

Geopolitical Dynamics of Digital Authoritarianism: Emerging Global Challenges

Digital Geopolitics: Explaining power shifts in the digital sector, an analysis of different battlegrounds

Working Paper Series
SOG-WP6/2024

Author: Martina Lucaccini
May 2024

Table of Contents

Abstract	3
1. Introduction.....	Error! Bookmark not defined.
2. Cyber Optimism and Cyber Pessimism	5
3. Defining Digital Authoritarianism.....	6
3.1. The dictator’s perpetual agenda: from analogic to digital	7
3.2. The Digital Authoritarian Toolkit	9
3.3. Emerging Global Challenges.....	11
4. Global patterns of digital authoritarianism	13
4.1. Digital repression and regime types.....	15
4.2. Comparing Digital Repression Capacity and Practice	19
5. Conclusion: Responding to Digital Authoritarianism	21

Abstract

This paper examines digital authoritarianism and the leverage of Information and Communication Technologies (ICTs) to maintain political control. The paper offers a theoretical framework of the digital authoritarian toolkit and argues that ICTs reinforce autocracies' tenets of stability – repression, cooptation, and legitimation. In line with cyberspace's borderless nature, the toolkit manifests through a set of practices and capabilities across regime types. Using cross-national, time-series data drawn from the Digital Society Project (DSP), I provide insights into the global patterns of digital authoritarianism. The research reveals variance among autocracies in selecting their digital authoritarian toolkit, with a bias towards surveillance and social manipulation. Autocracies tend to digitally repress beyond their inherent capabilities, resorting to lower-capacity strategies (e.g., Internet shutdowns) or relying on external service providers. Notably, democracies possess higher digital repression capabilities but refrain from using them; still, when ruled by illiberal leaders, they exhibit patterns akin to their autocratic counterparts.

Keywords: Cyber politics – Authoritarianism – Technologies – Political Regimes – State Power

1. Introduction

The digital age changed the context in which regimes operate. Information and Communication Technologies (ICTs) reduced barriers to coordination, making it easier for ordinary citizens to challenge repressive governments. Authoritarian regimes, however, have adapted to these challenges and learned to co-opt digital tools to shape political dynamics inside and beyond their borders. Digital authoritarianism is the misuse of the Internet and digital technologies by leaders with authoritarian tendencies to reduce trust in public institutions, increase social and political control, violate civil liberties, and distort the fundamental values of democratic and open societies: its aim is not to dismantle them but to reshape them into their authoritarian image. Digital authoritarianism extends the analogic pillars of authoritarian stability – repression, co-option, and legitimation. Precisely, in some cases, digital tools supercharge long-standing authoritarian strategies; in other cases, these tools can have a transformative effect on a regime’s repressive capacity (e.g., monitor citizens and identify dissidents and monitor the performance of regime elite, enhance the ability to co-opt support; censoring and shutting down the Internet; engaging in social manipulation and disinformation; mimic elements of democracy and increase the legibility of society reducing the so-called “dictator’s dilemma”). The digital authoritarian toolkit encompasses censorship, surveillance, cyberattacks, social manipulation and tools of great power (i.e. digital infrastructures and authoritarian visions of the Internet) and is deployed differently depending on which challenges it generates: **(1)** within autocracies, **(2)** towards the regime’s adversaries, **(3)** via export to like-minded regimes, and **(4)** within democracies. Although digital repression is more prevalent in authoritarian regimes than democracies, its use has grown significantly in both settings. As of 2022, the political system type is one of the most significant predictors of digital repression; autocracies perform worse in digital repression measurements than democracies and engage in digital repression beyond their capabilities. Indeed, authoritarian regimes frequently employ lower-capacity strategies for digital repression (i.e. Internet shutdowns) and rely on external service providers. In contrast, democracies possess a higher digital repression capacity than they deploy, showcasing a conscious choice to refrain from utilising capabilities; still, democracies ruled by illiberal leaders display tendencies closer to their autocratic counterparts. The spread of digital authoritarianism can challenge the principles of an open and free Internet; this has implications for the internal dynamics of authoritarian countries and the broader global order. Thus, understanding the interplay between digital authoritarianism and digital geopolitics is crucial for analysing the impact of technology on political systems.

2. Cyber Optimism and Cyber Pessimism

In the 1990s and early 2000s, at the dawn of the Internet age, a sense of optimism was diffused among scholars, who saw the World Wide Web as a virtual Habermasian public sphere fostering democratisation¹. Firstly, the Internet's infrastructure operates beyond conventional national borders, facilitating the swift conveyance of online information worldwide. Secondly, the Internet has a latent framework, allowing users to exchange messages concurrently as receivers and broadcasters (i.e. many-to-many communication)². **Cyber-optimism** peaked during the events of the Arab Spring, the mass protests facilitated by Information and Communication Technologies (ICTs), which were depicted as liberation technologies for social movements worldwide³. **Cyber-pessimists**, by contrast, deemed the optimistic view as a "Net Delusion" and argued that authoritarian regimes would soon promote the creation of an Internet that served state-defined interests⁴. While by design, the Internet was intended to be an "open common" (i.e. a separate, alternative sphere that exists outside the influence of the state or corporate power), today, it is embedded in contested cyberspace⁵, where various actors fight for influence. In this context, the increasing networking between individuals did not emerge without negative consequences⁶. Indeed, cyberspace has facilitated the activities of authoritarians in much the same way as it has for more benign civil society networks. In this sense, the aftermath of the Arab Spring looks more like a "cold winter" – a potent example of resurgent authoritarianism in cyberspace⁷.

¹ E. Frantz, A. Kendall-Taylor, J. Wright, Digital Repression in Autocracies, V-Dem Institute at the University of Gothenburg, 1-54, 2020.

² M. Castells, The Internet Galaxy: Reflections on the Internet, Business, and Society. Oxford: Oxford University Press, 2001.

³ L. Diamond, E. Donahoe, Digital Activism and Authoritarian Adaptation in the Middle East, Middle East Political Science. Stanford University, 2010.

⁴ S. Gunitsky, Corrupting the Cyber-Commons: social media as a Tool of Autocratic Stability. Perspectives on Politics, 13(1), 42-54, 2015; E. Morozov, The net delusion: the dark side of internet freedom, New York, NY: Public Affairs, 2011

⁵ Cyberspace can be defined as a human-made domain in constant evolution, comprising both a material and a virtual realm. Its first definition was coined by William Gibson in 1984: "A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts. A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding". See W. Gibson, Neuromancer, 1984.

⁶ R. Deibert, R. Rohozinski, Liberation vs. Control: The Future of Cyberspace, Journal of Democracy, 21(4), 43-57, 2010.

⁷ R. Deibert, Cyberspace Under Siege, Journal of Democracy, 26(3), 64-78, 2015.

3. Defining Digital Authoritarianism

An authoritarian regime is a «political system with limited, not responsible, political pluralism, without elaborate and guiding ideology, but with distinctive mentalities, without extensive nor intensive political mobilisation [...] and in which a leader or occasionally a small group exercises power within formally ill-defined limits but quite predictable ones»⁸. Despite the assumption that authoritarian rule systems were incompatible with the emerging fast-paced media environment, authoritarian regimes began shaping cyberspace to their strategic advantage, merging technological breakthroughs within their authoritarian toolbox.⁹ This process can be defined as **networking authoritarianism** (i.e. regimes adjusting to the inevitable changes brought by digital communications), **data-driven authoritarianism** (i.e. regimes transforming their social governance using big data, datafication and dataveillance) or **digital authoritarianism**. Digital authoritarianism is the use of digital information technology¹⁰ by authoritarian regimes to surveil, repress and manipulate domestic and foreign populations while retaining political control. Digital authoritarians often adopt the principle of cyber sovereignty, thus exerting control over the Internet within their borders. Additionally, authoritarians select from an arsenal of strategies that can act as replacements, additions, or complements to conventional pillars of authoritarian stabilisation and ensure their hold on power¹¹.

To fully understand authoritarian cyberspace, I group the control strategies deployed by digital authoritarians into three different generations¹². **First-generation controls** are defensive, involving the creation of national cyber borders to restrict access to external information. The most well-known example of this is the Great Firewall of China, while Iran, Pakistan, Saudi Arabia, Bahrain, Yemen, and Vietnam come close to China's level of sophistication. Parallely to establishing Internet sovereignty, regimes use filtering (e.g., applying to keywords, servers, domains and IP addresses) that censor political and security-related content or display “network errors” to Internet users¹³. **Second-generation controls** (e.g., backdoor functionalities in products and deep packet inspections; banning anonymising tools and virtual private networks) extend information monitoring through laws, regulations, and requirements imposed on privately owned networks. These controls also include finer-grained registration and identification requirements that tie people to specific accounts or devices or require citizens to obtain government permission before using the Internet. Often referred to as “just-in-time”, they grant dynamic Internet access management and plausible deniability, as second-generation controls are usually represented as

⁸ J. Linz, *Totalitarian and authoritarian regimes*. Lynne Rienner Publishers, 1975.

⁹ Freedom House, *Freedom on the Net 2018: The Rise of Digital Authoritarianism*, 2018.

¹⁰ I use digital information technology (DIT) as an umbrella term encompassing digital systems that store, retrieve and send information. DIT is commonly associated with computers and computer networks, but using this term allows us to encompass a much more comprehensive range of technologies, including servers and smartphones.

¹¹ E. Yayboke, Promote and Build a Strategic Approach to Digital Authoritarianism, *Centre for Strategic & International Studies*, 1-11, 2020.

¹² Please note that the “generations” of controls are not assumed to be strictly chronological: governments can skip generations, and several generations can exist together. Instead, they are a useful heuristic device for understanding the evolution of information control and channelling. See also R. Deibert (2015), *op. cit.* 64-78.

¹³ J. Earl, The digital repression of social movements, protest, and activism: A synthetic review, *Science Advances*, 8(10), 2022.

technical errors, making it easier for governments to deny involvement¹⁴. **Third-generation controls** are offensive and undermine civil society's participation by censoring content and actively framing and manipulating information (e.g., disinformation and misinformation, online harassment to discredit and intimidate critics). These information control and channelling practices generate chilling effects on society¹⁵ (i.e. self-censorship), undermining the networking advantages that civil society might otherwise gain from digital media. Third-generation controls also crowdsourcing techniques to intimidate regime critics, such as patriotic hackers (e.g., China's fifty-centres; Venezuela's Chavista communicational guerrillas, the Egyptian Cyber Army, the pro-Assad Syrian Electronic Army; the pro-Putin bloggers of Russia; Kenya's "director of digital media", Saudi Arabia's "ethical hackers")¹⁶. A potential **fourth generation of control** introduces an assertive international dimension of digital authoritarianism. In this context, the digital authoritarian toolkit is used for strategic competition among great powers (i.e. advancing authoritarian visions of the Internet).

3.1. The dictator's perpetual agenda: from analogic to digital

The stabilisation strategies of authoritarian regimes have been convincingly theorised based on legitimacy, repression and co-optation¹⁷. **Co-optation** is the ability to bind relevant elites or groups of elites to the regime, often through material inducements, rewards and policy concessions. In its analogic form, cooptation allows intra-regime cohesion and prevents defections through the institutional mechanisms of legislatures, parties, elections and other apparent democratic devices. In its digital form, cooptation is achieved by gatekeeping the Internet infrastructure and its platforms as a critical source of information collection and distribution for regime cohesion. A digital authoritarian regime will have a higher capacity for digital cooptation when ICTs are a scarce resource; additionally, ICTs can also supplement functions associated with deliberative institutions (e.g., gathering information about the performance of the regime's agents to identify and coordinate the supporters or defectors of the government)¹⁸. **Legitimation** refers to the attempts to guarantee active consent, compliance with rules, passive obedience and more tolerance within the population. In its analogic form, authoritarians use legitimacy claims on entitlement to rule through propaganda. In its digital form, ICTs are the vehicle for disseminating messages that legitimise the regime itself, and the internet is the venue for regime-dominated deliberation and consultation forums. A digital authoritarian regime will not limit itself to blocking access to content it finds threatening; it will actively shape its citizens' information environment and behaviours. **Repression** is one of the strategies of political control directed at the punishment or deterrence of opponents' activities that the state finds threatening. Whether repression is high-intensity (i.e. killings, torture, disappearances) or low-intensity (i.e. surveillance, censorship, harassment, administrative procedures to prevent gatherings), it imposes a cost on the target to deter its activities¹⁹. Digital repression comprises **(i)** the use of traditional repressive techniques against digital protesters (e.g., the arrest of political bloggers or private harassment and/or

¹⁴ A. R. Gohdes, Repression Technology: Internet Accessibility and State Violence, *American Journal of Political Science*, 64(3), 488–503, 2020.

¹⁵ D. Moss, the ties that bind: Internet communication technologies, networked authoritarianism, and 'voice' in the Syrian diaspora, *Globalizations*, 15(2), 265–82, 2018.

¹⁶ D. Conduit, Digital authoritarianism and the evolution of authoritarian rule: examining Syria's patriotic hackers, *Democratization*, 1–19, 2023.

¹⁷ C. Davenport, M. Eads, Cued to Coerce or Coercing Cues? An Exploration of Dissident Rhetoric and its Relationship to Political Repression. *Mobilisation: An International Quarterly*, 6(2), 151–171, 2006.

¹⁸ J. Gerschewski, A. Dukalskis, How the Internet Can Reinforce Authoritarian Regimes: The Case of North Korea, *Georgetown Journal of International Affairs*, 19(1), 12–19, 2018.

¹⁹ Davenport, C. State Repression and Political Order. *Annual Review of Political Science*, 10(1), 1–23, 2007.

violence against online activists); **(ii)** the use of digital tools to perform traditional repressive actions (e.g., using digital surveillance for political control); **(iii)** the development of information strategies designed to diminish protest (i.e. Internet shutdowns and disinformation)²⁰.

We are witnessing a technologically induced transformation of political rule. Adapting their perpetual analogic agenda to the dynamics of cyberspace, authoritarian regimes aim at **a)** obtaining perfect information about their subjects and **b)** influencing behaviour and beliefs so that their rule appears legitimate. **Firstly**, the shift from analogic to digital authoritarianism allowed dictators to engage in swifter information gathering. Dictators can obtain data from **(i)** local internet service providers (ISP); **(ii)** hardware (e.g., data probes, surveillance cameras); **(iii)** users interacting with digital applications (e.g., phishing campaigns; cookie settings or browser certificates); and **(iv)** intrusive techniques (e.g., malware and spyware). Dictators can then automate the data analysis process with algorithms that can access, sort, and analyse big data. **Secondly**, in pursuing their perpetual agenda, digital authoritarian regimes can preempt threats by directly influencing the behaviours of their subjects. **Digital cooptation** provides positive incentives (e.g., social credit scores granting or withholding privileges) and sanctions (i.e. shadowban or de-platforming users) for citizens’ compliant participation in society.²¹ **Digital repression** can be advanced using overt information control (i.e. shutting down the internet, limiting connectivity or performing Internet Filtering not only stifles the spread of anti-government information but also prevents individuals from collectively organising themselves), less detectable tactics (i.e. Denial of Service attacks, Distributed denial-of-service attacks, and slowing access to information) or targeted attacks towards specific individuals and organisations (e.g., malware, shadowbanning, hacking and spyware)²². Digital dictators also control narratives: in this context, their goal is information channelling (i.e. redirecting or influencing attention)²³. **Digital legitimization** creates a façade of participation and responsiveness to the dictators’ rule (e.g., utilising social media bots and trolls to spread pro-regime narratives)²⁴.

In **Table 1**, I systematically represented how the three pillars of authoritarian stability – cooptation, repression and legitimization – are adapted in the digital age. **Digital cooptation** involves strategically integrating digital tools to manipulate information and co-opt potential sources of opposition, **influencing their behaviours**; cooptation may be advanced with positive or negative incentives. **Digital legitimization** refers to how authoritarian regimes exploit digital platforms to **influence beliefs** and fortify their perceived

Cooptation		Repression		Legitimation
		Influencing Behaviours		Influencing beliefs
Positive Incentives	Negative incentives	Sanctions	Information Control	Information Channelling
Social Credit Scores	Deplatforming activists or organisations and/or moderating them; Down-ranking, search filtering, shadow banning, throttling the spread of, or otherwise making protest-related material more obscure.	Denial of Service (DoS) and Distributed Denial of Service (DDoS); Targeted Digital Threats (i.e. hacking, malware, spyware)	Limited national Internet connectivity, temporary Internet Shutdown, Content filtering not clear to users (e.g., returning 404 errors for filtered material), Internet Censorship	Government accounts posting distracting information (i.e. misinformation and disinformation) and/or flooding online spaces or hashtags with irrelevant material (i.e. patriotic hackers, trolls); Government misrepresentations that influence contention (i.e. bots)

Table. 1 – The three pillars of authoritarian stability – adapting to the digital age

²⁰ J. Earl (2022), *op. cit.*

²¹ J. Earl, Layers of Political Repression: Integrating Research on Social Movement Repression, *Annual Review of Law and Social Science*, 18(1), 227–248, 2022.

²² These tactics can be called “targeted digital threats” (i.e. attacks on specific targets, persisting over time and motivated by political objectives to compromise and infiltrate the network devices and infrastructure of individuals, groups, organisations, and communities). They lead to the silencing of the regime’s opponents and their compliance with authoritarian rule. See R. Deibert, *Communities @ Risk: Targeted Digital Threats Against Civil Society*, University of Toronto, 2014.

²³ J. Earl (2022), *op. cit.*

²⁴ *Ibidem.*

legitimacy. The process of **information channelling** results in distributing distracting information and/or flooding online spaces with irrelevant material. **Digital repression** encompasses **behaviour and beliefs influencing strategies** for controlling the information environment.

3.2. The Digital Authoritarian Toolkit

The theoretical framework defined in the previous paragraph deciphers the multifaceted dimensions in the arsenal of digital authoritarians.

First, **surveillance**, which has been a tool of repression, co-option, and legitimation for a long time, has become swifter to implement. Surveillance entails gathering information through identifying, tracking, monitoring, and analysing individuals, data, organisations, or systems.²⁵ Advances in metadata availability from public and private sources, algorithmic sophistication, and artificial intelligence (AI) have accelerated data gathering, allowing real-time tracking of perceived opponents²⁶. The collection of metadata enables states to monitor individuals' online activities, as well as information that describes their lives (e.g., location, number of devices and device usage, application statistics, browsing histories, contact lists, the volume, timing, and frequency of interactions between different users)²⁷. Surveillance can also be used to anticipate the population's political preferences, strengthening the regime's **legitimation**; additionally, tech-enabled incentive and punishment systems, fostering data transfer between private technology companies and government agencies, contribute to the shaping of societal participation, as only compliant citizens can participate fully in society²⁸. Techniques used to advance digital surveillance include **social media monitoring** (i.e. machine-driven programs monitoring millions of communications for specific keywords automatically) and **surveillance capitalism** (i.e. transactional data referring to visited websites, sent emails and chat messages, location-tracking and web-tracking information from accessed apps or browsers).

Second, **cyberattacks** (i.e. DDoS attacks, malicious software and network intrusions) allow for covert data collection and repress the voices of regimes' critics²⁹. Targeted methods rely on intrusive technology that manipulates software, data, computer systems, or networks to gain unauthorised access to user information and devices³⁰. Some of these cyber capabilities are commercially available (e.g., spyware sold by NSO Group, FinFisher, and Hacking Team). Less-detectable tactics include Denial-of-Service Attacks (i.e. intentionally rendering computer networks or websites inoperative by flooding them with data) and slowing access to information from specific sources. Unlike national or regional Internet Shutdowns, DDoS attacks deny access to all potential users globally; attacks may be implemented by groups loyal to the government but not directly under their command (e.g., pro-government hackers)³¹.

Thirdly, a longstanding authoritarian practice, **ensorship**, remains central in the digital authoritarian toolkit. While cyber-optimists argued that the rise of the Internet would have made it increasingly difficult

²⁵ G. T. Marx, What's New About the "New Surveillance"? Classifying for Change and Continuity, *Surveillance & Society*, 1(1), 2002, 9–29.

²⁶ S. Feldstein, The road to digital unfreedom: How artificial intelligence is reshaping repression. *KANT Social Sciences & Humanities*, 5, 2021, 39–51

²⁷ T. Gill, Metadata and the Web, Introduction to metadata, 3, 2008, 20–38.

²⁸ Y. Kabanov, Data-Driven Authoritarianism: Non-democracies and Big Data. In D. Alexandrov, A. Boukhanovsky, A. Chugunov, Y. Kabanov, & O. Koltsova, *Digital Transformation and Global Society* (858, 144–155). Springer International Publishing, 2018.

²⁹ S. Guriev, D. Treisman. Informational Autocrats. *Journal of Economic Perspectives*, 33(4), 2019, 100–127.

³⁰ R. Deibert, J. Palfrey, R. Rohozinski, e J. Zittrain, Access denied: The practice and policy of global internet filtering. The MIT Press, 2008.

³¹ W. Marczak, V. Paxson, Social Engineering Attacks on Government Opponents: Target Perspectives, Proceedings on Privacy Enhancing Technologies, 2, 2017, 172–185.

for dictators to control information, their efforts have been significantly centralised³². Online censorship can take many forms, and its impact can differ profoundly; in conceptualising it, I distinguish between **top-level censorship** targeting all forms of online communications and content (e.g., national or regional Internet Shutdowns, bandwidth throttling), **domain-level censorship** aiming at specific websites or services (e.g., blocking websites or apps; domain-level throttling), and **content-level censorship** directed at specific content published online³³. Put simply, authoritarian regimes can control citizens' access to undesirable content through partial or total filtering mechanisms, Internet Shutdowns and gatekeeping of the software and platforms their citizens can access³⁴. Private corporations may also independently restrict access to specific web pages and block the visibility of users' posts without their knowledge³⁵. If the core of authoritarianism remains the idea of governance in which those being governed are fundamentally denied a voice, then censorship allows for the sabotage of accountability³⁶.

Fourthly, misinformation and disinformation (i.e. spreading false information and engaging in the deliberate diffusion of false information) are tools for **social manipulation**. Online information can be censored by creating sufficient noise to drown out other content. Using bot armies and defamation instruments enables autocrats to manipulate election processes, predict voting behaviour, create a highly fragmented information landscape and strengthen their legitimisation³⁷. This category comprehends disinformation, flooding, automated methods, and vandalism, all intended to shape behaviours. **Disinformation** is the intentional dissemination of false, inaccurate, or misleading information to cause demonstrable and significant harm to the public; **flooding** involves promoting competing or distracting information that overwhelms legitimate information sources; **automated methods** are advanced by patriotic hackers (i.e. pro-regime agents amplifying propaganda and disseminating false information) or can be automated through **bots** and **algorithms** (i.e. social media accounts operated by computer programs and designed to create engagement spikes, promote pro-regime narratives or spread falsehoods about opposition figures). **Vandalism** involves unauthorised acts such as modifying a website or social media account; state agents use a technique to obscure legitimate information on a targeted website or account and may do so as a form of harassment or intimidation.

Finally, the digital authoritarian toolkit comprehends the so-called **tools of great power**. **Digital infrastructure** gatekeeping permits covert backdoor access to the data transmitted through communication channels. Additionally, while regimes generally portray themselves solely as service providers, supplying infrastructures always carries embedded norms and values, amplifying the capacity of authoritarian providers to influence international technology standards. Another element to consider is that while global connectivity has generally facilitated the emergence of an open, interoperable and reliable Internet, this connectivity confronts existential threats as digital authoritarians advocate for the Balkanization of the Internet (i.e. **digital sovereignty**). This approach emphasises data localisation

³² A. Gohdes, Repression Technology: Internet Accessibility and State Violence. *American Journal of Political Science*, 64(3), 2020, 488–503.

³³ A. R. Gohdes, Repression in the digital age: surveillance, censorship, and the dynamics of state violence. in *Disruptive technology and international security*. New York, NY: Oxford University Press, 2024.

³⁴ M. E. Roberts, Resilience to Online Censorship, *Annual Review of Political Science*, 23(1), 2020, 401–419.

³⁵ J. Adler, The public's burden in a digital age: Pressures on intermediaries and the privatization of Internet censorship, *JL & Pol'y*, 20, 231, 2011.

³⁶ Accountability is the relationship between an actor and a forum in which the actor must explain and justify his or her conduct. The forum can pose questions and pass judgment, and the actor may face consequences. Since authoritarianism presupposes power, its authority presupposes asymmetric relations among hierarchically ordered unit members. As a result, the relationship being sabotaged is one of downward accountability. See M. Bovens, Analysing and Assessing Accountability: A Conceptual Framework. *European Law Journal*, 13, 2017, 447–468; M. Glasius, Authoritarian Practices as Accountability Sabotage, in *Authoritarian Practices in a Global Age*, M. Glasius, Oxford University Press, 2023, 10–38.

³⁷ O. Schlumberger, How Authoritarianism Transforms: A Framework for the Study of Digital Dictatorship. *Government and Opposition*, 2023, 1–23.

requirements and the adoption of Internet protocols (IP) to delegate the regulation of information dissemination to the authority of sovereign states³⁸.

3.3. Emerging Global Challenges

Digital authoritarian regimes continually evolve their toolkit, resulting in the rise of four challenges:

1. Digital authoritarianism is expanding within consolidated autocracies through digital surveillance, censorship, social manipulation and advancing authoritarian visions of digital infrastructures and the Internet.
2. Digital authoritarian regimes extend their toolkit beyond national borders, exporting surveillance technologies, conducting cyberattacks towards regime critics and opponents abroad³⁹, engaging in electoral manipulation and building digital infrastructures. In line with the borderless nature of **cyberspace**, authoritarian power is no longer confined to a specific regime within geographic borders. This transnational challenge enables regimes to suppress dissent and control populations at home and abroad.
3. Digital authoritarians export their surveillance systems, malicious software and filtering capabilities to like-minded authoritarian states while growing their influence, setting international technology standards and advancing closed visions of the Internet.
4. The use of tools associated with digital authoritarianism is becoming pervasive within democratic societies, political parties, interest groups, and private companies at the expense of public trust, personal privacy and civil liberties. This challenge shows again that authoritarian power is no longer confined to a specific regime type; the digital authoritarian toolkit can manifest through authoritarian practices – patterns of actions that sabotage accountability to people over whom a political actor exerts control, resulting in disabling access to information and disabling voices. Whereas the twentieth century saw several waves of democratic liberalisation, scholars argue that the rise of **digital authoritarianism** indicates this century's trend in the opposite direction, one permeating autocracies and democracies alike.

³⁸ E. Yayboke, *op. Cit.* 1–11.

³⁹ This phenomenon can be defined as Digital Transnational Repression. States employ the conventional tactics of repression transnationally through digital technologies that enable instantaneous and constant communication across borders. This means that transnational repression is embedded in transnational authoritarianism and digital authoritarianism. M. Michaelsen, Far Away, So Close: Transnational Activism, Digital Surveillance and Authoritarian Control in Iran. *Surveillance & Society*, 15(3/4), 2017, 465–470.

Table 2 summarises the six components of the digital authoritarian toolkit (i.e. the digital authoritarianism taxonomy, composed of surveillance, censorship, cyberattacks, social manipulation and tools of great power). The table also highlights which strategies within the taxonomy are deployed to carry out the four challenges listed above. Surveillance primarily contributes to challenges (1), (2), (3), and (4). Censorship also contributes significantly to challenges (1), (3), and (4). Cyberattacks pose significant threats to challenges (2) and (3). Social manipulation significantly contributes to challenges (1), (2), and (4). Digital infrastructures play a role in challenges (1), (3), and (4). Advancing authoritarian visions of the Internet also contributes to challenges (1), (3), and (4)⁴⁰.

Challenges	Tools of repression, cooptation and legitimation				Tools of Great Power	
	Surveillance	Censorship	Cyberattacks	Manipulation	Digital infrastructure	Authoritarian Internet
Consolidated Autocracies	■	■	■	■	■	■
Targeted Adversaries	■	■	■	■	■	■
Export to like-minded states	■	■	■	■	■	■
Adoption in democracies	■	■	■	■	■	■

Table. 2 – The Digital Authoritarian Toolkit – creating a Taxonomy

⁴⁰ E. Yayboke, *op. cit.* 1-11.

4. Global patterns of digital authoritarianism

Digital authoritarianism defines authoritarian regimes' use of digital tools to supercharge longstanding survival tactics. In many cases, this entails autocrats' use of **digital repression** to control their citizens more effectively; still, digital autocracies use digital tools to co-opt support by enabling regime performance, mimicking elements of democracy, and increasing society's legibility to prevent discontent and influence beliefs and behaviours. For this discussion, digital repression refers to using digital technologies to repress citizens and maintain political control. Digital authoritarianism, therefore, is a broader concept than digital repression; however, at the same time, digital repression is **not** restricted to authoritarian settings: it can be employed in autocratic, hybrid, and democratic settings, although the latter use digital repression less than their autocratic counterparts. The following sections will examine the relationship between political system type and digital repression before delving into how authoritarian regimes rely on their digital authoritarian toolkit and understand its global patterns.

To empirically assess the global patterns of digital authoritarianism across regime types, I refer to the Digital Repression Index (DRI) and Digital Repression Capacity Index (DRCI)⁴¹. The Indexes were created on the basis of the Digital Society Project (DPS) data set, incorporating time-series data from 2003 to 2022⁴². DSP is insightful in separating capacity measurements from the actual enactments of digital tools; additionally, its cross-national data allows us to understand better how and where to intervene to curb internet-driven political violence, reduce electoral manipulation, and enhance democratic accountability. I organised the DSP indicators composing the DRI and DRCI Indexes to reflect what I referred to as the **digital authoritarian toolkit** (See **Table 2**, reflecting the taxonomy I describe below).

1. The level of digital surveillance is proxied to measuring governments' social media monitoring of political content (***v2mgovsmmon***).
2. The level of censorship is proxied by Internet filtering and social media censorship of political content in practice and capacity (***v2mgoufilprc***, ***v2mgovsnceprc*** and ***v2mgoufilcap***).
3. Social manipulation is measured using governmental and party-sponsored dissemination of false information on social media domestically (***v2mgovsmcenprc*** and ***v2goudom***) and governments' capacity to regulate online content using existing laws (***v2mregcap***).

⁴¹ The Indexes are calculated by referring to the data set created by the Digital Society Project (DSP), which contains eight DSP variables. See S. Feldstein, Digital Repression Index (updated 2021 data), **Mendeley Data**, V2, 2022.

⁴² DSP incorporates measurements for 179 country units. Following the scale of the measurement of the model variable (i.e. between -5 and 5, with 0 representing the mean for all country-years in the sample), a country displaying a negative score is performing below the mean for that variable (likewise, countries displaying positive scores are performing above the mean for the given variable). See V. Mechkova, D. Pemstein, B. Seim, S. Wilson, **Digital Society Project Dataset v4**, 2022.

4. The capacity to conduct cyberattacks is proxied by the measurements of governments’ social media and Internet shutdowns in practice (*v2mgovshut* and *v2mgovsm*) and in capacity (*v2mgovshutcap*). Additionally, I consider the targeted persecutions and arrests of online users for political content (*v2smarrest*) and the level of governments’ cybersecurity capacity⁴³ (*v2smgovcapsec*).

The selected DSP indicators serve as proxies for understanding the deployment of the digital authoritarian toolkit. Additionally, I also refer to the Varieties of Democracy (V-Dem) and the Regime of the World (RoW) classification by Lührmann, Tannenber, and Lindberg to provide insights into how digitalisation impacts democracies and to understand how the digital authoritarian toolkit can manifest itself across regime types⁴⁴. While I do not aim to replace the established regime-type literature classifying political regimes, I argue that, in line with the borderless nature of cyberspace, authoritarian power is no longer confined to a specific regime within geographic borders⁴⁵. In other words, I argue that the digital authoritarian toolkit may also be deployed within democracies. This tendency is confirmed when the DRI, DRCI Indexes and the DSP’s indicators reach levels comparable to their authoritarian counterparts. **Table 3** lists the selected indicators and explains how each reflects the components of the **digital authoritarian taxonomy**, constituting the basis for my quantitative analysis of the global patterns of digital authoritarianism.

Digital Authoritarianism Taxonomy	Applicable Digital Society Project (DSP) Variable
Surveillance Authoritarian Internet	Government social media monitoring of political content (<i>v2smgovsmmon</i>)
Censorship Authoritarian Internet	Government Internet filtering in practice (<i>v2smgovfilprc</i>) Government social media censorship of political content in practice (<i>v2smgovsmcenprc</i>) Government Internet filtering capacity (i.e. blocking access to websites) (<i>v2smgovfilcap</i>)
Manipulation	Government dissemination of false information on social media domestically (<i>v2smgovsmcenprc</i>) Party dissemination of false information on social media domestically (<i>v2smgovdom</i>) Government capacity to regulate online content by using existing laws (<i>v2smregcap</i>)
Cyberattacks Authoritarian Internet Digital Infrastructure	Government Internet shutdown in practice (<i>v2smgovshut</i>) Government social media shutdown in practice (<i>v2smgovsm</i>) Targeted persecutions of online users and arrests for posting online political content (<i>v2smarrest</i>) Government Internet shutdown capacity (<i>v2smgovshutcap</i>) Government cybersecurity capacity (<i>v2smgovcapsec</i>)

Table. 3 – The Digital Authoritarian Toolkit – Digital Society Project Indicators

⁴³ I included the measure of government cybersecurity capacity as closely related to a state’s ability to mitigate digital threats and carry out sophisticated strategies – comprising cyberattacks.
⁴⁴ A. Lührmann, M. Tannenber, S. Lindberg, Regimes of the world (RoW): Opening new avenues for the comparative study of political regimes. *Politics and governance*, 6(1), 60-77, 2018.
⁴⁵ M. Glasius, Extraterritorial authoritarian practices: a framework, *Globalizations*, 15(2), 179-197, 2018.

4.1. Digital repression across regime types

In this section, I provide insights into the global diffusion of digital repression practices and capabilities. **Figure 1** provides a regional overview of the DRI and DRI in 2022. The measurement model’s scale is between -5 and 5, with 0 representing the approximate mean for all country- years in the sample. Countries with negative scores perform below the mean. **Figure 1** shows that some regions are overrepresented in terms of their levels of digital authoritarianism. As of 2022, South and Central Asia and Africa exhibited the highest deployment of repression in cyberspace. Meanwhile, Europe, Eurasia, and Western Hemisphere countries had the lowest scores despite showing excess capacities for its enactment. Note that countries with poor human rights records display the highest global levels of digitally enabled repression, cooptation and legitimization.

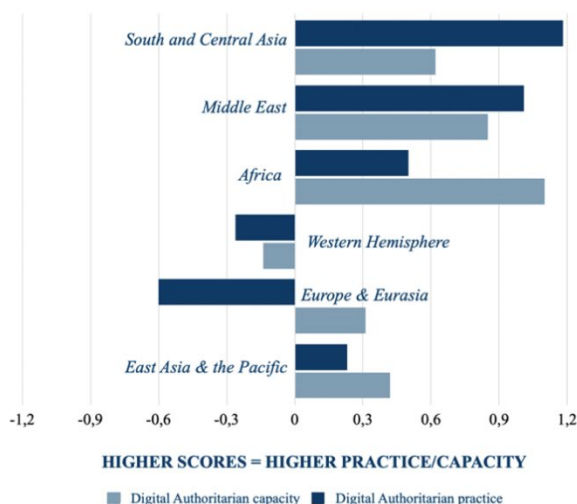


Figure. 1 – Regional distribution of the digital authoritarianism taxonomy in capacity and practice (2022)

Focusing on regime-type classifications, **Figure 2** displays the country-level scores in the DRI (2022). By referencing the Varieties of Democracy (V-Dem) and the Regime of the World (RoW), I classified their regime type. I used Freedom House’s Freedom of the Net (FOTN) Classification to assess their Internet freedom levels. High-scoring countries (i.e. North Korea, Turkmenistan, Eritrea, South Sudan, Iran, China and Syria) are exclusively closed or electoral autocracies and classified as “Not Free” by Freedom House’s Freedom of the Net (FOTN) Classification. Surprisingly, Russia, often coupled with China as a case study for **digital authoritarianism**, is absent from the top high-scoring DRI countries; interestingly, in two cases (e.g., Eritrea and South Sudan), lower digital repression capacity does not fully align with higher digital repression scores. This means that, when choosing which tactics to deploy from their toolkit, these states refrain from using sophisticated and costly tactics (i.e., spyware). Interestingly, there is little relationship between digital repression and national wealth: Saudi Arabia, UAE, and China are near the top of most global economic indices, while North Korea falls on the opposite end. Still, DPRK’s score is explained by its strict Internet connectivity restrictions and almost null Internet penetration levels. As expected, low-

scoring DRI countries in 2022 also align closely to regime types (i.e. Sweden, Denmark, Norway, Portugal, Lithuania, Finland, Belgium, Latvia, Netherlands). Every country is classified as an electoral and liberal democracy; interestingly, some countries possess advanced repression capabilities (e.g., Finland and Norway) but choose limited deployment. Several democracies have unexpectedly high digital repression scores: India and Brazil exhibit high DRI scores due to their high levels of state-sponsored Internet Shutdowns and political party-driven disinformation. In 2022, India shut down the internet 84 times, the highest number of any country worldwide for the fifth consecutive year. Still, Internet shutdowns are often deployed by countries that lack more sophisticated capabilities to counter mass protest movements; in this sense, they do not necessarily correlate with states exhibiting the highest levels of repression. Countries with poor democratic rankings (e.g., Belarus) displayed unexpectedly low DRI scores, while democracies ruled by illiberal leaders (e.g., Turkey) exhibit patterns more akin to autocratic counterparts, making clear that, rather than being anchored to conventional regime types, digital authoritarian practices can be observed in democracies, too.


Looking at different types of authoritarian regimes, **military dictatorships** rely on digital repression the most, whereas **personalist dictatorships** rely on it the least. **Monarchies** and **party-based dictatorships** are in the middle, though **party-based dictatorships** exhibit sizable variance. **Monarchies** have the most digital repression capacity, whereas **personalist dictatorships** have the least. The interesting takeaway here is that though personalist dictatorships are known to rely quite a bit on traditional forms of repression⁴⁶, they are the least likely of all dictatorships to use digital repression and to have the capacity to do so in a sophisticated fashion; thus, they mostly rely on rudimentary tactics, such as Internet shutdowns, which do not require high capacities. Overall, autocracies have fewer constraints on deploying the digital authoritarian toolkit, and the benefits for political stability are vast. Additionally, governments' reliance on traditional repression (e.g., imposing restrictions on civil liberties) significantly predicts digital repression. Still, there are a handful of electoral democracies that use digital repression substantially more than expected given their level of democracy (i.e. France, Nepal, and Taiwan) and of dictatorships that use digital repression markedly less than expected given their level of authoritarianism (i.e. Belarus and Thailand)⁴⁷. A ranking of authoritarian regimes' reliance on digital repression is provided in **Figure 3**; I considered authoritarian regimes that were in power as of 2022; the Figure indicates 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 2022⁴⁸.

⁴⁶ E. Frantz, *Authoritarianism: What Everyone Needs to Know*. Oxford University Press, 2018.

⁴⁷ S. Feldstein, *The rise of digital repression: How technology reshapes power, politics, and resistance*. Oxford University Press, 2021.

⁴⁸ Note that dark blue dots represent the regime's level of digital repression in 2022; the light blue dots represent the mean of the country-level DRI (2003-2022), while bars represent their range of scores (2002-2022).

Global distribution of digital repression in 2022

Digital Repression Index (2022) 
-1,43 3,26

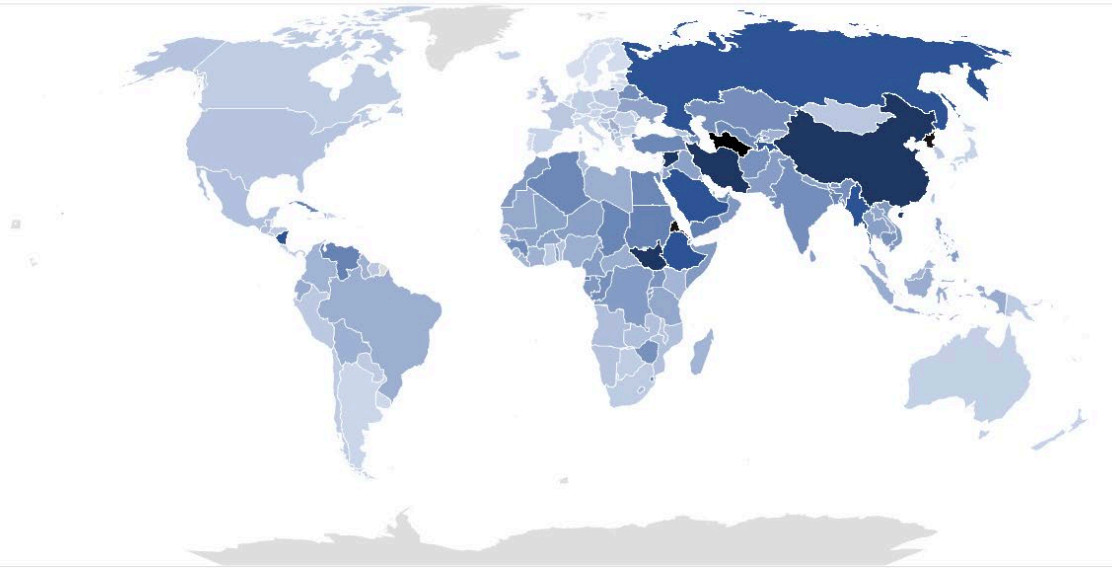


Figure 2. Global distribution of the Digital Repression Index (2022)

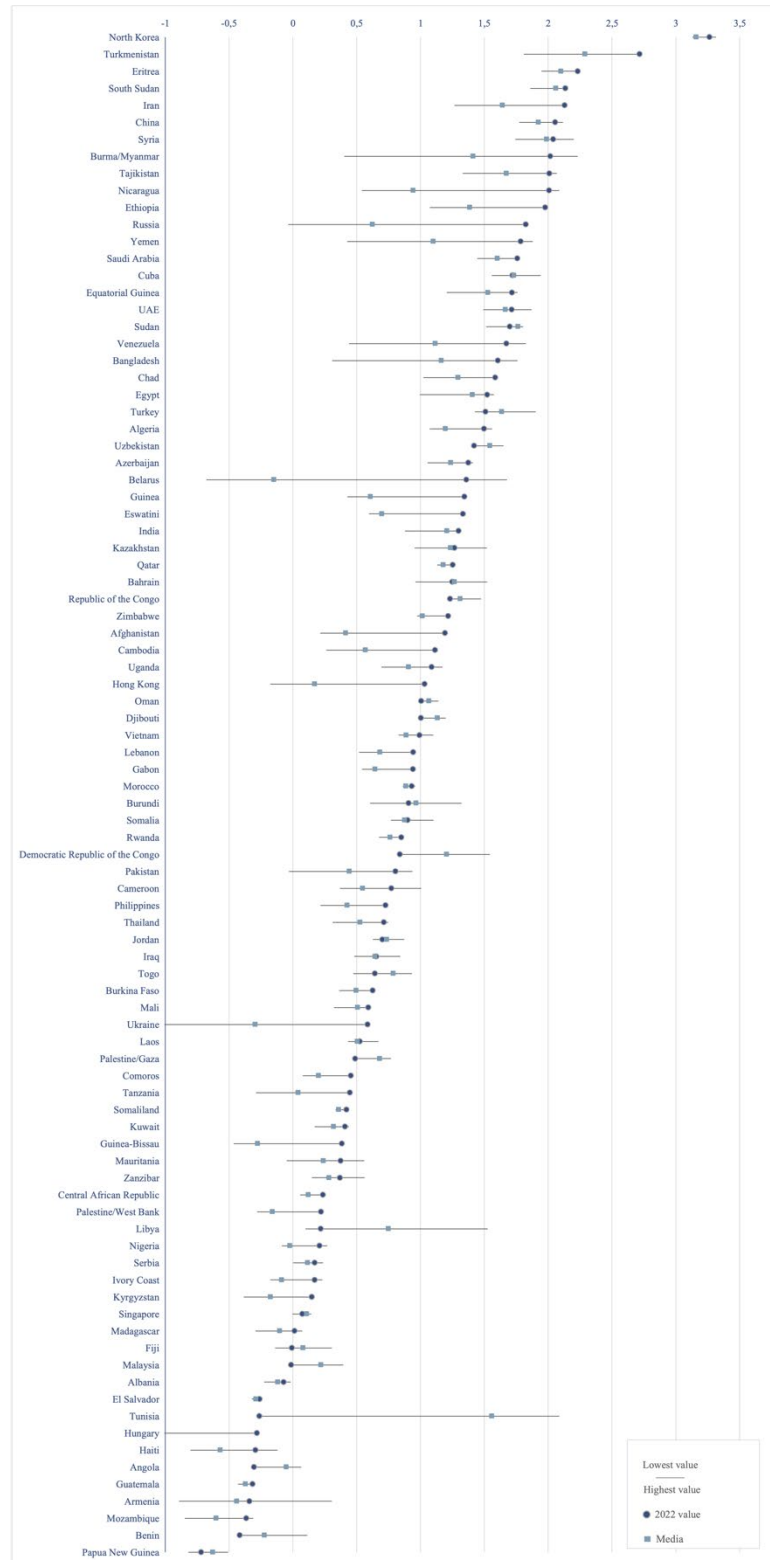


Figure. 3 – Ranking of DRI by authoritarian regime type (range, media and 2022)

4.2. Comparing Digital Repression Capacity and Practice

I now compare the capacity to enact the repressive dimension of the digital authoritarianism toolkit and its deployment across regime types. **Figure 4** illustrates the global trends of DRI and DRCI (2003-2022), suggesting a continued expansion of states' abilities to use digital tools for authoritarian purposes. This expansion is apparent after 2013 when the capacity to engage in digital repression became higher than its practical use globally. The rising tendencies of digital repression capacity and enactment are not unexpected – as dissent has moved online and digital tools have become cheaper, increasing the number of governments able to employ the digital authoritarian toolkit.

When looking at digital capacity, DSP's data reveal a nonlinear relationship with levels of democracy. Digital capacity tends to be highest among states that are the least democratic; it declines among hybrid states before increasing as states become highly democratic. While generally liberal and electoral democracies can engage in digital repression but refrain from deployment, closed and electoral autocracies exhibit apparent rising digital authoritarian tendencies, with the toolkit's deployment consistently exceeding regimes' domestic repression capacity. In **democracies** (i.e. liberal democracies and electoral democracies), governments with high capabilities (e.g., Estonia) also have political safeguards to mitigate the risk of using these tools for political repression. This is consistent with research on the effect of COVID-19 and the spread of health-related surveillance technology. At the same time, consolidated democracies managed to navigate the initial stages of crisis without significantly compromising democratic standards, adopting surveillance technology to facilitate pandemic responses that were proportional, limited in time and scope, and subject to democratic oversight⁴⁹. Looking at the state's approach to regulating online content, dictatorships are more likely than democracies to have the government take the lead. In contrast, democracies rely more on private actors to regulate online content. Differently, complete and electoral authoritarian regimes bridge the digital repression gap by relying on external suppliers – as highlighted by challenges (2) and (3) posed by digital authoritarianism.

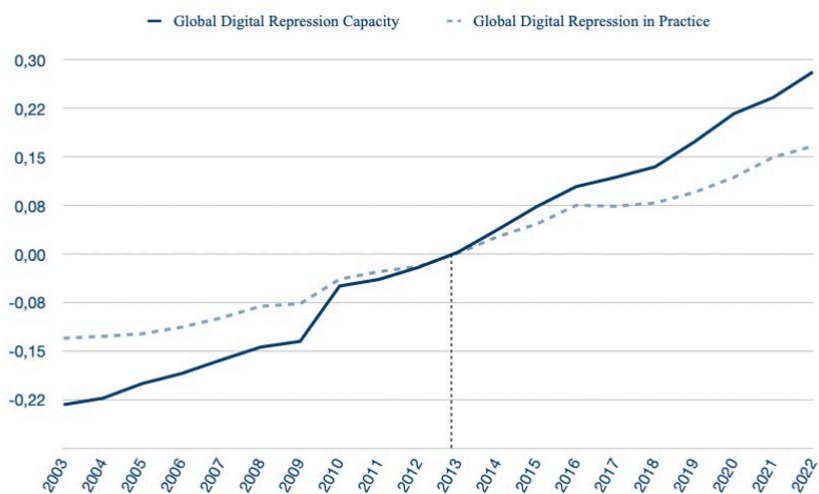
Looking at the components of the digital authoritarian toolkit, dictatorships currently have a high capacity to filter the Internet, followed by the ability to shut it down; they rank lowest in the capacity variables regarding cyber security. Global leaders in digital surveillance include Saudi Arabia and China, following North Korea. Since 2010, governments have been relying more widely on social media monitoring, aligning with the growth of online-based social movements for offline action. Additionally, inventories of commercial spyware confirm that China, Iran, Saudi Arabia, and North Korea are employing commercial malware for surveillance purposes, explicitly targeting political opponents, civil society activists, independent journalists, and regime critics⁵⁰. Regarding **social manipulation**, the gap between autocracies and democracies is narrow. Even in democracies with a lower DRI (e.g., Brazil), the spread of disinformation and misinformation, especially during significant events like national elections, are at high levels. Looking at the 2019-2021 time series, it is clear that the COVID-19 pandemic accelerated the adoption of social

⁴⁹ S. Greitens, Surveillance, Security, and Liberal Democracy in the Post-COVID World, *Int Org*, 74(S1), E169–E190, 2020.

⁵⁰ S. Feldstein, Commercial Spyware Global Inventory, *Mendeley Data*, V2, 2020.

manipulation, with China, Iran, Russia, and Turkey leading in disseminating pro-government narratives domestically and abroad. However, preventing online access is often more impactful – and effective – than controlling information: while Internet shutdowns are usually chosen by countries lacking sophisticated capabilities, DDoS and Internet filtering expand the censorship possibilities of politically sensitive content while offering states considerable deniability. Finally, it is worth noticing that as technology becomes more affordable, the rise of digital authoritarianism is anticipated to accelerate.

Figure. 4 – Digital Repression Capacity Compared to Digital Repression in Practice (2003-2022)



5. Conclusion: Responding to Digital Authoritarianism

The intersection of politics and digital technology is a two-way domain, and not just authoritarian regimes have advantages. Indeed, this field provides opportunities for democracies, civil society, and political activists to combat the rise of digital authoritarianism⁵¹. A critical overview of the extant literature reveals recurring themes and debates about what should be done to deal with the escalating trajectory of digital authoritarianism. **Firstly**, observers stress the pressing need to regulate private companies selling digital products with repressive potential. While the discourse acknowledges the possibility of self-regulation by businesses, the prevailing sentiment leans towards the imperative for governments to assume a more assertive role in regulatory frameworks⁵². Challenges associated with self-regulation, including its ineffectiveness and the lack of mechanisms for accountability, necessitate a more explicit articulation of the rights companies commit to safeguard users and the mechanisms in place to ensure such commitments⁵³. Companies must commit to rigorous human rights impact assessments for new markets; granting users control over their information, ensuring fair and transparent content moderation practices, and engaging in continuous dialogue with local civil society organisations are pivotal steps in building a digital environment that respects user rights.

Additionally, observers recommend tightening import and export controls to limit the spread of digital tools that can be used for repressive purposes while contending the need for stricter sanctions for those technology companies and governments that use and export repressive digital technologies⁵⁴. **Secondly**, democracies are strongly encouraged to promote international frameworks to deal with the rise of digital repression (e.g., the United Nations Guiding Principles on Business and Human Rights)⁵⁵ integrating digital technologies into existing human rights frameworks, leveraging established guidelines to counteract their potential for human rights violations⁵⁶. **Thirdly**, the role of civil society is crucial in holding governments and private companies accountable – fact-checking initiatives, monitoring collaborations with authoritarian regimes and continually raising awareness about government censorship and surveillance on data silos⁵⁷. **Fourthly**, at national and international levels, policymakers are responsible for championing the cause of

⁵¹ A. Shahbaz, The Rise of Digital Authoritarianism, *Freedom House*, 2018.

⁵² E. Yayboke, *op. cit.*

⁵³ A. Polyakova, C. Meserole, Exporting digital authoritarianism: The Russian and Chinese models, *The Brookings Institute*, 2019.

⁵⁴ United States Agency for International Development, DIGITIZED AUTOCRACY, 2021.

⁵⁵ S. Feldstein (2021), *op. cit.*

⁵⁶ E. Frantz, A. Kendall-Taylor, and J. Wright, Digital Repression in Autocracies, *V-DEM Institute*, 2020.

⁵⁷ N. Wright, Intelligence and Democratic Norms: Meeting the Authoritarian Challenge, *National Endowment for Democracy Sharp Power and Democratic Resilience Series*, 2020.

human rights in the digital sphere⁵⁸. Governments must proactively review and rectify any laws or practices encroaching on Internet freedom, from arbitrary website blockades to extralegal surveillance. Enacting robust data protection laws is paramount, ensuring transparency, user control, and strict principles governing the processing of personal data⁵⁹. **Finally**, a critical component of the strategy to counter digital authoritarianism sees democracies as role models in Internet management⁶⁰. Parallel to ensuring Internet Freedom, democracies need to posit the concept of human rights by design and urge the international community to encourage companies to consider human rights implications while developing new technologies, including AI-enabled technologies⁶¹.

Acknowledgements

Il presente paper è stato realizzato nell'ambito del progetto "Geopolitica del Digitale", promosso dalla Fondazione Med-Or, in collaborazione con il Center for International and Strategic Studies (CISS) della Luiss Guido Carli, grazie al sostegno della Fondazione Compagnia di San Paolo all'interno del bando "Geopolitica e tecnologia".

⁵⁸ T. Dragu, Y. Lupu, Digital Authoritarianism and the Future of Human Rights, *International Organization*, 2021, 1-27.

⁵⁹ J. Penney, S. McKune, L. Gill, and R. Deibert, Advancing Human Rights By Design in the Dual-Use Technology Industry, *SIPA Journal of International Affairs*, 2018.

⁶⁰ Freedom House, FREEDOM ON THE NET 2023: The Repressive Power of Artificial Intelligence, 2023.

⁶¹ E. Donahoe, M. MacDuffee Metzger, An Intelligent Human Rights Agenda for Artificial Intelligence, *Power 3.0: Understanding Modern Authoritarian Influence*, 2019.

About Luiss School of Government

The Luiss School of Government (SoG) is a graduate school training high-level public and private officials to handle political and government decision-making processes. It is committed to provide theoretical and hands-on skills of good government to the future heads of the legislative, governmental and administrative institutions, industry, special-interest associations, non-governmental groups, political parties, consultancy firms, public policy research institutions, foundations and public affairs institutions. The SoG provides its students with the skills needed to respond to current and future public policy challenges. While public policy was enclosed within the state throughout most of the last century, the same thing cannot be said for the new century. Public policy is now actively conducted outside and beyond the state. Not only in Europe but also around the world, states do not have total control over those public political processes that influence their decisions. While markets are Europeanised and globalised, the same cannot be said for the state.

The educational contents of the SoG reflect the need to grasp this evolving scenario since it combines the theoretical aspects of political studies (such as political science, international relations, economics, law, history, sociology, organisation and management) with the practical components of government (such as those connected with the analysis and evaluation of public policies, public opinion, interests' representation, advocacy and organisational leadership).

For more information about the Luiss School of Government and its academic and research activities visit www.sog.luiss.it

May 2024

Luiss
School of Government

Via di Villa Emiliani 14
00197 Roma
T +39 85 225052
sog@luiss.it