]. *Digital infrastructure* gatekeeping allows hidden backdoor access to data transmitted through communication channels. Furthermore, while governments often present themselves merely as service providers, the infrastructures they supply inherently contain embedded norms and values. Digital dictators also prioritize *digital sovereignty*, data localization requirements and the adoption of authoritarian visions of the Internet to regulate the dissemination of information within their national borders [31].

Digital authoritarian practices are now defining features of modern autocracies [28]. Democratic governments have utilized similar practices *exceptionally* to enhance national security, combat disinformation, protect democratic institutions, and maintain public order [8]. However, in democracies like India, which often experiences Internet shutdowns claimed to be necessary for preventing violence [32], and the Philippines, where the Anti-Terrorism Act of 2020 was enacted [33], such practices can be misused to suppress political opposition, weaken independent media, and concentrate governmental power. In making this argument, I place significant emphasis on a well-established [12, 10, 34] practice-based[1] definition of authoritarianism, resulting in a broad definition of digital authoritarianism applicable across regime types. Today, digital authoritarianism presents four overlapping challenges. *First*, it is expanding within consolidated autocracies through digital surveillance, censorship, social manipulation, and advancing authoritarian visions of digital infrastructures and the Internet [31]. *Secondly*, digital authoritarian regimes direct their toolkit towards regime critics and opponents abroad; this transnational challenge enables regimes to suppress dissent and control populations at home and abroad [35]. *Thirdly*, regimes export surveillance systems, malicious software, and filtering capabilities to like-minded authoritarian states, setting international technology standards and advancing closed

[1]Practices are patterns of actions that sabotage accountability to people over whom a political actor exerts control, resulting in disabling access to information and disabling voices.

| Dependent Variables | Appliable Digital Society Survey Variable[41, 42] |
|---|---|
| **Surveillance Authoritarian Internet** | Government social media monitoring of political content (*v2smgovsmmon*[43, 44]) |
| **Censorship Authoritarian Internet** | Internet filtering in practice (*v2mgovfilprc*[43, 44])) |
| | Social media censorship of political content in practice (*v2mgovsncebprc*[43, 44])) |
| | Social media censorship of political content in capacity (*v2mgovfilcap*[43, 44])) |
| **Disinformation** | Governmental dissemination of false information on social media (*v2mgovsmcenprc*[43, 44])) |
| | Party dissemination of false information on social media (*v2govdom*[43, 44])) |
| | Governments'capacity to regulate online content using existing laws (*v2mregcap*[43, 44])) |
| **Cyberattacks Digital Sovereignity Digital Infrastructure** | Governments' social media shutdowns in practice (*v2mgovsm*[43, 44]) |
| | Governments' social media shutdowns in capacity (*v2mgovshutcap*[43, 44]) |
| | Internet shutdowns in practice (*v2mgovshut*[43, 44]) |
| | Targeted persecutions of online users (*v2smarrest*[43, 44]) |
| | Governments' cybersecurity capacity (*v2smgovcapsec*[43, 44]) |

**Table 2**
The Digital Authoritarian Toolkit measured by DSP Indicators

visions of the Internet [7]. *Fourthly*, digital authoritarianism practices are becoming pervasive in democratic societies at the expense of public trust, personal privacy, and civil liberties. While the XX century experienced waves of democratic liberalization, the emergence of digital authoritarianism reflects an opposite trend, affecting both autocratic and democratic regimes [11].

Table 1 summarizes the digital authoritarian toolkit and highlights which strategies within the taxonomy advance the four challenges listed above.

## 3. Research design and data

My empirical investigation provides a descriptive analysis to assess how practices of digital authoritarianism are utilized across different regime types. I refer to Feldstein's (2019) Digital Repression Index (DRI) and Digital Repression Capacity Index (DRCI) [36]. Both indexes assume values between -5 and 5, with 0 representing the approximate mean for all country years in the sample, and countries with negative scores generally perform below the mean. I rely on expert-coded data from the Digital Society Project (DSP) data set, incorporating survey data from 2003 to 2022 [13, 37]. This version of the variables presents country-year point estimates resulting in a probability distribution for each score on a standardized interval scale [38]). These scores resemble a normal score, typically ranging from -5 to 5, with 0 representing the mean across all country-years in the sample. As *dependent variables*, I selected the indicators listed in Table 2 as proxies for the components of the digital authoritarian taxonomy (see Table 1). Operationalization of the *independent variable* (i.e., regime type) is performed referring to the Varieties of Democracy (V-Dem) [39] (i.e., *v2x_polyarchy*, electoral democracy index; *v2x_libdem*, liberal democracy index) and the Regime of the World (RoW) classification [40] (i.e., *v2x_regime*, distinguishing between Closed/Electoral autocracies and Liberal/Electoral democracies). In this paper, I answer the following research question: How does the digital authoritarian toolkit vary in its use between autocracies and democracies?

## 4. Descriptive insights

### 4.1. Digital Authoritarianism Across Regime types

Scholars have used digital authoritarianism to describe what Feldstein (2019) [14] designates as *digital repression*. Unlike digital authoritarianism, this designation does not imply a bias toward a specific regime type. Democracies frequently employ digital repression techniques for a variety of reasons, even when there is no explicit intention to transition toward authoritarian governance models.

In line with existing scholarship, countries with poor human rights records show the highest global

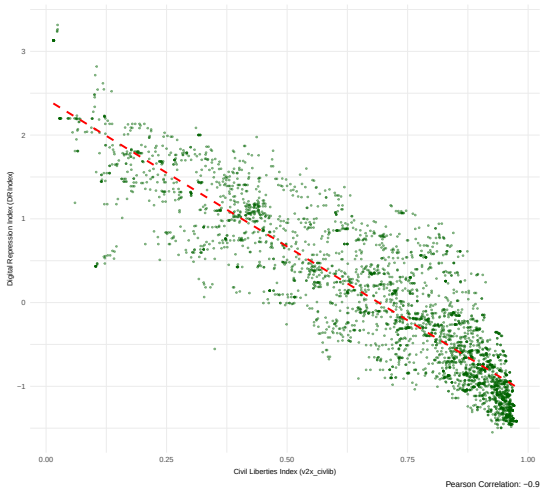


**Figure 2:** Linear Relationship, v2x_clpol and Digital Repression Index (DRI) [45].

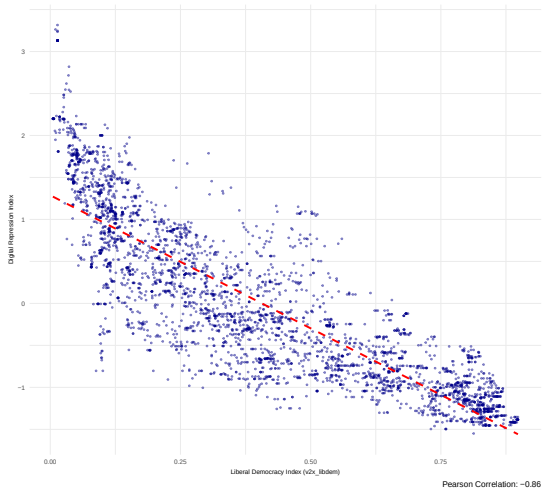


**Figure 3:** Linear Relationship, v2x_libdem and Digital Repression Index (DRI) [14, 43].

| | DRI | DRCI | v2x_regime | FoTN | | DRI | DRCI | v2x_regime | FoTN |
|---|---|---|---|---|---|---|---|---|---|
| North Korea | 3.3 | 2.6 | CA | Not Free | Sweden | -1.4 | 0.2 | LD | Free |
| Turkmenistan | 2.7 | 1.5 | CA | Not Free | Denmark | -1.4 | 0.9 | LD | Free |
| Eritrea | 2.2 | -0.04 | CA | Not Free | Norway | -1.3 | -0.01 | LD | Free |
| South Sudan | 2.1 | -0.6 | CA | Not Free | Portugal | -1.3 | 0.4 | ED | Free |
| Iran | 2.1 | 1.2 | CA | Not Free | Lithuania | -1.3 | 0.4 | ED | Free |
| China | 2.1 | 2.5 | CA | Not Free | Finland | -1.3 | -0.04 | LD | Free |
| Syria | 2.0 | 1.2 | CA | Not Free | Belgium | -1.3 | 0.4 | LD | Free |
| Myanmar | 2.0 | 0.8 | CA | Not Free | Latvia | -1.2 | 0.02 | LD | Free |
| Tajikistan | 2.0 | 0.8 | EA | Not Free | Netherlands | -1.2 | 0.2 | LD | Free |
| Nicaragua | 2.0 | 1.1 | EA | Partly Free | Uruguay | -1.1 | 0.7 | LD | Free |

**Table 3**
Countries with the highest and lowest values of DRCI and DRI, distinguished by their regime type and freedom of the Net (2022) [14, 46, 40].

levels of digital repression. Indeed, as civil liberties decline (*v2x_civlib*, an Index measuring restrictions on expression, political pluralism, and civil society 2), the level of digital repression increases. Similarly, there is a strong and statistically significant negative correlation (Pearson's Coefficient = -0.86) between the Liberal Democracy Index (*v2x_libdem*) and the DRI, suggesting that liberal democratic systems are associated with lower levels of digital repression (Figure 3). Figure 7 in the Appendix provides a deeper analysis of the correlation between DRI variables and V-Dem's Democracy Indices.

Figure 6 (see Appendix) provides an overview of the prevalence of digital repression across global regions in 2022. The two regions with the highest levels of digital repression in 2022 were South and Central Asia and the Middle East; in contrast, Europe and Eurasia and countries in the Western Hemisphere showed the lowest digital repression scores but higher digital repression capacity. In 2022, high-scoring countries in the DRI were exclusively closed or electoral autocracies (i.e., CA; EA) and classified as "Not Free" by Freedom House's Freedom of the Net (FOTN) Classification [46], except for Nicaragua (Table 3). In two cases (e.g., Eritrea and South Sudan), digital repression capacity does not fully align with digital repression scores. Low-scoring DRI countries in 2022 also align closely with regime types as they all classify as electoral and liberal democracies (i.e., ED; LD). There are inconsistencies (e.g., Finland) when countries possess advanced repression capabilities but choose limited deployment. Several countries with strong ED rankings have unexpectedly high digital repression scores (e.g., India and Brazil) due to their high levels of state-sponsored Internet Shutdowns and political party-driven disinformation [36]. Notably, electoral democracies and democracies ruled by illiberal leaders (e.g.,

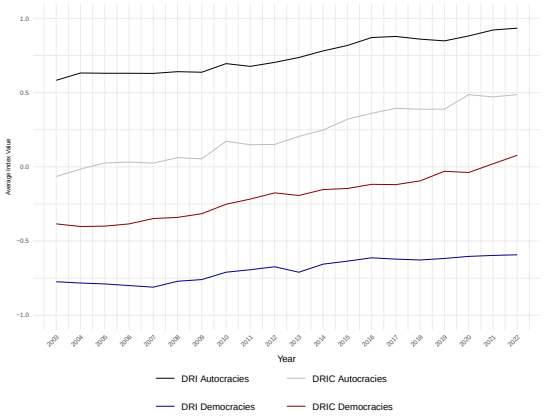


**Figure 4:** DRI and DRCI across regime types (2003-2022) [14].

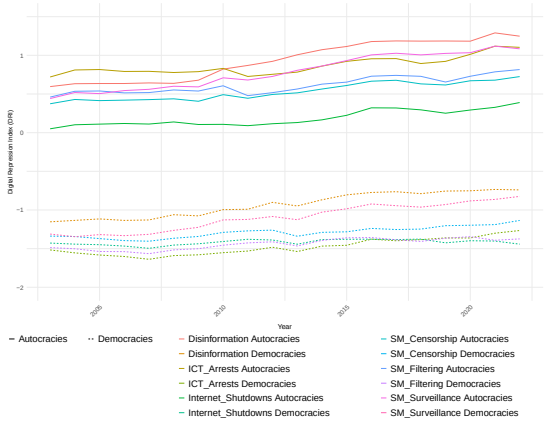


**Figure 5:** Evolution of the Digital Authoritarian Toolkit (2003-2022)[43].

| Country | Region | Regime | Internet Penetration | v2smarrest | v2smorgavgact | v2smgovsmmon | DRI | DRCI |
|---|---|---|---|---|---|---|---|---|
| Syria | MENA | CA | 49% | 3.1 | 1.3 | 2.4 | 2.1 | 1.9 |
| North Korea | EAP | CA | 0.1% | 2.9 | -3.5 | 3.7 | 3.3 | 2.6 |
| Bahrain | MENA | CA | 99% | 2.9 | 1.6 | 1.8 | 1.2 | 1.3 |
| Eritrea | AF | CA | 8% | 2.8 | -2.4 | 1.9 | 2.2 | -0.1 |
| South Sudan | AF | CA | 11% | 2.8 | -1.2 | 2.4 | 2.1 | -0.6 |
| UAE | MENA | CA | 99% | 2.5 | -2.5 | 2.1 | 1.7 | 1.8 |
| Qatar | MENA | CA | 100% | 2.4 | 2.8 | 1.9 | 1.3 | 2.1 |
| China | EAP | CA | 76% | 2.3 | 0.8 | 3.2 | 2.1 | 2.5 |
| Egypt | MENA | EA | 72% | 2.3 | 1.6 | 1.6 | 1.5 | 1.1 |
| Vietnam | EAP | CA | 79% | 2.3 | 1.7 | 1.5 | 1.0 | 1.3 |

**Table 4**
Countries with the highest levels of the targeted persecution of online users (*v2smarrest*) compared to their citizens' usage of social media to organize offline protests (*v2smorgavgact*)[45].

Turkey) can exhibit patterns of digital repression more akin to autocratic counterparts, and countries with poor democratic rankings can use digital repression markedly less than expected (i.e., Belarus and Thailand).

## 4.2. Comparing Digital Repression Capacity and Practice

The rising tendencies of digital repression capacity and enactment are not unexpected, as dissent has moved online and digital tools have become cheaper. Findings highlight the linear relationship between digital repression capacity and democracy levels (Figure 4). Liberal and electoral democracies have high capacities for digital repression but refrain from using it. At the same time, closed autocracies and electoral autocracies exhibit rising digital repression tendencies, with the toolkit's deployment consistently exceeding regimes' capacities. Still, democracies with higher repressive capabilities often have political safeguards to mitigate the risk of using these tools for political repression [47]. Differently, autocracies with lower repressive capacities usually bridge the digital repression gap by relying on external suppliers (as highlighted by challenges (2) and (3) in Table 2).

## 4.3. Breaking down the digital authoritarian toolkit

Authoritarian regimes rely differently on their digital authoritarian toolkit. Figure 8 displayed in the paper's Appendix provides a ranking of authoritarian regimes in terms of their reliance on digital repression practices. I considered authoritarian regimes currently in power as of 2022. I plotted the range of the minimum and maximum values reached by the DRI, the current value (2022), and the mean value the DRI assumed between 2003 and 2022. Figure 5 depicts the evolution of key components

| Country | Region | Regime | Internet Penetration | v2smgovshut | v2smgovshutcap | DRI | DRCI |
|---|---|---|---|---|---|---|---|
| North Korea | EAP | CA | 0.1% | 4.2 | 2.1 | 3.3 | 2.6 |
| Turkmenistan | SCA | CA | 38% | 2.8 | 1.3 | 2.7 | 1.5 |
| Sudan | AF | CA | 29% | 2.6 | -0.1 | 1.7 | 0.5 |
| South Sudan | AF | CA | 11% | 2.6 | -0.5 | 2.1 | -0.6 |
| Eritrea | AF | CA | 8% | 2.5 | 0.5 | 2.2 | -0.1 |
| Iran | MENA | CA | 84% | 2.4 | 0.7 | 2.1 | 1.2 |
| Ethiopia | AF | EA | 25% | 2.3 | 1.5 | 1.9 | 0.8 |
| Tajikistan | SCA | EA | 40% | 2.2 | 0.8 | 2.0 | 0.8 |
| Myanmar | EAP | CA | 46% | 2.2 | 1.9 | 2.0 | 0.8 |
| Yemen | MENA | CA | 18% | 1.7 | 1.2 | 1.8 | 0.5 |
| India | SCA | EA | 48% | 1.6 | 1.6 | 1.3 | 1.4 |
| | | | | **v2smgovsm** | **v2smgovsmcenprc** | **DRI** | **DRCI** |
| North Korea | EAP | CA | 0.1% | 4.0 | 4.9 | 3.3 | 2.6 |
| Turkmenistan | SCA | CA | 38% | 3.1 | 3.3. | 2.7 | 1.5 |
| Iran | MENA | CA | 84% | 2.8 | 1.9 | 2.1 | 1.2 |
| Sudan | AF | CA | 29% | 2.7 | 0.9 | 1.7 | 0.5 |
| Tajikistan | SCA | EA | 40% | 2.7 | 1.8 | 2.0 | 0.8 |
| Myanmar | EAP | CA | 46% | 2.6 | 3.0 | 2.0 | 0.8 |
| Ethiopia | AF | EA | 25% | 2.6 | 1.9 | 1.9 | 0.8 |
| Eritrea | AF | CA | 8% | 2.3 | 2.2 | 2.2 | -0.1 |
| Russia | EUR | EA | 89% | 2.1 | 1.5 | 1.8 | 1.9 |
| China | EAP | CA | 71% | 2.0 | 2.4 | 2.1 | 2.5 |
| | | | | **v2smgovfilprc** | **v2smgovfilcap** | **DRI** | **DRCI** |
| North Korea | EAP | CA | 0.1% | 3.9 | 2.6 | 3.3 | 2.6 |
| Saudi Arabia | MENA | CA | 97% | 3.4 | 2.4 | 1.8 | 1.8 |
| Cuba | WH | CA | 73% | 3.3 | 2.2 | 1.7 | 1.6 |
| Turkmenistan | SCA | CA | 38% | 3.2 | 1.9 | 2.7 | 1.5 |
| Nicaragua | WH | EA | 44% | 3.2 | 2.1 | 2.0 | 1.1 |
| China | EAP | CA | 71% | 2.9 | 2.5 | 2.1 | 2.5 |
| United Arab Emirates | MENA | CA | 99% | 2.8 | 2.3 | 1.7 | 1.8 |
| Iran | MENA | CA | 84% | 2.6 | 1.9 | 2.1 | 1.2 |
| Syria | MENA | CA | 49% | 2.6 | 1.0 | 2.0 | 1.2 |
| Ethiopia | AF | EA | 25% | 2.5 | 1.2 | 2.0 | 0.8 |
| | | | | **v2smgovdom** | **v2smpardom** | **DRI** | **DRCI** |
| Russia | EUR | EA | 89% | 3.6 | 2.8 | 1.8 | 1.9 |
| Turkmenistan | SCA | CA | 38% | 3.5 | 3.4 | 2.7 | 1.5 |
| Nicaragua | WH | EA | 44% | 3.3 | 1.0 | 2.0 | 1.1 |
| Syria | MENA | CA | 49% | 3.3 | 3.4 | 2.1 | 1.2 |
| Venezuela | WH | EA | 72% | 3.1 | 2.1 | 1.7 | 1.4 |
| Azerbaijan | EUR | EA | 88% | 3.1 | 0.9 | 1.4 | 1.5 |
| North Korea | EAP | CA | 0.1% | 2.9 | 2.1 | 3.3 | 2.6 |
| Myanmar | EAP | CA | 46% | 2.8 | -0.1 | 2.0 | 0.8 |
| Hong Kong | EAP | CA | 96% | 2.7 | 2.8 | 1.0 | 0.3 |
| Brazil | WH | ED | 80% | 2.7 | 1.7 | 0.2 | 0.1 |

**Table 5**
Internet Shutdown (*v2mgovshut*); Internet Shutdown capacity (*v2mgovshutcap*); Social media shutdown (*v2smgovsm*) and censorship (*v2smgovsmcenprc*); Internet filtering(*v2smgovfilprc*) and capacity (*v2smgovfilcap)*; Governmental (*v2mgovsmcenprc*) and Party dissemination of false information on social media (*v2govdom*) [45, 44].

of the digital authoritarian toolkit between 2003 and 2022, highlighting trends in state-led digital repression strategies. The data reveals a consistent increase in practices such as government social media monitoring, censorship, and the dissemination of false information, underscoring the growing reliance on digital tools to control information and suppress dissent. While practices like Internet filtering and arrests for political content remain stable and prominent, more intermittent but significant measures, such as social media and Internet shutdowns, reflect a selective use of extreme tactics. In 2022, higher or moderate levels of Internet access did not equate to unrestricted online freedom (Table 4), with governments (e.g., UAE, Syria and Qatar) imposing strict controls over social media (*v2smgovsmmon*) and online users (*v2smarrest*) resulting in their shallow usage for organizing offline protests (*v2smorgavact*) [48].

China's relatively high internet penetration coexists with substantial government monitoring of social media (*v2smgovsmmon*); additionally, while the DSP does not provide an analytic measurement of physical surveillance measures [49], commercial spyware inventories confirm that China, Iran,

Saudi Arabia, and North Korea are leaders in commercial malware for surveillance, explicitly targeting political opponents [14, 35]. Top censoring countries usually display lower Internet penetration levels, as preventing online access is more efficient than controlling its content (Table 5).

North Korea's digital environment remains highly isolated, with its low Internet penetration levels (Table 5) and its near-constant Internet shutdowns (*v2smgovshut*) and very limited access to global online spaces. Despite its near-zero internet penetration, the regime effectively curates the content that is accessible, relying on filtering practices (*v2smgovfilprc*; *v2smgovfilcap*) to limit dissent. This form of control is somewhat simpler to enforce due to the lack of external internet infrastructure, which places fewer demands on the government's capacity to enforce comprehensive censorship. In contrast, China and Russia, with relatively high internet penetration, showcase more sophisticated forms of repression. China displays strong reliance on internet filtering (*v2smgovfilprc*) while Russia has strengthened its reliance on social media shutdowns and censorship (*v2smgovsm* and *v2smgovsmcenprc*). Russia has also demonstrated a high capacity for manipulating public discourse through social media shutdowns and reliance on state-driven misinformation campaigns aimed at domestic and international audiences(*v2smgovdom* and*v2smpardom*). Internet shutdowns are often observed in countries with lower DRI (e.g., India [50]) or with lower capacities for sophisticated censoring practices (e.g., Sudan, Ethiopia, Eritrea). Previous studies have assessed how the COVID-19 pandemic exacerbated social manipulation (i.e., disinformation) in China, Iran, Russia, and Turkey [51]. In 2022, Russia, exhibits significant values in both social media censorship (*v2smgovsm*) and governmental dissemination of false information (*v2govdom*), highlighting that despite higher internet penetration levels, the government manipulates online narratives (Table 5). Finally, Brazil, while not traditionally seen as a digital authoritarian state, reflects growing concerns over governmental and party-driven misinformation. With a lower level of DRI compared to the aforementioned countries, Brazil's government still engages in the dissemination of false information on social media (*v2govdom*). Turkmenistan, instead, demonstrates extensive control over information flow (*v2smgovsm*; *v2govdom*), using the Internet for propaganda despite a small online population.

## 5. Conclusions

This paper conceptualized digital authoritarianism and analyzed how its toolkit reinforces the conventional pillars of authoritarian stability of repression, cooptation, and liberalization. The theoretical part of the paper argued that while digital authoritarian practices have become core characteristics in modern autocracies, they are also applied by democratic governments to some extent. The empirical part of the paper is a systematic descriptive analysis of digital authoritarianism's diffusion across regime types and provides evidence of the increasing threats posed by digital authoritarianism globally.

Autocracies tend to digitally repress beyond their inherent capabilities, resorting to lower-capacity strategies (e.g., Internet shutdowns) or relying on external service providers. Democracies ruled by illiberal leaders exhibit patterns more akin to their autocratic counterparts. The research reveals significant variance among autocracies in selecting their digital authoritarian toolkit, with a bias towards surveillance and social manipulation. Transnational challenges and targeted digital threats against regime critics are rising, parallel to the use of social media to organize offline action. Addressing the global challenges posed by digital authoritarianism requires a nuanced, interdisciplinary approach bridging political science and cybersecurity.

# 6. Appendices

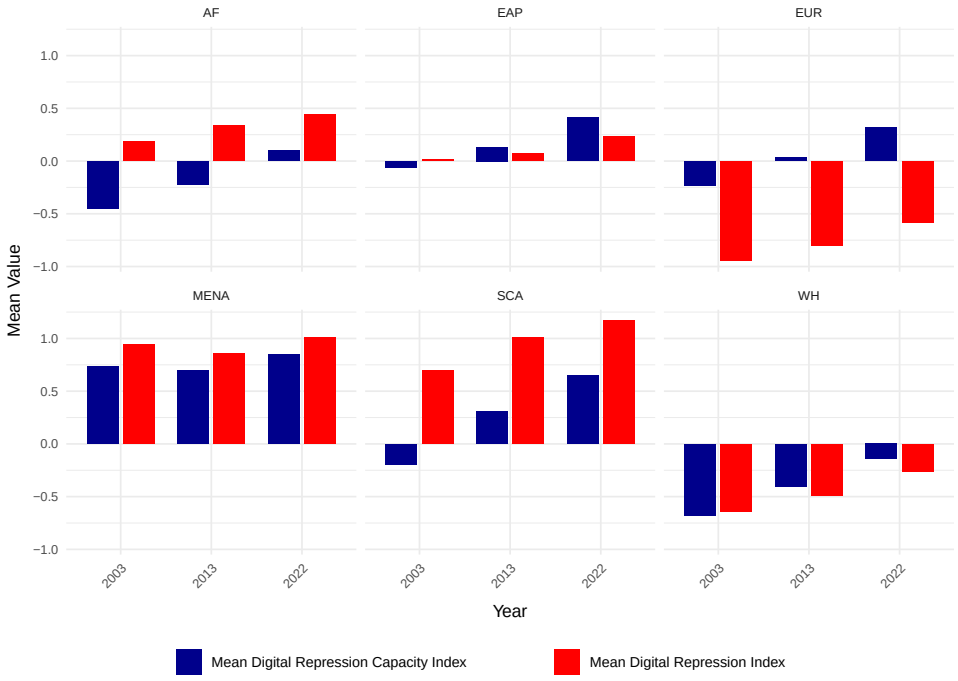


**Figure 6:** Regional Distribution of DRI and DRCI (2003, 2013, 2022) [14].

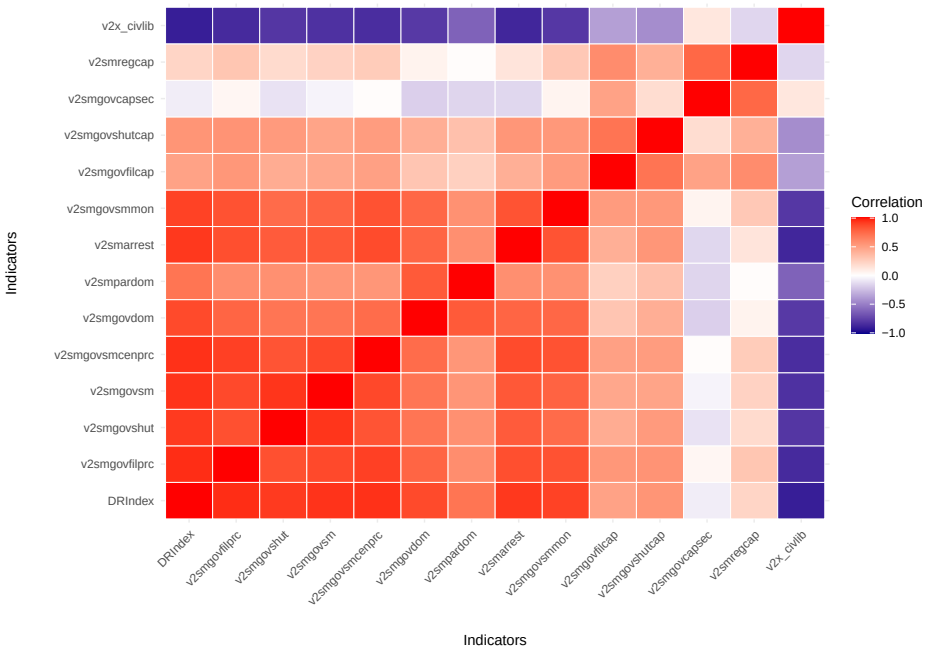


**Figure 7:** Pearson Correlation Heatmap of Selected Indicators of DRI [36] and V-dem Democracy Indexes [45].

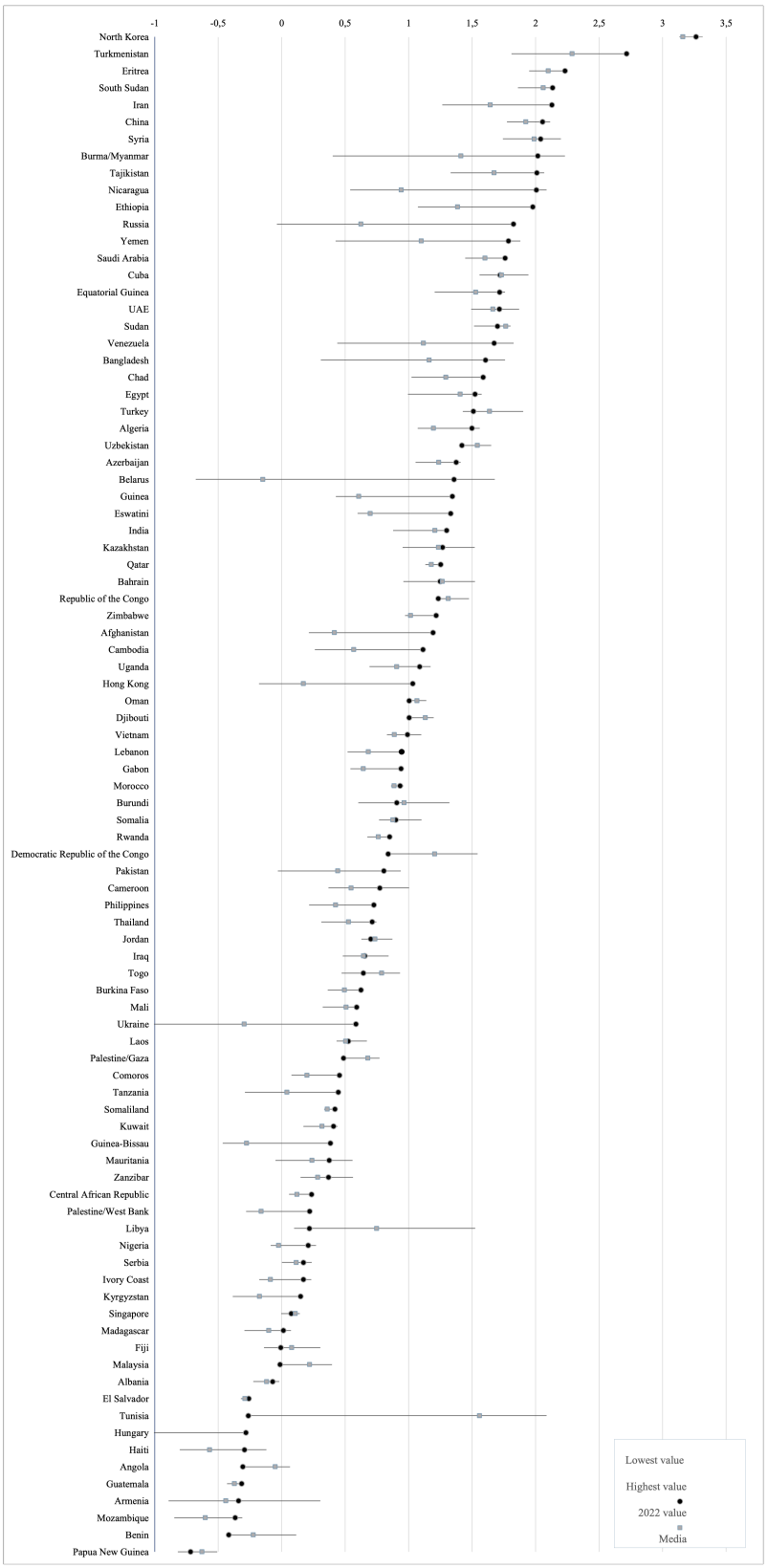


**Figure 8:** Ranking of Digital Repression Index by authoritarian regimes (range, media and most recent value (2022). Data elaborated from [36].

## Declaration on Generative AI

*(by using the activity taxonomy in ceur-ws.org/genai-tax.html):*
During the preparation of this work, the author used Grammarly in order to: Grammar and spelling check. After using this tool, the author reviewed and edited the content as needed and takes full responsibility for the publication's content.

## References


[1] E. Frantz, A. Kendall-Taylor, J. Wright, Digital repression in autocracies, Varieties of Democracy Institute Users Working Paper (27) (2020) 1–22.
[2] M. Castells, The Internet galaxy: Reflections on the Internet, business, and society, Oxford University Press, 2002.
[3] M. Lynch, Digital activism and authoritarian adaptation in the middle east, Digital Activism and Authoritarian Adaptation in the Middle East 43 (2021).
[4] S. Gunitsky, Corrupting the cyber-commons: Social media as a tool of autocratic stability, Perspectives on politics 13 (2015) 42–54.
[5] R. Deibert, R. Rohozinski, Liberation vs. control: The future of cyberspace, Journal of democracy 21 (2010) 43–57.
[6] A. Kendall-Taylor, E. Frantz, J. Wright, The digital dictators: How technology strengthens autocracy, Foreign Aff. 99 (2020) 103.
[7] E. G. Rød, N. B. Weidmann, Empowering activists or autocrats? the internet in authoritarian regimes, Journal of Peace Research 52 (2015) 338–351.
[8] O. Schlumberger, M. Edel, A. Maati, K. Saglam, How authoritarianism transforms: A framework for the study of digital dictatorship, Government and Opposition 59 (2024) 761–783.
[9] E. Keremoğlu, N. B. Weidmann, How dictators control the internet: a review essay, Comparative Political Studies 53 (2020) 1690–1703.
[10] M. Michaelsen, M. Glasius, Authoritarian practices in the digital age—introduction, International Journal of Communication 12 (2018) 7.
[11] S. F. Maerz, F. Schulte, C. Trinn, Autocratization and political conflict, in: The Routledge Handbook of Autocratization, Routledge, 2024, pp. 441–454.
[12] M. Glasius, What authoritarianism is… and is not: a practice perspective, International affairs 94 (2018) 515–533.
[13] V. Mechkova, D. Pemstein, B. Seim, S. Wilson, Measuring Internet Politics: Digital Society Project (DSP) Annual Report v4, Technical Report, V-dem Democracy, 2022.
[14] S. Feldstein, Commercial spyware global inventory, Mendeley Data 1 (2020).
[15] J. J. Linz, Totalitarian and authoritarian regimes, Lynne Rienner Publishers, 2000.
[16] L. Martino, La quinta dimensione della conflittualità. l'ascesa del cyberspazio ei suoi effetti sulla politica internazionale, Politica & società 7 (2018) 61–76.
[17] G. Giacomello, National governments and control of the Internet: a digital challenge, Routledge, 2004.
[18] A. Shahbaz, The rise of digital authoritarianism, 2018. URL: https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism, accessed: 2024-11-27.
[19] R. Deibert, R. Rohozinski, Liberation vs. control: The future of cyberspace, Journal of democracy 21 (2010) 43–57.
[20] J. Earl, T. V. Maher, J. Pan, The digital repression of social movements, protest, and activism: A synthetic review, Science Advances 8 (2022) eabl8198.
[21] A. R. Gohdes, Repression technology: Internet accessibility and state violence, American Journal of Political Science 64 (2020) 488–503.
[22] D. Conduit, Digital authoritarianism and the devolution of authoritarian rule: examining syria's patriotic hackers, Democratization 31 (2024) 979–997.

[23] J. Gerschewski, The three pillars of stability: Legitimation, repression, and co-optation in autocratic regimes, in: Comparing autocracies in the early Twenty-first Century, Routledge, 2015, pp. 58–83.
[24] S. Feldstein, The global expansion of ai surveillance, Carnegie Endowment for International Peace Washington, DC 17 (2019).
[25] M. E. Roberts, Resilience to Online Censorship, Annual Review of Political Science 23 (2020) 401–419.
[26] S. Feldstein, The road to digital unfreedom: How artificial intelligence is reshaping repression, Journal of Democracy 30 (2019) 40–52.
[27] Y. Kabanov, M. Karyagin, Data-driven authoritarianism: Non-democracies and big data, in: Digital Transformation and Global Society: Third International Conference, DTGS 2018, St. Petersburg, Russia, May 30–June 2, 2018, Revised Selected Papers, Part I 3, Springer, 2018, pp. 144–155.
[28] S. Guriev, D. Treisman, Informational autocrats, Journal of economic perspectives 33 (2019) 100–127.
[29] B. Spens, The spyware industrial complex, Tech4Humanity Lab (2024).
[30] M. Glasius, Authoritarian practices in a global age, Oxford University Press, 2023.
[31] E. Yayboke, Promote and build: A strategic approach to digital authoritarianism, Center for Strategic and International Studies (CSIS) (2020).
[32] K. Ruijgrok, The authoritarian practice of issuing internet shutdowns in india: The bharatiya janata party's direct and indirect responsibility, Democratization 29 (2022) 611–633.
[33] R. U. Mendoza, R. J. G. Ong, D. L. L. Romano, B. C. P. Torno, Counterterrorism in the philippines, Perspectives on Terrorism 15 (2021) 49–64.
[34] E. Adler, V. Pouliot, International practices, International theory 3 (2011) 1–36.
[35] M. Michaelsen, J. Thumfart, Drawing a line: Digital transnational repression against political exiles and host state sovereignty, European Journal of International Security 8 (2023) 151–171.
[36] S. Feldstein, The rise of digital repression: How technology is reshaping power, politics, and resistance, Oxford University Press, 2021.
[37] V. Mechkova, D. Pemstein, B. Seim, S. Wilson, Digital society project dataset v6, 2024. URL: https://digitalsocietyproject.org/data/, accessed: 2024-12-12.
[38] D. Pemstein, K. L. Marquardt, E. Tzelgov, Y.-t. Wang, J. Medzihorsky, J. Krusell, F. Miri, J. von Römer, The V-Dem Measurement Model: Latent Variable Analysis for Cross-National and Cross-Temporal Expert-Coded Data, Technical Report V-Dem Working Paper No. 21, 8th edition, University of Gothenburg: Varieties of Democracy Institute, 2023.
[39] M. Coppedge, J. Gerring, C. H. Knutsen, J. Krusell, J. Medzihorsky, J. Pernes, S.-E. Skaaning, N. Stepanova, J. Teorell, E. Tzelgov, et al., The methodology of "varieties of democracy"(v-dem), Bulletin of Sociological Methodology/Bulletin de Méthodologie Sociologique 143 (2019) 107–133.
[40] A. Lührmann, M. Tannenberg, S. I. Lindberg, Regimes of the world (row): Opening new avenues for the comparative study of political regimes, Politics and governance 6 (2018) 60–77.
[41] M. Coppedge, J. Gerring, C. H. Knutsen, S. I. Lindberg, J. Teorell, L. Gastaldi, A. Good God, S. Grahn, V-dem country coding units v14, 2024. Varieties of Democracy (V-Dem) Project.
[42] M. Coppedge, J. Gerring, C. H. Knutsen, S. I. Lindberg, J. Teorell, K. L. Marquardt, J. Medzihorsky, N. Natsika, D. Pemstein, L. Fox, L. Gastaldi, A. Good God, S. Grahn, J. Pernes, O. Rydén, J. von Römer, E. Tzelgov, Y.-t. Wang, S. Wilson, V-dem methodology v14, 2024. Varieties of Democracy (V-Dem) Project.
[43] V. Mechkova, D. Pemstein, B. Seim, S. Wilson, Measuring internet politics: Introducing the digital society project, 2019. Digital Society Project (DSP).
[44] M. Coppedge, J. Gerring, C. H. Knutsen, S. I. Lindberg, J. Teorell, D. Altman, F. Angiolillo, M. Bernhard, C. Borella, A. Cornell, M. S. Fish, L. Fox, L. Gastaldi, H. Gjerløw, A. Glynn, A. Good God, S. Grahn, A. Hicken, K. Kinzelbach, J. Krusell, K. L. Marquardt, K. McMann, V. Mechkova, J. Medzihorsky, N. Natsika, A. Neundorf, P. Paxton, D. Pemstein, J. Pernes, O. Rydén, J. von Römer, B. Seim, R. Sigman, S.-E. Skaaning, J. Staton, A. Sundström, E. Tzelgov, Y.-t. Wang, T. Wig, D. Ziblatt, V-dem codebook v14, 2024. Varieties of Democracy (V-Dem) Project.
[45] M. Coppedge, J. Gerring, C. H. Knutsen, S. I. Lindberg, J. Teorell, D. Altman, F. Angiolillo,

M. Bernhard, C. Borella, A. Cornell, M. S. Fish, L. Fox, L. Gastaldi, H. Gjerløw, A. Glynn, A. Good God, S. Grahn, A. Hicken, K. Kinzelbach, J. Krusell, K. L. Marquardt, K. McMann, V. Mechkova, J. Medzihorsky, N. Natsika, A. Neundorf, P. Paxton, D. Pemstein, J. Pernes, O. Rydén, J. von Römer, B. Seim, R. Sigman, S.-E. Skaaning, J. Staton, A. Sundström, E. Tzelgov, Y.-t. Wang, T. Wig, S. Wilson, D. Ziblatt, V-dem [country-year/country-date] dataset v14, 2024. URL: https://doi.org/10.23696/mcwt-fr58, varieties of Democracy (V-Dem) Project.

[46] F. House, Freedom on the net 2022 (2022).

[47] S. C. Greitens, Surveillance, security, and liberal democracy in the post-covid world, International Organization 74 (2020) E169–E190.

[48] E. Frantz, A. Kendall-Taylor, J. Wright, Digital repression in autocracies, Varieties of Democracy Institute Users Working Paper (27) (2020) 1–22.

[49] R. Deibert, Communities@ risk: Targeted digital threats against civil society, Citizens Lab Report (2014).

[50] T. Dragu, Y. Lupu, Digital authoritarianism and the future of human rights, International Organization 75 (2021) 991–1017.

[51] A. Polyakova, C. Meserole, Exporting digital authoritarianism: The russian and chinese models, Policy brief, democracy and disorder series (2019) 1–22.