Democracies, Dictatorships, and Digital Technologies

The Transformations of Politics and Political Systems in the Twenty-First Century

Dissertation

zur Erlangung des Doktorgrades

der Wirtschafts- und Sozialwissenschaftlichen Fakultät

der Eberhard Karls Universität Tübingen

vorgelegt von

Koray Saglam, M.A.

Tübingen

2024

1. Betreuer:	Prof. Dr. Oliver Schlumberger
2. Betreuer:	Prof. Erica Frantz, Ph.D.

Tag der mündlichen Prüfung:	01.07.2024
Dekan:	Prof. Dr. Frank Stähler, stv. Dekan

1. Gutachter:	Prof. Dr. Oliver Schlumberger
2. Gutachter:	Prof. Erica Frantz, Ph.D.

Plagiatserklärung:

Ich erkläre hiermit, dass ich die zur Promotion eingereichte Arbeit mit dem Titel "Democracies, Dictatorships, and Digital Technologies - The Transformations of Politics and Political Systems in the Twenty-First Century" selbstständig verfasst, nur die angegebenen Quellen und Hilfsmittel benutzt und wörtlich oder inhaltlich übernommene Stellen als solche gekennzeichnet habe. Ich versichere an Eides statt, dass diese Angaben wahr sind und dass ich nichts verschwiegen habe. Mir ist bekannt, dass die falsche Abgabe einer Versicherung an Eides statt mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft wird.

Tübingen, den

Koray Saglam, M.A.

Statement of Authorship:

I hereby declare that I have independently authored the thesis submitted for the attainment of the doctoral degree titled "Democracies, Dictatorships, and Digital Technologies - The Transformations of Politics and Political Systems in the Twenty-First Century", utilizing only the specified sources and aids, and have duly indicated any directly quoted or paraphrased passages as such. I solemnly affirm that these statements are true and that I have not withheld any information. I am aware that making a false declaration under oath may be punished with imprisonment for up to three years or with a fine.

Tübingen,

Koray Saglam, M.A.

Für Dede

und meine Großeltern,

die all dies erst möglich machten.

Für Mama und Papa,

und all eure Entbehrungen.

Für Lea

und das Licht, dass du in mein Leben trägst.

Further, I would also like to express my gratitude to my friends, and colleagues, who helped me overcome every obstacle on this journey – Tobi, Fabi, Peter, Dominic, Stief, Petra Will, Miri, André, Ahmed, Thomas, Erica, Oli, Sarah, Thore, Edward,Vicky, Felix, Jane, Philipp, Pascal, Benni, Toni, Janosch, Lara, and Nicole.

I am also grateful for the generous scholarship awarded by the ZEIT-Stiftung Bucerius.

Table of Contents

1. Introduction (Framework Paper) 4
1.1. Technologies and transformations 4
1.1.1. The proliferation of digital technologies 5
1.1.2. Politics, political systems, and digital transformations 6
1.2. How digital technologies transform politics 8
1.2.1. The political economic nexus of digital technologies and authoritarian practices 8
1.2.2. Shopping with Orwell 10
1.2.3. How authoritarianism transforms 10
1.2.4. Information environment and democratic decay 12
1.3. The core contributions 14
2. The digital blender: conceptualizing the political economic nexus of digital technologies and authoritarian practices 15
2.1. Introduction 16
2.2. The digital blender in a nutshell 18
2.3. Developing a relational perspective on digital technologies 20
2.3.1. The technical characteristics of digital technologies 21
2.3.2. Relating technical characteristics to commercial dynamics of capital accumulation 22
2.3.3. The political embeddedness of digital technologies 23
2.4. Authoritarian and illiberal practices beyond the state 24
2.4.1. Meta platforms inc. – providing virtual spaces and digital infrastructure for coercive practices 25
2.4.2. Cambridge Analytica – transnational commodification of electoral manipulation 27
2.4.3. NSP group – Interlocking state and capital interests via commodified coercive practices 29
2.5. Conclusions 31
2.5.1. A proto-typology of tech companies 32
2.5.2. Imaginaries and manifestations of authoritarian power and its contestation 32
2.5.3. Limits of the digital blender and ways forward 34
3. Shopping with Orwell: procurement patterns of commercialized surveillance software 35
3.1. Introduction 36
3.2. Digital Technology, Politics, and the Commercialization of Global Repression 38
3.3. Determinants of Acquisition 40
3.4. Research Design 43
4.3.1. Drawbacks and Assumptions 43
4.3.2. Concepts and Operationalizations 48
3.5. Analysis 50
3.5.1. Overview over mercenary surveillance software acquisitions 50
3.5.2. Model specification 52

3.5.3. Model specification ... 54
3.5.4. Results for structural determinants and MSS acquisition ... 54
3.5.5. Results for Structural Determinants and Digital Repression Capacity ... 60
3.5. Interpretation ... 61
3.5. Outlook ... 63
4. How authoritarianism transforms: a framework for the study of digital dictatorship ... 66
4.1. Introduction ... 67
4.2. A new framework for analysis: why and how? ... 68
4.3. The dictator's perpetual agenda: power maintenance ... 72
4.4. Enter the digital ... 74
4.4.1. Techniques to know ... 75
4.4.2. Techniques to influence behavior ... 78
4.4.3. Techniques to influence beliefs ... 80
4.5. Transformations of political dynamics in authoritarian regimes ... 82
4.5.1. New elite actors and partially reconfigured regime composition ... 82
4.5.2. Institution-building and -reconfiguration ... 83
4.5.3. The intension of political rule: reconfigured state-society relations ... 85
4.5.4. The reconfiguration of coalitions and micro-steered co-optation ... 86
4.5.5. The frequency, forms and targeting of repression ... 87
4.5.6. Legitimacy and informational agnosticism ... 88
4.5.7. The extension of political rule: the transnational reach of power ... 89
4.6. A technologically induced transformation of authoritarian politics ... 92
5. Information doubt and decay: how digitization spurs democratic decay ... 93
5.1. Digitization, Information, and democratic decay ... 94
5.2. How digitization transforms citizens' information environment ... 97
5.3. Why informational agnostics and misbelievers endanger democracy ... 100
5.4. Our Cases: US and Germany ... 103
5.4.1. From "Stop the Steal" to the steps of the Capitol ... 106
5.4.2. From COVID scepticism to the steps of the Reichstag ... 108
5.5. Conclusion ... 111
6. Conclusions (Framework Paper) ... 113
6.1. Democracy at risk… ... 113
6.2. … autocracy on the rise… ... 115
6.3. … and companies profiting. ... 117
6.2. Dependence, convergence, and classification ... 118
6.2.1. Perpetuating dependencies, internalizing profits, and socializing externalities ... 119
6.2.2. Democracy and autocracy in the twenty-first century ... 123
7. References ... 129
8. Appendix ... i

1. Introduction (Framework Paper)

1.1. Technologies and transformations

What are the effects of digitally induced transformations of politics and political system in the twenty-first century, and what are the corresponding consequences? Technological advancements have always shaped the structures and processes through which humans compete for power, and how they exercise it over one another, from taming fire to the discovery of gun powder. If power is understood as "[…] any opportunity within a social relationship to enforce one's own will even against resistance, regardless of the nature of this opportunity" (Weber 1921, 28), then any technologically enabled advancement of these opportunities can potentially cause far-reaching consequences for politics, understood as the "[…] the authoritative allocation of values for a society" (cf. Easton 1965, 50).

With the advent of digital technologies and their advancing proliferation, human civilization is witnessing such a fundamental technologically induced transformation of politics and power: Only two decades into the twenty-first century, and there is barely any aspect of human life left that has not been affected by new and digital information and communication technologies (ICTs) and the advancement of digital infrastructures. On par with the steam engine during the first wave of the industrial revolution, and electricity in the second one, the advent of digital ICTs, and the resulting dissolution between the physical and digital realms, have already come to be labelled as third and fourth wave of industrialization, respectively (Schwab 2016a; 2016b).[1]

Much like the ripples caused by the discovery of steam power, and the subsequent tsunami that was the steam engine, digital technologies have come to cause far-reaching transformations of our lives as well:

[1] Digital technologies are to be understood as technological devices and services that are based on the electronic transformation of analogue and continuously scaled information signals into discretely binary scaled ones (i.e., digitized information, cf. Bloomberg 2018; Gupta 2020; Legner et al. 2017). This conceptual understanding consequently serves as a broad and overarching category that entails information technology (IT), and information and communication technology (ICT), so that it encompasses, among other, the internet, servers, social media platforms, digital services, audio-visual recording devices, personal computers, and smart devices; smart devices, in turn are to be understood as devices that exchange data with other devices and servers through internet connections and other wireless forms of information transmission such as Bluetooth or infrared (cf. Silverio-Fernández, Renukappa, and Suresh 2018).

Never before has humanity been able to access, collect, analyze, and exchange information at such speeds, and never before has knowledge been produced and made accessible at comparable rates. Imaginings previously confined to science-fiction have not only been realized but have found their ways into our daily lives already. Consequently, this thesis engages with the questions concerning the proliferation of such technologies and how they affect political systems and politics in the twenty-first century. More specifically, it focuses on how the effects of digital technologies on democracies and autocracies, and their political economic underpinnings, and how to study these transformations.

1.1.1. The proliferation of digital technologies

Digital technologies have changed the way we communicate and consume information, how we interact with another, and how we perceive of the world. They have lowered the threshold to produce and consume media content, fundamentally altering the way that cultural industries work (Massi 2021), changing the creative and organizational dimensions of cultural creation (Bannikova et al. 2023), and creating new creative potentials through new entrepreneurial modes of commodification (Lazzeretti et al. 2022). In medicine, digital technologies revolutionize various subdisciplines through the advancement of new diagnostical and therapeutical methods (Li et al. 2013; Béranger and Rizoulières 2021) – not the least exemplified by their invaluable role in curbing the scope of the SARS-CoV-2 pandemic: Without the latest big data-based predictive modelling technologies, and digital contact-tracing mechanisms, this pandemic could have had much worse consequences worldwide (Alghamdi and Alghamdi 2022).

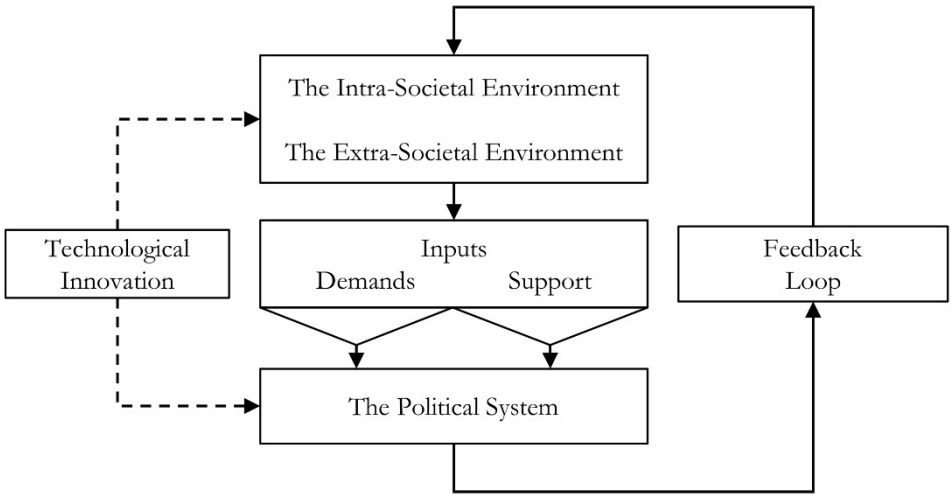
Likewise, digital technologies have fundamental and transformative effects on education (West 2012) by altering the underlying structures of knowledge industries with far reaching changes of the accessibility of knowledge, as well as speed and scope of knowledge production and diffusion (Fabre, Messerschmidt-Mariet, and Holvoet 2016; Bensoussan et al. 2018). And whether it is e-commerce, platform economies, predictive modelling, or generative artificial intelligence and automated intelligent manufacturing: countless changes of the economic sector have fundamentally altered modes of production and consumption (Furman and Seamans 2019; Kassem 2023; Staab 2019; Śledziewska and Włoch 2021; Guerrieri and Bentivegna 2011)

Taken together, these technologically induced changes of human interaction amount to transformations comparable to previous waves of industrialization (Philbeck and Davis 2018; Caruso 2018; Schwab 2016a; 2016b), and therefore warrant appropriate and systematic analyzes, especially with respect to their political economic and political ramifications.

1.1.2. Politics, political systems, and digital transformations

The effects of digitally-induced transformations on the authoritative value allocation in a society (cf. Easton 1965, 50) can be conceptualized to work through two ways: First, they can indirectly affect the political system through systemic changes in, and of, extra- and intra-societal environmental systems (Easton 1965, 108–11). These environments entail, as highlited in the previous section, other ecological, cultural, or social systems on a national and international level (Ibid.). The changing extra- and intra-societal environments, in turn, stand in a reciprocal relationship with the political systems: They shape new inputs of the political system, and interact in new ways with the respective systemic outputs (Ibid., see Figure 1).

Figure 1 Where technological innovations affect political systems (based on Easton 1965, 110)



Second, digital transformations can also directly affect the political system itself. New means of communication and transportation ultimately change the possibilities and speed of how power can be delegated, exercised, and contested (cf. Schlumberger et al. 2023), and how demands are transformed into outputs. New technologies will require new expertise, potentially changing the composition of actors needed

within a political system (Ibid, 11). And the cross-national nature of these infrastructures alters the geographic scope of political power (Ibid, 16; cf. also Saglam 2022). All this can impact on the nature and composition of the formal and informal processes, actors, and structures involved in transforming inputs into outputs (cf. Fishman 1990, 428).

What must not be neglected, however, is that digital technologies themselves are not a force *ex machina*. They emerge within this complex interplay of different systems as products and services that are provided by private sector companies (Saglam 2022). It is therefore important to avoid a *functionalist* understanding of digital innovations, i.e., treating these technologies merely as tools that are at the disposal of their masters (Ibid). Such a perspective would neglect the economic systems in which these technologies are embedded in, and the effects these might have on political systems. Also, technologies by *themselves* do not cause social change; instead, it is partially through their use, but especially through their reciprocal relationship with other systems that they shaped change (cf. Caruso 2018).

Consequently, to fully grasp technological changes, and to adequately analyze the transformative effects of digital innovations, a *relational* perspective is required (Saglam 2022). This requires acknowledging the technical characteristics of digital innovations, as well as their political economic embeddedness as infrastructure and commodified goods and services (Ibid). As infrastructures, these technologies further accelerate globalization, i.e., the interconnectedness of societies and their consciousness about this development (cf. Robertson and White 2007, 64).[2] Their proliferation is shaped by existing power structures that determine where and to what extend these new infrastructures are implemented, how they are regulated, who operates them, and to what ends (cf. Bogart 2022). Likewise, as goods and services, their purpose is also of commercial nature, highlighting the relevance of economic dynamics in the analysis of digital transformations.

[2] Here, the concept of infrastructure is introduced as a means to capture the relational nature of digital technologies as they provide new, digital spaces in the form of online platforms, but also entail the advancement and integration of physical structures and devices into everyday lives, from cable-systems and transmission towers, to servers and terminal devices such as smartphones.

1.2. How digital technologies transform politics

This myriad of complex systemic interrelations between digital technologies, their political economic embeddedness, and their effects on 'the political' thus warrants careful analysis. To get a better sense of these transformations and relations, it is helpful to consider political regimes, i.e., "[…] the formal and informal organization of the centre of political power, and of its relations with the broader society" (Fishman 1990, 428). Regimes determine "[…] who has access to political power, and how those who are in power deal with those who are not" (Ibid). This perspective sheds light on two stakeholders: incumbents as *those in power*, and societies as *those not in power*. Additionally, and incorporating the relational understanding of digital technologies into this analysis, tech-companies emerge as a third group of stakeholders. Thus, a comprehensive analysis of the transformative impact of digital technologies on political systems, and politics in generally, also requires a nuanced consideration of the formal and informal interplay of these three stakeholder groups.

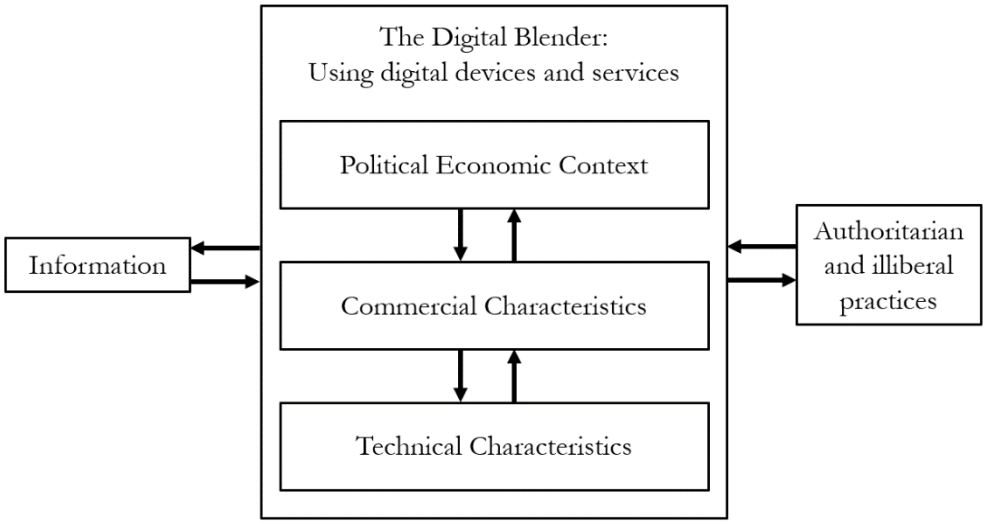
Consequently, this dissertation approaches the analysis of digitally induced transformations of the political sphere with a regime perspective, and a relational conception of digital technologies. This incorporates the power structures between societies, incumbents, and companies, in which these technologies are embedded in. In its first part, i.e., Chapter 2 and 3, the thesis engages with the political economic dimensions, and the nexus between private sector companies and the state. The second part, i.e., Chapter 4 and 5, turns towards regimes and political systems more explicitly, and highlights the intersection of authoritarian ruling logics with 'the digital', as well as how societies are affected by transformed information environments in the context of democratic political systems.

1.2.1. The political economic nexus of digital technologies and authoritarian practices

The first article (Chapter 2) presents the political economic relational perspective of digital technologies (published as Saglam 2022). Its contribution lies in the development of a first, comprehensive theoretical framework that links the technical and commercial nature of digital technologies to the political economic dynamics between tech-companies and governments. To this end, the article develops the heuristic tool of the *digital blender*: a triadic model of digital infrastructures that links the (a) technical with the (b) commercial characteristics of digital technologies, and then relates those to their political economic context of coercive

forms of capital accumulation (cf. Bruff and Tansel 2019; Jessop 2019; Tansel 2018; 2017). This model structures how, through digitization, information enters a complex set of technical, commercial, and political economic dynamics geared towards profit generation. These structures, then, incentivise the use of this information in the context of illiberal and authoritarian practices, such as digital surveillance or information manipulation (see Figure 2).

Figure 2 The digital blender (source: author's own compilation, based on Saglam 2022)



The theoretical lens of the digital blender highlights the transformative effects of digital technologies on political spatiality, as well as the role of tech-companies that develop and market digital products and services (cf. Deibert 2019; Zuboff 2019; Glasius 2018a). The industry of digital technologies, as well as the new virtual spaces they create, are gravely underregulated. Together with the territorially transcendent nature of these infrastructures, companies are incentivised to develop new ways to capitalize on digitally facilitated illiberal practices. This renders companies that engage in such business models to be complicit in coercion and repression: either as facilitating actors that provide the infrastructure for such practices without preventing malevolent practices, or as perpetrators that provide commercialized forms of manipulation, surveillance, and repression. These roles are exemplified by investigating the roles the tech companies NSO Group, Cambridge Analytica, and Meta Platforms Inc.

1.2.2. Shopping with Orwell

Chapter 3 elaborates on the political economic dimension of digital technologies and the private sector companies' role as facilitators and perpetrators of coercive practices. The main contribution of this article lies in presenting the first systematic large-n tests of the propositions regarding the determinants of public procurement decisions from the private surveillance technology industry. Regimes of all traits want to possess the powerful capabilities of digital surveillance, be it for criminological and national security concerns, or repression and power maintenance strategies. However, the development of own surveillance technologies can be costly and resource intensive (Palmer 2024; cf. also Feldstein 2021, 63; as well as Schlumberger et al. 2023, 11). Providers from the private sector, which are predominately located in the Global North (Feldstein and Kot 2023a), might therefor appear as cost-effective alternative (Ibid). To test these theoretically derived, yet partially contradicting hypotheses the article analyzes recently published data on the procurement of surveillance software by governments.

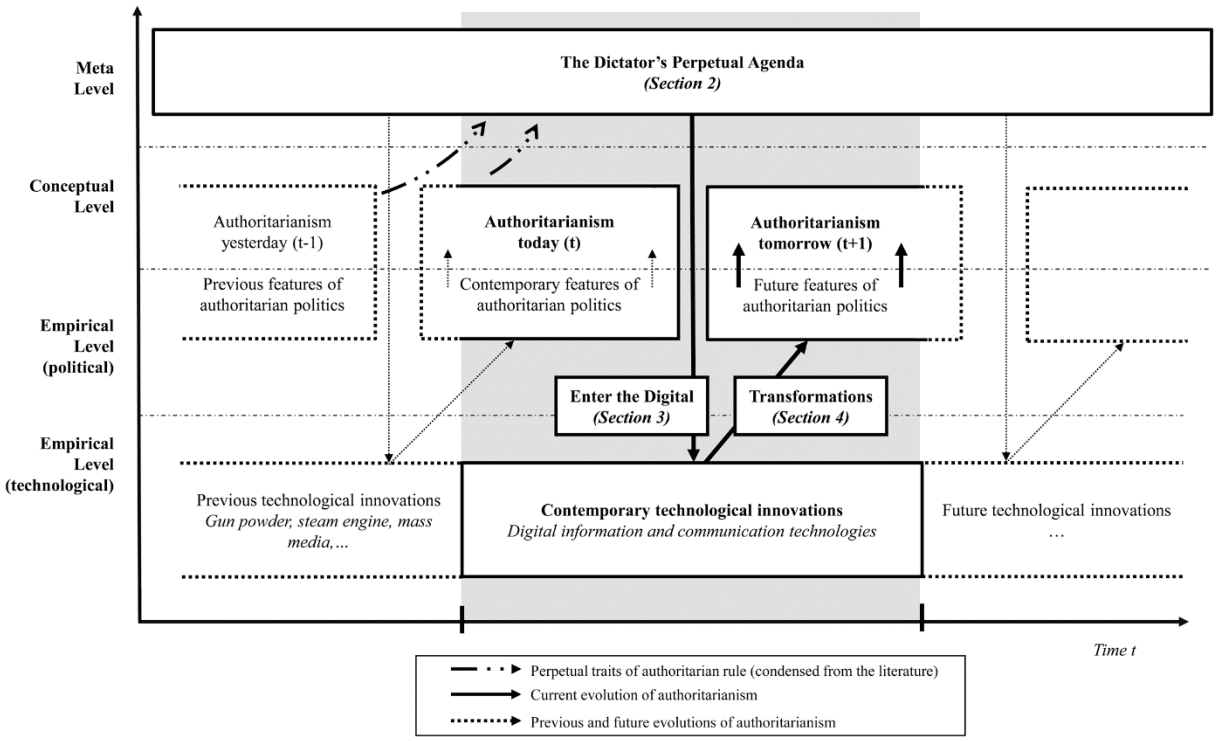
The analysis finds qualified support for a substitution effect where, *ceteris paribus*, factors such as limited financial resources or human capital can be compensated if the respective regimes turn to the private sector. Beyond that, however, regimes characteristics do not help to explain procurement patterns, if other variables are controlled for. Based on these findings, then the article discusses two points that arise: (I) The necessity of more effective regulatory frameworks of surveillance industries; (II) a critical observation of the patterns of acquisition between by different political regimes. Further, these findings are contextualized by discussing their implications concerning the wider political economic dynamics of digital technologies that perpetuate global structures of dependence, as well as regarding the context of global democratic backsliding and mounting challenges in classifying democracies and autocracies in the twenty-first century. Together with the findings of Chapter 4 and 5, these points are then further elaborated on in Chapter 6.

1.2.3. How authoritarianism transforms

Chapter 4 is a collaboratively written article that proposes a framework and research agenda for the study of digitally induced transformations of authoritarian regimes and authoritarianism in the twenty-first century. Previous technological innovations, such as the steam engine or mass media, have altered the ways

for autocrats to maintain and perpetuate power (see also Figure 3). Consequently, this chapter engages with the ways in which digital technologies interact with this autocratic agenda in the digital age.

Figure 3 The argument (source: Schlumberger et al. 2023, 4)



To do so, it condenses the literature on authoritarianism into "The Dictator's Perpetual Agenda" (Schlumberger et al. 2023, 6), i.e., a triparted disaggregation of ruling dimensions related to the overarching motivation of autocrats to maintain power (see Table 1): To achieve the overarching goal of continued incumbency, autocrats must control their subjects. To do so, they need to know about challenges and options that could potentially affect this objective. This enables autocrats to then either influence their subjects' behaviors through coercion and cooptation, or – more preferable and effective – to control their beliefs and convince them about the righteousness of their incumbency, and the futility of seeking alternatives.

Based on this authoritarian ruling logic, then, the chapter maps out different digital innovations and how they relate and interact with the dimensions of autocratic power maintenance. The mapping of these technologies highlights how most digital innovations do not simply adhere to only one dimension of the dictator's agenda. Instead, many technologies, like AI-assisted CCTV cameras linked to massive databases, as in the case of China's Scoail Credit System (cf. Qiang 2019), serve multiple purposes at once and

automatize control. Consequently, digital technologies are not merely another set of instruments in the toolkits of autocrats: Instead, these technologies hold the potential to fundamentally transform various aspects of authoritarian power maintenance strategies.

Table 1 The dictator's agenda (source: Schlumberger et al. 2023, 6).

Control subjects					
Know		**Influence beliefs**		**Influence behavior**	
Collecting information	Processing information	Constructive: through creation and promotion of narratives	Destructive: through discrediting and censoring narratives	Negative incentives and sanctions (mostly repression)	Positive incentives (mostly cooptation)

These transformations are then presented along seven clusters. These entail (I) changes of the relevance and composition of elite actors, and the emergence of new ones; (II) new structures and processes that will affect how autocratic rule is maintained; (III) a reconfiguration of state-society relations; (IV) new coalitions and modes of configuration; (V) changing patterns of repression; (VI) new legitimation strategies, as well as (VII) an extension of the geographical scope of autocratic rule. Taken together, these transformations might very well change the face of authoritarianism in the twenty-first century.

The contributions of this article are therefore threefold: (I) it provides a well-structured model of the autocratic ruling logic; (II) it maps different digital technologies and how technological innovations interact with autocratic ruling strategies; and (III) it provides an agenda for the research of authoritarianism in the twenty-first century.

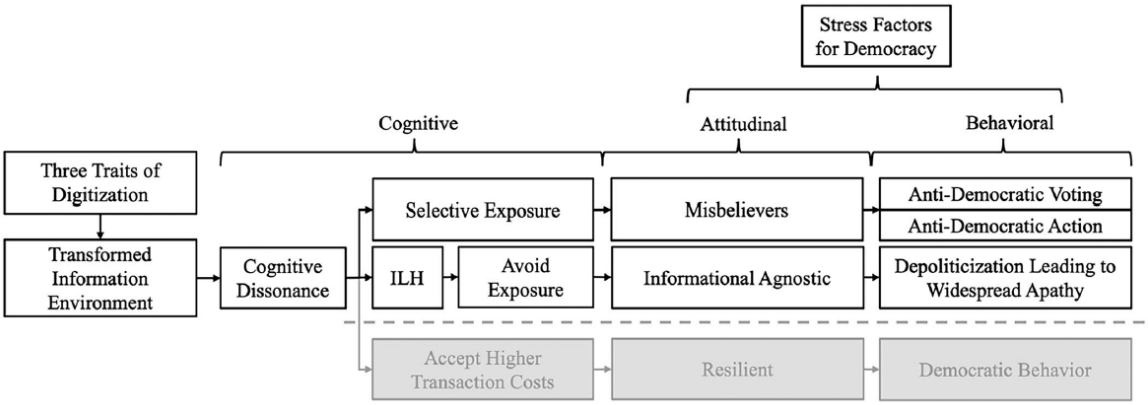
1.2.4. Information environment and democratic decay

In Chapter 5, a second collaborative article focuses on the effects of advancing digitization on societies in democratic contexts, and how the transformation of information environments can spur democratic decay. Digitization primarily affects societies by transforming the information environment, i.e., how information is produced, disseminated, consumed, and regulated. As presented in Chapter 2, digital technologies are

embedded in a myriad of political economic dynamics, both as products and services, but also as infrastructures for new business models and ways of revenue generation. This causes distinct changes to the information environment, and how malevolent actors can take advantage of it.

Primarily, these changes are attributable to (a) a flood of, also contradicting, information, (b) exacerbated challenges in information verification, and (c) artificial intelligence-assisted content personalization (cf. Maati et al. 2023, 3; see also Figure 4). In this transformed information environment, cognitive dissonance and heightened transaction costs expose societies to greater risks of falling prey to disinformation or informational agnosticism. These theoretical propositions are subsequently illustrated by plausibility probes, at the hand of the United States of America and Germany. In these two cases, varying degrees of democratic decay can partly be attributed to different regulatory and institutional frameworks of the information environment. These, in turn, mitigate the effects of digitally transformed information environments and how they translate into democratic decay.

Figure 4 Causal link between digitization and democratic decay (source: Maati et al. 2023, 8)



The main contributions of this article are twofold. For one, it provides the theoretical link between digital technologies, their transformative effects on information environments, and how they may translate into political behavior that is detrimental to democracies. Another important achievement is the development and integration of the concept of informational agnostics, i.e., individuals overwhelmed with contradicting information, ultimately resulting in depoliticization and apathy over their inability to take positions. This can translate into democratic decay by subverting societal foundations of healthy democracies that necessitate informed and engaged citizens (cf. Dahl 1982, 10–11; 1989, 108–14) through apathy or outright anti-democratic behavior. Consequently, democracy in the twenty-first century is then not only endangered

by anti-democratic mobilization of citizens based on misinformation and conspiracy narratives; it is also threatened by a potentially growing, yet understudied group – the informational agnostics.

1.3. The core contributions

As laid out in this thesis, information, and therefore digital information and communication technologies, inevitably affect how power can be accessed, contested, and exercised in the age of digital information. This work therefore provides a valuable contribution to the study of comparative political science in the twenty-first century with a particular focus on regime-type research. The different chapters present comprehensive studies of the digitally induced transformations of politics and political systems by focusing on regime dynamics and the political economic embeddedness of digital technologies, and their technical characteristics: (I) they provide theoretical frameworks on how to study the changes caused by technological innovations in democracies, as well as autocracies; (II) they highlight the importance of incorporating a political economic perspective and the role of companies into the analysis of technologically-induced changes of politics and political systems; (III) they substantiate these theoretical claims with various empirical analyzes using different methodologies, from anecdotal evidence and comparative plausibility probes to cross-sectional data-analyzes, and analyzing novel empirics. And lastly, (IV) this thesis reveals new puzzles for future research, as discussed in the conclusions: The findings highlight how the political economy of digital technologies reproduces existing dependencies that warrant a more critical consideration in future analysis of the transformative impacts of digital innovations. The thesis also sheds new light on the necessity to emphasize the analysis of information environments and how they are regulated when distinguishing democracies form autocracies in the twenty-first century. And, as presented in Chapter 6, the discussion of the main findings identifies three key areas that are in dire need for reforms if democracy is to prevail in the decades to come.

2. The digital blender: conceptualizing the political economic nexus of digital technologies and authoritarian practices

Published in: *Globalizations*, online, p. 1 – 18; 11 Oct 2022; doi.org/10.1080/14747731.2022.2131235

Abstract

This article develops the concept of the digital blender to comprehensively address the extent to which digital technologies further authoritarian practices and power beyond the state. By focusing on the primarily commercial nature of digital technologies, and their reciprocal transformational political economic embeddedness, the digital blender allows to highlight the role of private companies in enabling practices that are detrimental to democratic values and processes, irrespective of the formal regime-type context of a given polity, and less confined by national borders. While previous discussions primarily focus on digital technologies as mere tools at the discretion of their master, this relational perspective allows for the incorporation of transnational non-state actors and dynamics in constituting and contesting manifestations of authoritarian power beyond the state. These dynamics will be illustrated and discussed in light of insights into recent incidents involving companies such as Cambridge Analytica, Meta Platforms Inc., and the NSO Group.

2.1. Introduction

To what extent do digital technologies further authoritarian practices and power? [3] Initial research on the pro-democratic effects of digital technologies (cf. Diamond and Plattner 2012) has become outnumbered by accounts that engage with the Janus-faced nature of these technologies (cf. Diamond 2019; Kendall-Taylor, Frantz, and Wright 2020; Keremoğlu and Weidmann 2020; Rød and Weidmann 2015). New digital ways to surveil (Farries 2019; Feldstein 2019a), repress (Feldstein 2019b; Tsourapas 2020; Xu 2020), legitimize authoritarian regimes (Gunitsky 2015), manipulate information, and exert social control (Guriev and Treisman 2019; Jones 2013; 2019; 2022)(Guriev and Treisman 2019; Jones 2013, 2019, 2022) are now available to autocrats. More recently, however, attention is shifting towards trends of convergence in digital coercive practices between democratic and autocratic actors (Gunitsky 2020).[4]

These developments raise doubts about the suitability of classical analytical regime-type dichotomies in analyzing digitally enabled authoritarian practices and cross-regime convergences (cf. also Michaelsen and Glasius 2018), and in understanding authoritarian power, understood as the cumulation of coercive practices and capacities that undermine accountability (cf. Glasius 2018c, 517; Jenss and Schuetze 2021, 83). Together with an increase in digitally enabled transnational political interferences by state and non-state actors (Boehnke and Zensus 2022), reconsiderations of conceptual and spatial imaginaries of authoritarian power, and its articulation become more pressing.[5] Central to this development are digital

[3] Here, digital technologies are treated as an overall category. They entail any services or devices that produce, process or store digitized information via the use of processing units. The term is treated synonymously with information technologies (ITs) and includes personal computers, smart devices, as well audio-visual recording devices, but also programs, algorithms, as well as the internet, and social media. Information and communication technologies (ICTs) refer to digitally enabled communication. Smart devices in turn are devices that are connected to other digital devices, networks, or processing units via the use of connection systems such as an internet connection, Bluetooth, or other wireless forms of data transmission (Silverio-Fernández, Renukappa, and Suresh 2018).

[4] Illustrative in this regard is the 2013 NSA scandal, where whistleblower Edward Snowden revealed the US agency's extensive and illicit global digital surveillance program that targeted people in the US and abroad.

[5] E.g., the recurring digital electoral manipulation by Russian online trolls in various countries to undermine the integrity of democratic institutions and public trust (Perlroth, Wines, and Rosenberg 2017; Švedkauskas, Sirikupt, and Salzer 2020; Tennis 2020).

technologies and private tech companies. By commodifying data and digital tools that enable and incentivize state – and non-state actors to resort to coercive practices such as surveillance and electoral manipulation (cf. Aho and Duffield 2020; Deibert 2019; Shahbaz and Funk 2019), tech-capital is simultaneously reinforcing the proliferation of the required digital infrastructures through which these practices can be employed, and authoritarian power can manifest (cf. Couldry and Mejias 2019; Zuboff 2019).[6] Ultimately, this renders digital technologies and tech companies to be central factors in constituting authoritarian power and transforming the notion of its spatiality: from being mostly articulated by state-actors within a given territory, authoritarian power is now more deeply embedded into the dynamics of capital accumulation and is shaped by state- and non-state actors alike, irrespective of geographic boundaries (cf. Glasius 2018b). Furthermore, via the commodification of human experiences in the form of behavioral data (cf. Zuboff 2019) and advancing digital consumerism, individuals subject themselves to be more vulnerable to such coercive practices in a rather consensual, yet uninformed manner which renders surveillance and manipulation to be more obfuscated and thus more vicious and effective (cf. Bakir 2020).

Yet, these considerations are still to be incorporated into the study on authoritarian practices and digital innovations due to the drawbacks of a prevailing functionalist understanding of digital technologies. Digital technologies have primarily been understood as tools that are at the discretion of their master – typically state actors – to serve either democratic or autocratic purposes within a nationally confined context. However, this yields at least three shortcomings:

First, such a functionalist perspective neglects the commercial and transformational nature of digital technologies which are reciprocally embedded in distinct political and economic relations. These include tech companies, new forms of capital accumulation, and capital interests that co-determine the development and usage of digital technologies.

Second, functionalism fails to consider how digital political and economic dynamics transcend conceptual and national borders. Analyzing digital phenomena under methodological nationalism, and along classical regime-type dichotomies, neglects spatial and political-economic transformations. These are in turn

[6] "[I]nfrastructures are critical locations through which sociality, governance and politics, accumulation and dispossession, and institutions and aspirations are formed, reformed, and performed" (Anand, Gupta, and Appel 2018, 2).

induced by digital technologies that go beyond individual political systems and hold important implications for imaginaries of authoritarian power.

Consequently, and third, a functionalist perspective is ill-equipped to assess how authoritarian power is also constituted by international private companies and digital technology. While functionalism might be suitable to explain strategies or motives of the usage of digital technologies, it does not help in analyzing the effects of transnationally operating nonstate actors, incentive structures, and dynamics of capital accumulation on the externalization and decentralization of authoritarian power.

Therefore, to facilitate a better understanding of the political-economic nexus between digital technologies and authoritarian practices, and their effects on authoritarian power, this article develops the idea of the digital blender: a multilayered relational theoretical perspective on digitalization that relates characteristics and dynamics of (1) the technical, (2) the commercial, and (3) political economic level of digital technologies with one another. Analyzing the business practices of three tech companies under this analytical perspective suggests that tech companies and digital technologies are co-constitutive of authoritarian power:[7] (a) by enabling and tolerating authoritarian and illiberal practices as an externality to their core business operations; and (b) by offering such practices as commodities in exchange for payment, rendering them pivotal to their business strategy. This paper concludes with a discussion of how tech companies and digital technologies become central to manifestations of authoritarian power via digital infrastructures beyond the state and its spatial imaginaries.

2.2. The digital blender in a nutshell

The replacement of analogue technologies with digital ones (i.e., digitization) has amounted to fundamental transformations of human interactions that collectively constitute the analytically rather awkward phenomenon of digitalization (Bloomberg 2018; Gupta 2020; Legner et al. 2017). The digital blender is

[7] Meta Platforms Inc. (or Meta), Cambridge Analytica, and NSO Group (or NSO) – all of which have received heightened media attention over the past years due to international networks of investigative journalists and internal documents being leaked to the public.

therefore a theoretical lens that focuses on the nuanced interrelation of digital technologies' multi-layered political and economic dimensions and the implications of digital infrastructures.

On its first level, the digital blender considers the technical characteristics of digital technologies. By enhancing computing capacities, they transform data availability and processability ('information blending'). Likewise, they transform spatiality by compressing physical proximity through the augmentation of existing spaces and the creation of new virtual spaces, ultimately transcending national borders or regimes ('spatial blending'). On the second level, the digital blender relates the technical dynamics of blending to the dual role of digital technologies as commercial products and factors of transformation. For tech companies, this enhances (a) the scope of commodification and (b) market expansion which jointly facilitates new business models. Lastly, the digital blender contextualizes these technical and commercial dynamics in the larger global political-economic context of authoritarian neoliberalism. In this environment, capital interests and indicators of neoliberal economic performance, are prioritized by state actors and transnational companies over other considerations and are increasingly insulated from democratic contestation (cf. Bruff 2014; Bruff and Tansel 2019; Tansel 2017).

Concordantly, transnational virtual spaces and global tech markets are extremely challenging to be effectively regulated, especially since most digital innovations can be used for civilian and autocratic purposes.[8] As tech companies seek to maximize profits, like any other company, and since countries have a national interest in fostering their domestic tech industry, enterprises in the digital sector are encouraged to exploit the full potential of these new technology markets. This entails expanding digital infrastructures to develop new markets, as well as (a) the provision of goods and services irrespective of their negative social and political externalities, including the enabling of practices that are detrimental to democratic processes and institutions, as well as (b) the commodification of anti-democratic practices as services and products. Ultimately, this renders digital technologies and tech companies co-constitutive of notions of authoritarian power beyond the state.

[8] For example, algorithms designed to recognize patterns in large-n data can be used for face-recognition surveillance technology, but also cancer research (Steele et al. 2022). This utility for autocratic and civilian purposes alike constitutes a feature of digital dual use inherent to most digital technologies.

2.3. Developing a relational perspective on digital technologies

An increasing number of politicians, irrespective of regime contexts, capitalize on digitally enabled misinformation campaigns and manipulation of public discourses (Bradshaw and Howard 2017). This includes mounting instances of external digital interferences in elections (Boehnke and Zensus 2022); as well as striking similarities of justifications for expanding digital surveillance during the Covid pandemic in democracies and autocracies alike (Maati and Švedkauskas 2020). These trends have been framed as "digital authoritarianism come[ing] to democracies", in the form of "a convergence in how democratic and autocratic governments are using surveillance and disinformation to shape political life" (Gunitsky 2020).

This development necessitates going beyond a limiting regime-centred understanding of authoritarianism that is confined by the nation-state. Instead, one should analyze factors that constitute this form of authoritarian power which seems to be enabled by digital technologies and perpetrated by non-state actors irrespective of their geographic location.[9] To move beyond classical analytical regime categories, Michaelsen and Glasius study digitally enabled practices that either "sabotage accountability and thereby threaten democratic processes" (i.e., "authoritarian practices"), or that "infringe on the autonomy and dignity of the person" (i.e., "illiberal practices") (Michaelsen and Glasius 2018, 3789).[10] This approach allows for a holistic engagement with converging non-democratic practices under consideration of the role of digital technologies and non-state actors, such as tech companies – aspects that are systematically neglected by state-centrist approaches. Consequently, an analytical concept that focuses on the effects of digital technologies on manifestations of authoritarian power should primarily rely on a notion of practices.

[9] This does not mean that classical regime-type distinctions are obsolete; however, for these new phenomena of digitally enabled transnational authoritarian practices, new analytical approaches are required.

[10] For matters of simplicity, this article refers to coercive practices to entail both, illiberal and authoritarian ones.

2.3.1. The technical characteristics of digital technologies

Digital technologies are to be understood as commercial products, instead of being only tools, as they are primarily developed and sold by private corporations.[11] Consequently, digital innovations are subject to market dynamics and are designed to generate profits. Unlike most other products, however, technical characteristics inherent to digital technologies fundamentally transform the political economy they are embedded in by blending information and blending spatiality.

Blending information refers to the effects of digitizing information. Just as a blender turns ingredients of different textures into a homogenous mass, digitization turns information into binary and re-programmable signals that are universally machine-readable and self-referential (Yoo, Henfridsson, and Lyytinen 2010).[12] Improvements in computing capacities and the increasing interconnectedness of digital devices, enhance the cross-compatibility of digital information.[13] Consequently, information that is too complex for systematic analogue analysis, or unfeasible to collect, can nowadays be automatically collected in ways processable for a myriad of purposes.

Spatial blending refers to the transformation of spatiality. Innovations in digital technologies, especially in ICTs, create new spaces of interaction and communication, as well as new forms of digital and virtual infrastructure. For one, via two-dimensional virtual spaces of instant interaction and communication (e.g., messenger services or social media platforms). Or via three-dimensional interactive platforms that rely

[11] While pioneering research and development of the precursor of the internet as we know it was a state funded research project under the supervision of the United States Department of Defense, the development and distribution of digital technologies is nowadays a lucrative market dominated by private sector capital.

[12] I.e., turning continuously scaled analogue information into discretely scaled digital one (Bloomberg 2018; Gupta 2020; Legner et al. 2017).

[13] If one wanted to record and transcribe a conversation using analogue technologies, this data would be stored in different formats that are incompatible with one another (the spoken conversation, the recording tape, the paper with the written or printed transcript). Digital technologies and digitization allow for a cross-compatibility of data that enables automatized processing by various programs and devices. That way, a digitally recorded conversation can be automatically transcribed and simultaneously analyzed for sentiment analysis or keywords.

on virtual reality or augmented reality technology.[14] But also, through 'non-spaces' that are invisible to consumers, and which are created by the growing wireless interconnectedness of digital (smart-)devices.[15]

Collectively, these transformations compress notions of geographic proximity which renders human interaction less contingent on physical vicinity, and more on the availability of digital infrastructure. Likewise, just as these new spaces transcend geographic borders, so do power dynamics and the political-economic underpinnings of these new spaces and infrastructures. These, in turn, are created and operated by private-tech companies to generate profits and are therefore shaped by market dynamics and (tech-)capital interests. Consequently, dynamics and interactions in these new and blended spaces are directly and indirectly shaped by interests in digital capital accumulation.

2.3.2. Relating technical characteristics to commercial dynamics of capital accumulation

Blending information and spatiality impact capital-labour relations and enable new forms of capital accumulation (cf. Aho and Duffield 2020; Zuboff 2019; Deibert 2019; Fuchs 2014; Staab 2019; Starr 2019). More systematically, however, digital spatial and information blending transforms and reinforces capital accumulation by (a) expanding the scope of commodification and (b) market expansion.

Information blending drastically expands the scope of commodification by enabling new business models. Every interaction with a digital device or service that is connectable or linked to a data centre produces data that can be collected and that can provide detailed insights into personal lives. Advancing digitization of human interaction consequently provides staggering amounts of processable – and thus

[14] Virtual reality refers to the immersion into a virtual 3-D room by using audio-visual headgear, enabling virtual face-to-face interaction and communication while physically separated (e.g., VR-games, chatrooms, etc.); augmented reality refers to the use of digital technologies (smartphones, smart glasses, etc.) to integrate digital information and services into the physical world (e.g., scanning QR-codes, AR-games such as Pokémon Go, etc.).

[15] Non-spaces (cf. Messler 1986) here refer to infrastructures that are, unlike virtual chatrooms, invisible, e.g., peer-to-peer connections between devices, or in colloquial parlance spatial imaginaries such as 'data highways'.

commodifiable – data to companies (cf. Aho and Duffield 2020; Zuboff 2019; Deibert 2019).[16] This enables an emerging demand-prediction-based economic order that "[…] unilaterally claims human experience as free raw material for translation into behavioral data […]"(Zuboff 2019, 8, 495–504)(Zuboff 2019: 8, 495–504), which can then also be used for various non-commercial and political purposes.

Consequently, spatial blending allows for a significant expansion of the dynamics of capital accumulation: For one, by compressing geographic proximity via new ways of virtual instant interaction and communication, companies can nowadays operate in markets across the globe in a geographically rather unrestricted manner. Additionally, by transforming spatiality and creating new virtual spaces for communication and interaction, new markets are developed: through commodifying access to such virtual spaces. And by utilizing these virtual spaces as digital markets for "[...] deep and relentless surveillance of consumers' personal data to target advertisements [...]" (Deibert 2019, 26) or other business models based on virtual interaction or behavioral data.

2.3.3. The political embeddedness of digital technologies

Due to its profitability, tech-capital advances digital technologies and infrastructures into all spheres of life. This ultimately reinforces the reciprocal dynamics of the digital blender: information and spatial blending, enhanced commodification, and expanded marketization. However, these processes of capital accumulation do not unfold in a vacuum. Instead, digital technologies and their infrastructures are situated in a permissible political-economic context characterized by authoritarian neoliberalism, i.e., the advancing insulation of neoliberal capital accumulation processes from public contestation and democratic considerations (Bruff 2014; Bruff and Tansel 2019; Jessop 2019, 352; C. Smith 2018; Tansel 2017).

The concept of authoritarian neoliberalism focuses primarily on the conjunction of capital interests and the state as the embodiment of social relations. It highlights the imposition and entrenchment of neoliberal processes via constitutional and legal mechanisms in an authoritarian coercive manner that

[16] This includes the composition, analysis, and utilization of individual walking patterns compiled by devices with an active wireless data transmission such as Bluetooth, GPS, or internet, as well as voice- and face-recognition (Nanos 2018).

represents capital- and not labour-interests (Tansel 2017, 2–3). The state is understood as the manifestation of power-relations, not isolated from but entangled in transnational accumulation processes that are likewise shaped by capital interests This implies that processes of capital accumulation also stand about forms of authoritarian power that transcends individual national contexts, or imaginaries of the state or a regime.

In this permissible macro-political economic context that prioritizes neoliberal performance indicators, such as growth and profit, over considerations like the integrity of democratic processes and institutions, the "circuits of capital accumulation" are increasingly protected by the means of "coercive, rather than consensual capacities" (Tansel 2018, 199). Likewise, as digital infrastructures become a central element of these circuits of capital accumulation, their profitability and commercial potential are prioritized over related negative externalities. This renders authoritarian and illiberal practices inherently compatible with neoliberal forms of capital accumulation (Bruff 2014, 124; Tansel 2017, 2–3). As the new forms of capital accumulation enabled by digital technologies unfold in a such context where capital interests and profit-generation reign supreme, tech companies are also incentivized to fully exploit the commercial potential of 'the digital', irrespective of social or political externalities, also in the form of anti-democratic practices.

2.4. Authoritarian and illiberal practices beyond the state

Recent leaks of internal documents of the following tech companies allow an analysis of their business practices from the perspective of the digital blender regarding their agency in constituting authoritarian power. As seen under the lens of the digital blender, the interrelation of tech-capital interests, characteristics of digital technologies, and the centrality of digital infrastructures to processes of capital accumulation renders the agency of tech companies central in constituting authoritarian power beyond the state. Symbiotically embedded in the permissible context of authoritarian neoliberalism, tech companies are also incentivized to offer products and services that (a) produce externalities that are detrimental to core-democratic principles, or that in themselves are (b) commodified illiberal and authoritarian practices. Due to lacking regulatory frameworks and capacities, and an overriding profit paradigm, these companies can readily accept the negative outcomes of their business models and socialize undesired effects as externalities on affected societies. These outcomes include the spread of unconstitutional surveillance and violations of

privacy, the manipulation of elections and political discourses via social media algorithms and deep fakes, as well as polarization and the subversion of mutual recognition as legitimate political opponents.

2.4.1. Meta platforms inc. – providing virtual spaces and digital infrastructure for coercive practices

In October 2021, former Meta manager Frances Haugen disclosed a comprehensive collection of internal documents to the United States Securities and Exchange Commission (B. Smith 2021; WSJ Staff 2021). The leaked files consisted of email conversations and classified internal reports of the company. It substantiated claims regarding Facebook's detrimental effects on mental health and politics, and the company's awareness thereof (WSJ Staff 2021). It also documented how Facebook managers, to not scrutinize profits, tolerated systematic misinformation campaigns, demagoguery with lethal consequences, and overall negative effects on public discourses (Facebook 2019b; Pierce and Kramer 2021; B. Smith 2021).

On the technical level, Meta's business model relies on blending information and blending spatiality. By transforming spatiality, the company provides new virtual platforms and the infrastructure for digital interaction and communication that encompass individuals from numerous countries and communities. Meta's digital infrastructure encompasses a significant portion of the world's population of around 8 billion people, amounting to 2.9 billion Facebook users, 1.28 billion Instagram users, and over 2 billion WhatsApp users (Data Reportal 2022; Statista 2022; Think Impact 2021). These platforms of interaction are commodified as new markets for the advertisement industry by using virtual spaces to place advertisements. In 2020, the advertisement business made up 98 percent of the company's total revenue (U.S. Securities and Exchange Commission 2021).

To increase its attractiveness as an advertisement platform, the company exploits the full potential of information blending by collecting and analyzing all available user data for targeted individualized ad campaigns. This includes the collection of data consensually revealed by users on the company's social media platforms, but also information collected from digital devices on which the respective applications are operated.

Consequently, Meta's attractiveness as ad space to potential clients is determined by (a) the traffic on its services;[17] and (b) the precision of the platforms' advertisement services in targeting the demographic desired by its clients. These factors are contingent on the amount and quality of user data collected and analyzed by the platform which incentivizes Meta to (1) increase traffic and (2) increase the of and precision of information collected and analyzed (cf. Deibert 2019; Pereira 2020; Zuboff 2019).

In the context of authoritarian neoliberalism, Meta's business model, together with its infrastructure of transnational virtual platforms and services, could long unfold without any meaningful regulations. The extent and depth of data collection, as well as accountability and responsibility to prevent negative externalities, were of neglectable interest. Only recently, following the leak of internal documents, have these aspects received greater attention from the public. The leaked files document how Meta could pursue business practices and profit maximization without taking any real responsibility for severe negative externalities in the form of demagoguery, abuse, harassment, mental stress, and misinformation.

One instance is the greater leeway for politicians and public figures to violate Meta's terms of service. As their online followings generate greater traffic and profit, Facebook and Instagram rather tolerate rule violations of these profiles than lose them. This however creates the externality, that these profiles can share misinformation, as well as violent and hateful content without any consequences, harassing individual people or groups, which poisons and polarizes political discourse (Horwitz 2021).

Another instance is the 2018 update of the Facebook algorithm. To reverse downward trends in traffic, Meta reconfigured how the platform assesses the value of digital content, which is determined by its likelihood to spark user interaction. More valuable content is then disseminated to a wider audience. Greater value was attributed to content with longer comments, interactions with Facebook's 'reaction'-feature (including emojis that resemble 'care', 'love', 'sadness', 'laughing', and 'anger'), as well as with interactions between groups with different socio-economic and political backgrounds. Ultimately, however, this resulted in greater dissemination of sensational, divisive, controversial, hateful, and polarizing content, as well as misinformation (Hagey and Horwitz 2021).

[17] I.e., the number of users interacting with one another and with contents on a website, as well as the intensity and duration of this interaction.

According to internal documents, this contributed to the undermining of global vaccination efforts in the face of the SARS-CoV-2 pandemic by promoting conspiracy beliefs and misinformation narratives (Schechner, Horwitz, and Glazer 2021). Likewise, in the United States, similar misinformation and conspiracy narratives fueled extremist groups in the run-up to the riots on Capitol Hill on January 6th (Timberg, Dwoskin, and Albergotti 2021). In India, the algorithm and Meta's ad services promoted demagoguery by politicians and extremist groups which came to be linked to deadly riots targeting Muslim minorities (Purnell and Horwitz 2021); similar content was targeted against Rohingyas in the wake of the genocide in Myanmar (Stevenson 2018). As documented by the leaked files, Meta was not only aware of these problems but did not attribute great attention to preventing these externalities in the form of illiberal and authoritarian practices, as this would jeopardize their business model and, ultimately, profit, as was the case in India (Purnell and Horwitz 2021).

Interestingly, however, Meta's tolerance of such externalities is partly contingent also on whether affected societies are located in countries of the Global South (e.g., Mexico, Myanmar, India), where deadly riots remained largely without consequences for the company; or whether they are located in the Global North (e.g. US, EU), where such practices are subject to more scrutiny by the public and the company itself. Nonetheless, Meta Platforms Inc. provides the virtual infrastructure and spaces for authoritarian power to manifest, exerted by state- and non-state actors, and territorially unbound through processes of spatial blending. Likewise, Meta is reluctant to fundamentally adjust the way its infrastructure and spaces function to not scrutinize profits, rendering it to be an exemplary element of the circuits of capital accumulation that are willfully compatible with coercive practices.

2.4.2. Cambridge Analytica – transnational commodification of electoral manipulation

Leaks of internal documents from 2018 onwards by former employees Cristopher Whiley and Brittany Kaiser, detailed, how Cambridge Analytica illicitly obtained the private data of more than 80 million Facebook users (Barry 2018; Cadwalladr 2020; Rosenberg 2018). This data was then used to compile millions of socio-psychological profiles for targeted political advertisement for Donald J. Trump's 2016 US election campaign which enabled tailored advertisement via social media that explicitly exploited individual fears and preferences (Collins and Dance 2018, 201; Confessore 2018; Merrill and Goldhill 2020; Salinas 2018, 201).

This digitally enabled manipulation of public discourse has been assessed to be decisive in the 2016 elections, according to whistleblower Christopher Wiley, as well as by former digital director of Donald J. Trump, Brad Parscale (Barry 2018; Beckett 2017).

At its core, again, the digital blending of information and spatiality provides the foundation of Cambridge Analytica's business model: information blending enabled by services such as Facebook allows for detailed insights into the lives of individuals. Spatial blending, in turn, renders the target group's proximity irrelevant, as these practices manifest via the digital infrastructure provided by companies such as Meta. While Cambridge Analytica did not engage in the primary raw material collection, it does tab into the – illicit and licit – availability of these collected data archives. The Facebook dataset was acquired under a false pretense, but documents released by Brittany Kaiser imply that Cambridge Analytica's involvement in at least 67 other countries relied on additional data that go beyond the Facebook data trove (Cadwalladr 2020). Only through the aspects of blending information could the company engage in behavioral analysis to approximate individual psycho-sociological profiles that were then used during elections to fine-tune advertisement and misinformation to influence electoral outcomes. The virtual, and territorially unbound manifestations of these practices were, in turn, contingent on digital infrastructures provided by Meta's services.

Whereas Meta tolerated anti-democratic practices on its virtual platforms as an externality to profit-maximization, the case of Cambridge Analytica involves a company whose service consists of commodified anti-democratic practices, i.e., electoral manipulation. Downplaying this as an instant of regular market research, strategic communication, and political campaigning would neglect the far-reaching implications of the leaked internal documents provided by Wiley and Kaiser: companies like Cambridge Analytica use digital infrastructures to offer highly potent services to manipulate electoral outcomes indiscriminately of their customers' agenda or the political consequences with regards to core-democratic values, or the validity of the content advertised (Cambridge Analytica 2020a; 2020b). While the motivation of clients certainly impacts the way the company's services are used, Cambridge Analytica's exploitation of personal data to finetune misinformation renders it rather a collaborator, than a negligent facilitator of coercion.

The provision of such services by a private company on a transnational scale is only possible in a permissible global economic context that enables the commodification of coercive practices and safeguards the digital infrastructure through which they can manifest. Neither are potential clients required to be

citizens of the targeted polity nor do they need to hold any formal position. The contractually relevant factors are solely determined by the dynamics of an unregulated global market of digital electoral manipulation, client-solvency, and capital accumulation. The non-transparent and subliminal nature of services, as offered by companies such as Cambridge Analytica, and the oblivious consensual interaction of users with such services, allow the use of personal data for targeted campaigns of misinformation, fake news, and slander without tying it directly to the service provider or its client (cf. Bakir 2020). Here, the conjunction of (a) digital business models that operate under the supreme logic of total commodification and market expansion, and (b) authoritarian practices enabled by the digital blending of information and spatiality, renders electoral processes even more vulnerable to manipulation.

2.4.3. NSP group – Interlocking state and capital interests via commodified coercive practices

In 2016, renowned UAE-based human rights activist Ahmed Mansoor was targeted by a spyware called Pegasus, developed, and sold by the Israel-based private intelligence company NSO Group (or NSO). Pegasus allows its operator to secretly infiltrate a targeted device and use its full functions without the victim's notice, effectively rendering the device into an omnipotent surveillance tool. Further, the operator can add, manipulate, or delete information on the device, and even incapacitate it (Gurijala 2021; Levenson 2022; Marczak and Scott-Railton 2016; Rueckert 2021).

Officially, NSO's sales are contingent on the approval of the Israeli government and its product is only to vetted governments and state agencies. Subsequent investigations of the Citizen's Lab at the University of Toronto, however, uncovered the spyware's full potential and its widespread use also among countries with dubious human rights track records (Marczak and Scott-Railton 2016). Clients of NSO include "[...] Azerbaijan, Bahrain, Hungary, India, Kazakhstan, Mexico, Morocco, Rwanda, [...], Togo, and the United Arab Emirates (UAE)" (Amnesty International 2021), but also exemplary democracies such as the United States or Germany (Deutsche Welle 2021).

Consequently, individuals across the globe have been infected by NSO's spyware (Priest, Timberg, and Mekhennet 2021), such as business executives, human rights activists, over 180 Journalists, "[...] and more than 600 politicians and government officials – including cabinet ministers, diplomats, and military

and security officers, as well as 10 prime ministers, three presidents and one king" (Washington Post 2021). In Israel, it has been used domestically by the police to target numerous citizens without a warrant, including CEOs, politicians, and activists (Benjakob 2022; Benjakob and Breiner 2022; Kingsley and Bergman 2022). In Hungary, Orbán's regime targeted several opposition politicians and journalists (Benjakob 2022; Walker 2021). Saudi Arabia relied on this spyware before the assassination of Jamal Khashoggi, targeting him as well as his wife, friends, and close associates (BBC 2021a; Travère 2021).

NSO's business model crucially depends on the dynamics captured by the digital blender. Pegasus's potency is due to its full exploitation of a smartphone's capacity to blend information: collecting and digitizing analogue information through audio(-visual) recordings, monitoring movements via digital GPS signals, as well as any transaction or interaction done via the device. That way, it subjects its targets to the invisible digital infrastructure of surveillance without their knowledge and fully exploits the potential of spatial blending: by relying on the digital transformation of spatiality which contracts notions of proximity, rendering geographic location irrelevant for digital surveillance of an individual; and by blending 'the physical' with 'the digital', as the spyware does not only monitor interaction and transaction of the victim via the infected device but also renders every interaction in the physical world near the infected device to be subject of information blending. This means, it also subjects nearby Individuals that are not Its primary targets to authoritarian power manifested in the form of surveillance via the digital infrastructure.

Providing access to this powerful tool is a lucrative service that is only made possible by the relational dynamics of digital technologies captured by the digital blender and the permissible political economic context of authoritarian neoliberalism. Just as Cambridge Analytica's core services are fundamentally anti-democratic, NSO's core service is the manifestation of a coercive practice that enables the encroachment on civil rights. However, unlike Cambridge Analytica, NSO's status as a private company comes closer to one of the arms industries, as its sales are contingent on the Israeli government's approval. Yet, the government's oversight has not prevented the use of this spyware for illiberal and authoritarian practices. Instead, the Israeli government has frequently levered its control over the company's sales as an informal extension of its foreign policy agenda (Bergman and Mazzetti 2022a; 2022b; Levenson 2022).

This illustrates the complex and multilayered transnational interrelation of tech-capital, coercive practices, and authoritarian neoliberalism that helps to grasp the variegated manifestation of authoritarian power beyond the state: Following the authoritarian neoliberal dogmatism, NSO seeks to increase its profits

and to grow at all costs, even if that means commodifying authoritarian and illiberal practices; likewise, the Israel government has an interest in sustaining the company's growth as it belongs to its domestic tech-industry– albeit with strategic foreign policy concerns irrespective of resulting coercive practices of NSO's clients. Ultimately, however, instrumentalizing commodified anti-democratic practices as a foreign policy strategy, and providing regimes such as Saudi Arabia, Morocco, or Hungary with powerful spyware, renders the democratic government of Israel, but also NSO to be co-constitutive of authoritarian power beyond a single nation-state: (a) as the spatial blending of spyware such as Pegasus (re)subjects victims to authoritarian power, even in exile, transcending the reach of coercive practices beyond national borders; (b) as the authoritarian capacities of state actors in one country are co-facilitated and expanded by the approval of a formally democratic government of another country, as well as through a private tech-company that solely operates along a profit-paradigm. That way, as states are understood as the manifestation of a myriad of globalized socio-economic, cultural, and political relations (cf. Bogaert 2018), state actors themselves are drawn into globalized configurations of authoritarian power.

2.5. Conclusions

The relational analytical perspective of the digital blender helps to capture the transnational political-economic interrelations of tech-capital, authoritarian neoliberalism, and authoritarian power. Tech companies, driven by a dogmatic profit paradigm, exploit the characteristics of digital technologies and the digital infrastructure to enable and commodify manifestations of authoritarian power in the form of coercive practices. The theoretical interrelation of the multilayered dynamics of digital capital accumulation demonstrates how tech companies and their business models are central in (a) providing digital and virtual infrastructures, and (b) exploiting these infrastructures to provide commodified coercive practices. Consequently, this also holds implications with regards to potential classifications of different types of tech companies, their relation to coercive practices, but also regarding manifestations and imaginaries of authoritarian power and its contestation.

2.5.1. A proto-typology of tech companies

Companies such as Meta, constitute silent facilitators that provide digital and virtual infrastructures of transnational reach through which coercive practices can manifest. Social media business models create new spaces for interaction, data commodification, and the development of new advertisement services. Thus, they have a distinct interest in expanding digital and virtual infrastructures to attract and bind growing numbers of users. Lacking regulations enable the resort to algorithms and mechanisms that increase traffic, irrespective of negative externalities and their adverse effects on accountability, as well as on civil rights and liberties. Consequently, third parties can exploit these mechanisms for coercive purposes: to subvert democratic institutions, spread polarizing misinformation, and incite lethal ethno-religious hatred. Due to the embeddedness of processes of capital accumulation characterized by authoritarian neoliberalism, companies such as Meta tolerate such practices not to jeopardize revenue.

The second cluster of companies is that of active perpetrators. Companies such as Cambridge Analytica or NSO Group rely on these digital and virtual infrastructures and their embeddedness in processes of capital accumulation which are underpinned by authoritarian neoliberalism. These infrastructures, and their underlying political-economic dynamics, allow them to commodify products that consist of coercive practices, and to provide them to state- and non-state actors alike. However, whereas Cambridge Analytica might be labelled as an autonomous active perpetrator, NSO Group's dependence on the Israeli state renders it a semi-autonomous active perpetrator: the actions of autonomous active perpetrators are mostly determined by market forces and capital interest; the agency of semi-autonomous perpetrators is co-determined by third-party interests.

2.5.2. Imaginaries and manifestations of authoritarian power and its contestation

Tech companies play a central role in the manifestation of authoritarian power via the provision of digital and virtual infrastructures and the provision of digitally enabled coercive practices. In both instances, tech companies rely on digital technologies and services that, as products, are targeted at consumers who become obliviously subjected to these underlying processes of capital accumulation and surveillance capitalism. However, while most users subject themselves obliviously (yet consensually), choices to resist the advancing digitization look rather bleak – even more so following the global SARS-CoV-2 pandemic and its catalysing

effect on digitalization. Avoiding subjection to digital dynamics would imply a complete withdrawal from the digital, severely limiting participation in numerous social, cultural, economic, and even political aspects of everyday life.[18] Paradoxically, 'the consensual' and 'the coercive' are territorially unbound and interrelated, as both are embedded in transnational infrastructures of digital capital accumulation, commodification, and consumerism.

Consequently, the cumulation of digitally enabled coercive practices amounts to a manifestation of authoritarian power that is territorially unbound (cf. Glasius 2018b) and co-constituted by state- and non-state actors such as tech companies. Likewise, and following the relational theoretic approach of the digital blender, spatial imaginaries of authoritarian power need to be rethought: In the twenty-first century, authoritarian power is no longer solely constituted by authoritarian regimes that are bound to an agglomeration of state institutions and wielded predominately within a geographically bound territory by state- and non-state actors. Instead, the externalization and internationalization of digitally coercive practices via the advancement of digital infrastructures through which authoritarian power can manifest demands to reconsider the spatial imaginaries associated with authoritarian power to be closely associated with global modes of capital accumulation and complex interrelations between capital and state interests, irrespective of formal classical regime-type dichotomies.

Likewise, the theoretical lens of the digital blender also grants insights into new forms and actors in contesting these spatially unbound forms of authoritarian power. For one, insiders took a central role in leaking classified internal documents to the public that granted insight into the inner logic of their business operations. This information was then analyzed, contextualized, and communicated to the public by international investigative networks, journalists, academics, and activists, who ironically also rely on digitally reduced spatial proximity in their collaboration. In all cases, insiders and networks have played a crucial role in informing the public about coercive effects and increasing the pressure on companies: Meta CEO Marc Zuckerberg had to testify before congress, Cambridge Analytica went bankrupt after the revelations, and

[18] While there are ways to obfuscate one's identity and protect certain personal information, for example via the use of virtual private networks (VPN) or TOR-browsers, progressing digitalization not only entails the gathering of personal data while surfing, but virtually services that are connected to data centres, including payment services (i.e., debit card, credit card), modern cars, and digital public surveillance cameras.

NSO Group was blacklisted by several countries including the United States. While this does not mean, that structural changes are underway, the agency of tech companies is contested concerning anti-democratic practices. Ultimately, state actors seek to curtail the infringements of private capital on their monopoly of coercion: In 2013, President Erdogan's amendments to Law No. 7253 now require social media companies to appoint a national representative as a liable point contact person for authorities, expanding regime control over the digital sphere (Coskun 2021). Similarly, China's doctrine of internet sovereignty effectively prevents any autonomous utilization of digital blending processes outside the state's control. The digital infrastructure has become a central pillar of Xi Jinping's regime and the state's coercive capacity (Qiang 2019).

2.5.3. Limits of the digital blender and ways forward

While it does provide fresh analytical perspectives on the interrelation of authoritarian power and digital technologies, the digital blender has its limits. Cases like China, where the state has monopolized the entire (digital) political economy require some further theoretical reconsiderations of how these phenomena fit with the digital blender. Getting a better understanding of how processes of spatial and information blending might unfold in regionally varying political and economic contexts demands further comparative analysis. Likewise, this article only provides a snapshot of how three digital tech companies have digitally enabled or perpetrated coercive practices. More systematic research into different digital business models and the articulation of authoritarian power is necessary to get a better understanding of the conjunction of tech capital and the convergence of autocratic practices across countries.

And as public awareness has increased regarding the involvement of private tech companies in facilitating and perpetrating manipulation, surveillance, and repression, reforms to regulate data protection and the digital sector are underway in different countries, and Europe (Bentzen and Krause 2021; European Commission 2022). Yet, it remains to be seen, whether these reforms will also help to move towards a more coherent regulatory framework that counters authoritarian power that transcends the state, or whether tech capital will further be able to capitalize on digitally enabled authoritarian and illiberal practices.

3. Shopping with Orwell: procurement patterns of commercialized surveillance software

Submitted to American Political Science Review

Abstract

This article analyzes determinants of public surveillance software acquisition, and tests substitution effects between limited state resources to develop own software and alternatives from the private sector. From 2010 to 2022, several cross-sectional analyzes find qualified support for substitution effects and structural requirements for public surveillance acquisitions. Regime traits merely play a marginal role. The strongest acquisition-predictor is digital repression capacity, which emerges as intervening variable for structural determinants. These findings are discussed concerning (a) their implications for the reproduction of political economic structures of dependence, and (b) their meaning for the wider research on regime-types in the digital age: Structural factors do not directly impair the pursuit of governments to possess powerful surveillance technologies, and insufficient regulatory frameworks allow private sector companies to indiscriminately provide these instruments also to autocracies. In a context of global democratic backsliding, these are developments that warrant closer observation and critical reflection.

Keywords: Digital Technology, Authoritarianism, Democracy, Surveillance, Political Economy.

3.1. Introduction

What determines public procurement of digital surveillance technologies from private sector providers? [19] Government of all traits have recognized the potential of surveillance technologies, albeit for different purposes: in autocracies like Russia and China, they have become central to ruling strategies (Dixon 2021; Qiang 2019); in democracies such as Great Britain, they have become integral elements of the national security strategy (Clarke 2024; Kayali 2023). Private companies have recognized this growing market and cater to their global clients with mercenary surveillance software (or MSS) (Feldstein and Kot 2023a).[20] These MSS have been linked to countless human rights violations - in autocrats, but also in democracies (Amnesty International 2021; BBC 2021; Kość 2022; Scott-Railton et al. 2022). The dual-use nature of MSS as protective *and* repressive tool, and their ready availability, consequently necessitate to (a) expand our understanding of the global state-business relations of the commercial surveillance industry; and to (b) enhance our knowledge on the patterns of acquisition; to be able (c) to device more effective international regulatory frameworks of these technologies and the industries that sell them (cf. Feldstein and Kot 2023a). Analyzing the determinants and patterns of MSS procurements by governments is therefore a direly needed first step into this direction.

Not all regimes possess the technical and financial capacities to develop their own digital surveillance systems (Palmer 2024). Surveillance software provided by private sector companies might therefore appear as cost-efficient alternatives. However, integrating a foreign commercial entity into strategies of national security or autocratic power maintenance creates potential vulnerabilities. These

[19] Digital surveillance entails the use of digital technologies in the "[…] gathering of information through the identification, tracking, monitoring, and analysis of individuals, data, organizations, or systems" (Feldstein 2021, 25 & 27).

[20] To date, and to the author's best knowledge, there is no single and established formal definition of the concept of 'mercenary spyware' despite its frequent use. Therefore, mercenary surveillance software is understood as intrusive software, developed, and commercialized by private sector companies to generate profit, and to facilitate access to restricted information or private communication, usually by infecting terminal user devices. Subcategories entail spywares that provide covert access and control over the device, and over its data and functions without their owners' knowledge (Brunsdon 2023; Feldstein and Kot 2023a); and digital forensics that can recover deleted data, facilitates access to encrypted information, or finds hidden data (Homeland Security 2016; Schlumberger et al. 2023, 7–9).

companies in turn have own dependencies and interests, as exemplified by the case of the Israeli NSO Group (cf. Bergman and Mazzetti 2022).

These procurement-related risk-benefit calculations are certainly context-specific, and likely influenced by regime-internal dynamics. However, a bourgeoning literature on digital surveillance proposes also structural factors, such as regime type or financial resources, to affect procurement decisions (Feldstein 2021; Feldstein and Kot 2023a; Palmer 2024; cf. also Zuboff 2019 and Schlumberger et al. 2023). Most prominently, this literature suggests substitution effects: Lacking technological, financial, or state capacities are compensated for by the private sector as attractive alternative to government-developed surveillance software (Palmer 2024; cf. also Schlumberger et al. 2023, 11; Feldstein 2021, 63). However, the theoretically derived, and partly contradicting, propositions have yet to be clarified and systematically tested. Therefore, the article engages with the research question of *what macrostructural factors determine public mercenary surveillance software acquisitions.*

In analyzing MSS acquisition data of 179 country observations between 2010 and 2022 in several cross-sectional regression models,[21] the article provides three crucial contributions: (I) It closes a research gap by clearing up several partly contradicting hypotheses, e.g., concerning the effects of regime type and other structural factors on MSS acquisition. (II) It identifies digital repression capacities as the most significant variable with a consistently positive effect on MSS procurement. A subsequent analysis suggests that digital repression capacities serve as an intervening variable for structural factors and regime type, which merits further analysis and interpretation. And finally, (III) it highlights the dire need for more effective regulatory frameworks of digital surveillance technologies that targets providers and clients alike, and how these products are used – especially in a time where democracy is at risk worldwide (Schmelzer and Karppi 2024). The relevance of these contributions is then exemplified in an outlook on (a) the global political economic patterns of digital technologies, and (b) on the digitally induced transformations in autocracies and democracies, and the future challenges of regime-typology.

[21] If not specified otherwise, programs used for this analysis are Stata version 2015 and 2017.

3.2. Digital Technology, Politics, and the Commercialization of Global Repression

All types of governments are resorting to digital surveillance technologies: be it social media surveillance in the US (Levinson-Waldman, Panduranga, and Patel 2022), targeted surveillance of 'suspected criminals' in France (Kayali 2023), surveillance-assisted total social control in China (Qiang 2019) or lethal surveillance-based repression in Myanmar (Hinz 2022) – the unprecedented technologically enhanced ability "to know" (Schlumberger et al. 2023) appears to be an irresistible trait for democracies and autocracies alike.[22] These technologies may indeed be used for legitimate reasons of national security (cf. Interpol 2024).[23] But their dual-use potential as powerful repressive instruments warrants critical and strong oversight. After all, securitization discourses and framings of national security are context dependent, and are also frequently employed by autocrats (cf. Ilbiz and Kaunert 2023; and Lai 2023; Maati and Švedkauskas 2021; 2020). Additionally, in times of authoritarian resurgence (Schmelzer and Karppi 2024), legitimately acquired surveillance capabilities might very well be turned against political opponents in backsliding democracies (cf. Bermeo 2016; and Freedom House 2019).

This development demands closer observation. Private sector tech industry has recognized a lucrative market. And contrary to its claims to sell only to selected governments solely for the purpose of national security, their products have been detected on the devices of human rights activists, journalists, opposition figures, and politicians (Amnesty International 2021; Benjakob 2022; Benjakob and Breiner 2022; Kirchgaessner 2021). MSS has also been linked to assassinations and forced disappearances, as in the case of Jamal Khashoggi (Kaster and Ensign 2023; Priest, Timberg, and Mekhennet 2021; Schaffer 2020), the repression of Uyghurs in China (Bhuiyan 2022), the torture and disappearances of dissidents in Egypt (Tesquet 2017; cf. Palmer 2024), and to massacres of civilian protestors in Khartoum, Sudan, in 2019 (Teloglou et al. 2022; cf. Palmer 2024).

To these companies, the desires of governments to possess such digital capabilities are demands of a solvent clientele in a lucrative market (cf. Borgeaud 2023; Hiebert 2023; Feldstein and Kot 2023a). This development matches other patterns in an underregulated market, where companies have come to provide

[22] When referring to democracies, and if not specified otherwise, this article refers to Dahls polyarchy (Dahl 1971, 3). Likewise, authoritarianism is to be understood as defined by Juan Linz (Linz 1964, 297–311).

[23] For example, the surveillance of known violent terrorists or criminals to track down organizational structures.

numerous digital goods and services, from commercializing personal information, to electoral manipulation and digital surveillance (Zuboff 2019; Deibert 2019; Saglam 2022). The ready availability of these technologies, the apparent wide-spread demand for such capabilities, and the potentially lethal consequences of using them with malicious intentions underscore the urgency of expanding our understandings of the factors and determinants that motivate governments to acquire them.

In this market, then, governments face the decision whether to invest financial, technological, and human resources to develop their own software solutions within their security apparatuses, or to turn to private sector providers instead (Palmer 2024; cf. also Feldstein 2021, 63). For government budgets, the latter might pose as cost-efficient alternative to 'in-house' development which might take years and cost millions: offers can be as cheap as "[…] $650,000, plus a $500,000 setup fee […]" to target ten device, as charged by NSO Group in 2016 (Perlroth 2016).

On the other hand, and when it comes to national security and intelligence, turning to private sector providers for critical and sensitive services is not without risk. Apart from principal-agent problems, security and intelligence agencies are dependent on the company when issues with their software arise. As in the case of Bahrain, where leaked emails with Germany's *FinFisher* documented the frustrated interactions between the Bahraini officials and the company's customer support services (Currier and Marquis-Boire 2014). Also, these companies usually cater to the needs of more than one country (Feldstein and Kot 2023a), potentially creating conflicts of interest for the companies to the detriment of individual client countries (cf. Bergman and Mazzetti 2022). Lastly, integrating a foreign entity into a country's security and intelligence strategy creates potentially far-reaching vulnerabilities: Democracies risk public backlashes once (ab)use of such mercenary software is made public, as in the case of Poland (Kość 2022); autocracies, in turn, may risk intrusion by actors outside of their own control with potentially destabilizing consequences for the regime.

In addition to such internal and contextual considerations, procurement decisions are also argued to be affected by structural factors. Turning to external private companies might only be a transitory phenomenon until these client-countries have developed their own technological internal capacities (Schlumberger et al. 2023, 11); others propose that limited capacities might be substitutable by the private sector also on the long-run (Palmer 2024). Yet others highlight the role of regime types and the necessity of elaborate administrative state capacities to effectively operate these technologies (Feldstein 2021, 63).

However, these determinants have not yet been tested systematically: While Palmer (2024) has established a first theoretically derived framework, her propositions, and her two non-systematic probability probes, still await rigorous and systematic empirical testing.[24] Feldstein (2021), in turn, has engaged in more systematic testing of digital repression and digital repression capacities; however, his analysis does not include a separate analysis of the acquisition of MSS. Therefore, this article tests the proposed hypotheses on structural determinants of MSS procurement which are presented in the following section.

3.3. Determinants of Acquisition

Until recently, information on the buyers of spyware was unsurprisingly limited, as surveillance is a sensitive area and regarded as an issue of national security. It is known, however, that clients of such companies entail consolidated authoritarian regimes, as well as democracies such as Germany, the United Kingdom, Canada, or Italy (Feldstein and Kot 2023a; 2023b).

Generally, authoritarian regimes are found to be more likely to rely on digital repression than democracies,[25] which also entails the acquisition and use of commercial spyware (Feldstein 2021, 11 & 62; Feldstein and Kot 2023a). This implies that, *ceteris paribus*, authoritarian regimes should be expected to acquire more commercial surveillance technology than democracies (Feldstein 2021, 63; Feldstein and Kot 2023a). Moreover, Feldstein also finds higher levels of offline repression to be also associated with higher levels of *digital* repression, which in turn might also come with more MSS acquisition. Consequently, one should expect more repressive regimes to acquire more surveillance technology. Here, the presence or

[24] Also, Palmer's framework unfortunately lacks conceptual clarity in defining and distinguishing the central concepts 'infrastructural control' versus 'state capacity'; or 'cyber capabilities' versus 'human resources' (cf. Palmer 2024, 288–89).

[25] Whereas MSS acquisition does not necessarily translate into repression, but studying procurement patterns is another step understanding forms of digital repression, which in turn, is understood "[…] as the use of information and communications technology to surveil, coerce, or manipulate individuals or groups in order to deter specific activities of beliefs that challenge the state" (Feldstein 2021, 25). However, instead of 'the state', this paper will use the notion of 'regime' as understood by Robert Fishman (Fishman 1990, 428). Distinguishing state and regime adds more nuance to the formal institutional structures and more informally structured power relations that determine access to and exercise of political power (Altmeppen and Edel 2017).

absence of institutional mechanisms of oversight, rule of law, and checks and balances are the suggested causal mechanism that explain differences along regime types (Ibid p.15). Consequently, the corresponding hypotheses $H_{1.1}$ - $H_{1.3}$ on regime characteristics are:

$H_{1.1}$: *Democracies are associated with lower levels of MSS acquisition, whereas autocracies are associated with higher levels.*

$H_{1.2}$: *High levels of rule of law are associated with lower levels of MSS acquisitions.*

$H_{1.3}$: *High levels of repression are associated with higher levels of MSS acquisitions.*

As for structural factors that are not immediately linked to regime types, Feldstein (2021, 42–44) and Palmer (2024) propose several, partly contradicting hypotheses. Feldstein highlights the necessity of greater state capacities to operate advanced digital (mercenary) surveillance systems effectively ($H_{2.1.}$).[26] In addition, Feldstein underscores the necessity of technological capacities (i.e., the *know-how*) to operate sophisticated surveillance software (Feldstein 2021, 42–44). [27] Palmer proposes an opposing mechanism: lower technological capabilities capacities ($H_{2.2}$), limited financial resources ($H_{2.3}$), and limited human capital ($H_{2.4}$) are all linked to more MSS acquisition (Palmer 2024, 288 & 289). Thus, hypotheses on capacity-related causalities are:

$H_{2.1}$: *Higher levels of state capacities are associated with higher levels of MSS acquisitions.*

$H_{2.2}$: *Higher technological capacities are associated with lower levels of MSS acquisitions.*

$H_{2.3}$: *Higher levels of financial resources are associated with lower levels of MSS acquisitions.*

[26] While 'state capacity' is not really defined by Feldstein in greater detail, at the most general level, it can be understood as the degree to which "[…] governmental institutions [are] capable of achieving the goals that they set for themselves" (O'Reilly and Murphy 2022a, 713). This entails the question of whether state administrations are professionalized, as well as sufficiently equipped, staffed, and trained.

[27] Less sophisticated digital surveillance technology would entail, for example, simple bugging devices that transmit audio signals but can easily be found.

$H_{2.4}$: *Higher levels of human capital are associated with lower levels of MSS acquisitions.*

Additionally, Palmer proposes that infrastructural control, i.e. "[…] the degree to which a state controls its domestic telecommunications infrastructure" (Palmer 2024, 288), also adheres to a causal mechanism.[28] Control over the information infrastructure is assumed to facilitate surveillance which might alleviate a state from seeking external help in the form of MSS. Thus:

H_3: *Higher infrastructural control of a state is associated with lower levels of MSS acquisitions.*

These eight hypotheses speak to three general clusters of proposed determinants of MSS acquisition which will be systematically tested: regime traits, capacities, and infrastructure (for an overview, see Table 2). The following section will layout the dataset used, critically reflect on its drawbacks, specify the operationalization of concepts and different models tested, and spell out the underlying assumptions.

Table 2 Expected effects of independent variables on mercenary surveillance software acquisition

Independent Variable	Expected Effects on Surveillance Acquisitions
Democracy	Negative
Rule of Law	Negative
Repression	Positive
State Capacity	Positive
Technological Capacity	Negative
Financial Resources	Negative
Human Capital Resources	Negative
Infrastructural Control	Negative

[28] Unfortunately, though, Palmer does not provide an elaborate definition of the concept of infrastructural control, nor is it clear, in how far it may or may not relate to other concepts, such as technological capacities or state capacities. For the sake of this analysis, infrastructural control will be approximated by the extent to which a regime can *legally* interfere in the digital information infrastructure, and the *capacity* to then sue this legal competency to enforce regulations.

3.4. Research Design

The dependent variables on MSS procurement are drawn from the Global Inventory of Commercial Spyware and Digital Forensics (GICSDF) dataset by Feldstein and Kot (2023a; 2023b). The independent variables are drawn from Feldstein's Digital Repression Index (Feldstein 2023), data from the Digital Society Project, as well as the Varieties of Democracy dataset (version 13.0; Coppedge, Gerring, Knutsen, et al. 2023; Coppedge, Gerring, Knutsen, et al. 2023; V-Dem 2022; Mechkova et al. 2019; Digital Society Project 2024), as well as the World Bank open dataset (World Bank 2024b).[29] To merge these datasets and construct coherent regression models for hypotheses-testing, several assumptions have been formulated that demand transparent and critical reflection.

4.3.1. Drawbacks and Assumptions

The GICSDF dataset is an incident-count based dataset that lists known events of a state's acquisition of a certain MSS. This information is based on the reports of different watchdog organizations, investigative journalistic projects, public records, and other sources. The dataset contains information on which country purchased what type of surveillance software from which commercial entity, together with the respective enterprise's country of origin, the period in which the software was used, and the time of disclosure of its use. The dataset consists of 192 acquisition observations between 74 different countries. Cross-checking the instances included, and researching beyond this dataset, yielded 20 additional instances of spyware purchases by 19 countries. These instances were previously excluded in the 2023 version of the GICSDF (cf. Marczak and McKune 2015; VSquare 2023; Marzocchi, and Mazzini 2022; Palmer 2024).[30]

[29] Additional datasets considered in the preliminary analyzes were the State Capacity Index, as well as the World Bank's Worldwide Governance Indicators (O'Reilly and Murphy 2022a; 2022b; Kaufmann and Kraay 2024). However, due to conceptual and methodological considerations, the respective variables were excluded from the final analysis. For more details (cf. Appendix Section 6, xi-xii; Section 7, xiii; and Section 8.4. to 8.5., xv- xvi).

[30] Some countries have previously been already included but new acquisitions were added. See Appendix Section 1. Table A.1.

This highlights the problem of hidden figures. Digital forensics and spyware usually fall within the jurisdiction of national security and intelligence agencies.[31] Therefore, information on MSS acquisitions is often classified, and not easily publicly accessible. Consequently, the *actual* figures of MSS acquisitions are likely higher than in the expanded GICSDF dataset. However, with the added observations, the dataset contains procurement information on 80 countries which is already a rather sizable sample. This is potentially just the tip of the iceberg, but due to the sample's size, it stands to reason that the dataset at least *approximates* the *relative* distribution of acquisition figures, i.e., what type of countries tend to buy, and if so, how much. To also include non-client countries, all other 99 countries that are not listed in the procurement dataset have been included.[32] Together, the dataset should therefore approximate at least the relative distribution of acquisition patterns:

$Assumption_1$: *The expanded dataset approximates the relative distribution of MSS acquisitions.*

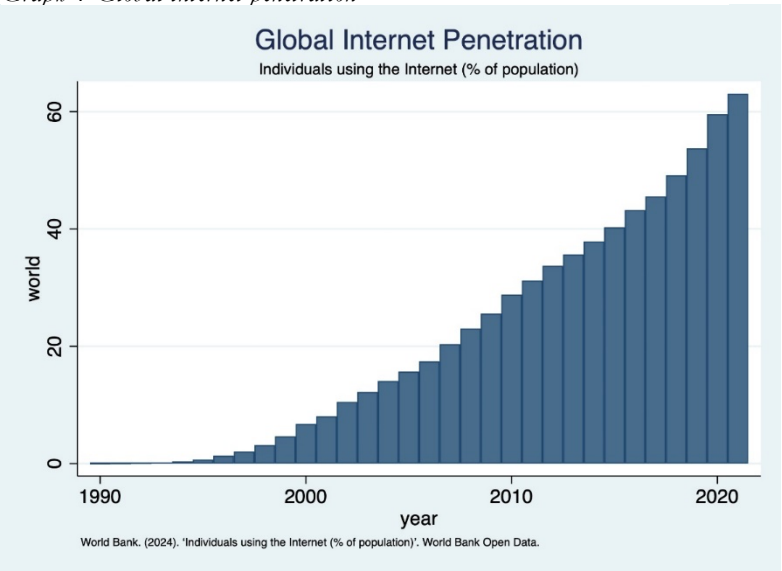
The largest drawback of the GICSDF dataset consists of the lacking temporal information. With the additional 20 observations, the dataset consists of 213 observations of MSS acquisition of which at least 99 are either fully or partially lacking time-related information (i.e., when exactly the acquisition took place). This is a major problem for cross-sectional analyzes, as the exact point in time of the respective acquisition is unknown and can thus not be precisely explained by the explanatory variables. To work around this problem, two crucial assumptions are proposed and tested: one concerning (a) the *period of relevance*, and another on (b) the *relative stability of macrostructural variables*:

[31] An assumed democracy-bias in the form of overreporting due to more transparent oversight by independent courts, a vibrant civil society, and a liberal media landscape can be refuted. If this bias existed in the dataset at a problematic level, the analysis would find democracies to be more strongly associated with acquisitions than autocracies – which is not the case. Instead, repressiveness was found to have an impact on acquisitions which alleviates this concern, as autocracies are generally more repressive than democracies.

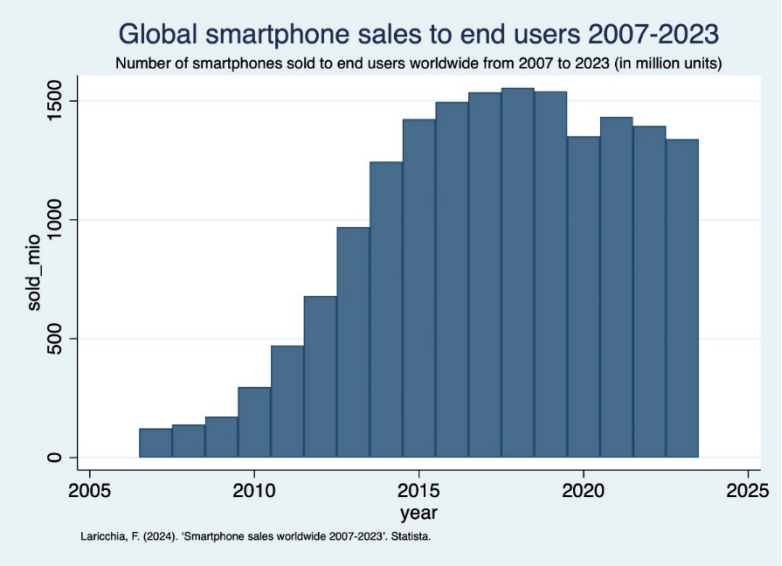
[32] As the country coding of the GICSDF is based on the V-Dem dataset, all other countries that V-Dem covers in the period of interest and that were not listed as buying regimes in the procurement dataset have been added as non-clients, with procurement numbers equaling zero.

Concerning (a) *the period of relevance*, the motivation is to establish an *ante quem* point in time for MSS acquisition, as clients would first have to acknowledge the relevance of digital surveillance and see an added value in procuring these technologies. As the most potent and most frequent use of, e.g., spyware is to infect mobile terminal-devices like smartphones, the market shares of these products, as well as the global rate of internet penetration provide a helpful indication to narrow down the window of relevance.[33]

Graph 1 Global internet penetration



Graph 2 Global smartphone sales to end users



[33] In addition to the theoretical foundation of this assumption, the models of the subsequent analysis have also been tested for different time periods to ensure the robustness of the results, and the models' time-sensitivity (cf. Appendix Section 11. Tables A.24-A.29.).

As displayed in Graphs (1) and (2), mobile and connected devices (*the* target for mercenary spyware and digital forensics software) have mostly picked up in numbers 2010 onwards, with annual smartphone sales only reaching more than a billion in 2014. Additionally, wide-spread surveillance of end-users with digital mercenary software was not yet as elaborate or prominent as demonstrated by the Arab Uprisings in 2011: during these protests, which came to be referred to as "Twitter-" or "Facebook-Revolutions", protestors mobilized and coordinated the protests via social media applications on their smartphones, then still able to evade the regimes' more rigid surveillance strategies (cf. Eaton et al. 2013; Smidi and Shahin 2017).

Observations of the GICSDF that come *with* temporal information (i.e., period of use), support this picture: only one observation predates 2010.[34] All other observations with temporal information fall into a time after 2010, with most lying sometime between 2013 and 2019. Thus, the idea is to narrow down the window of relevance for mercenary surveillance software acquisition as pseudo "point in time" for the dependent variable, spanning a period from 2013 to 2022.

$Assumption_{2a}$: *The efficacy of mercenary surveillance software has become particularly relevant and interesting for governments 2013 onwards; consequently, surveillance software acquisitions before 2013 are assumed to be marginal and of limited relevance.*

With respect to (b) *the relative stability of macrostructural factors*, the idea is to further narrow down the relevant time window for the explanatory variables of the cross-sectional data-analysis: If the dependent variable, MSS acquisition, is assumed to take place sometime between 2013 and 2022 (2022 as cut-off point determined by the availability of data), independent variables would have to fall within a range between 2010 to 2015. This lag would allow macrostructural variables to have a meaningful impact on acquisition decisions in the following years.

To select the appropriate base-years for the dependent variables, structural determinants of mercenary surveillance acquisition are assumed to remain relatively stable on a year-to-year basis. Especially, when comparing them in *relative* terms across all countries: annually, richer countries will likely stay *relatively*

[34] Germany, DigiTask spyware, used from 2007 to 2011.

richer at comparable levels than poorer countries; likewise, more democratic countries are assumed to likely remain *relatively* more democratic on comparable levels than their non-democratic counter-parts. While individual cases in this period might increase or decrease in 'democraticness', the focus is on the *overall* development of these variables, and the *relative* distribution between country values.

To test this assumption, all dependent variables (specified under section 4.b.) have been tested concerning their relative variation in several ways: (I) coefficients of variation, i.e., relative standard deviations, have been calculated across each variable for each country across the years 2010 to 2016 to get an impression of the changes of a country with respect to the particular variable.[35] (II) These country-year variation coefficient values were then analyzed to see in which value intervals they fall, to test whether variations of country-values were above the threshold of 1 or not. (III) The same was done for country-values but instead with annual values, the coefficients were calculated and analyzed for averages formed for 2010-15, 2012-15, 2014-15, as well as 2013-16. Additionally, (IV) for each variable, the variation was also calculated within each year *across all* countries, to then compare over all variations of all countries on an annual basis. Extremely different variations between years would indicate a greater annual change within the variable that would violate the assumption of relative stability. However, almost all structural variables passed the tests, yielding sufficiently low relative changes on a yearly base, thus substantiating the assumption.[36]

$Assumption_{2b}$: *The relevant macro-structural data for the independent variables are comparatively stable in relative and comparative annual perspective across the universe of cases, allowing for averages to be analyzed instead of yearly values.*

[35] Values between 0 and 1 indicate low to moderate variation; values over 1 indicate greater relative variation (Frost 2020) which renders arithmetic averages to be less appropriate mean models. The coefficient of variation can only be calculated for positive values. The CV for variables that take negative values was approximated by referring to absolute values; however, this heavily distorts the result. To control for the robustness of the regression results, different models were run with different years for dependent variables. These results were found to be robust and consistent irrespective of the base year or average chosen (cf. Appendix Section 11. Tables A.24-A.29.).

[36] E.g., Patent applications by resident, a proxy for technological capacities, varied too much and was subsequently excluded (cf. Appendix Section 2. on the calculation, and Section 3. Tables A.2.-A.9. on the results).

This means, that the final analytical models will test the potential determinants of MSS acquisitions with values taken from the period between 2010 and 2016. To validate the time-sensitivity and the robustness of the regression results, each model is also tested with different year- and average-based variables. Once again, the results indicate robust results.[37]

4.3.2. Concepts and Operationalizations

The hypotheses generated from the literature highlight six core concepts relevant for this analysis: (I) MSS acquisition, (II) state capacity, (III) financial resources, (IV) regime traits, (V) technological capacities, and (VI) infrastructural control (Feldstein 2021, 5, 10f, 14, 24, 42ff, 63f; Palmer 2024). The list of proxies used to operationalize the variables, and to test the hypotheses have been compiled in Table 3 for an overview.[38][39]

(I) Mercenary surveillance software acquisition, or MSSA, has been measured in two general ways: (a) in absolute numbers, aggregating the expanded GICSDF dataset by countries, generating new variables for spyware acquired (*spy*), digital forensics software acquired (*foren*), as well as the sum thereof (*digitool*);[40] but also (b) as dichotomous dummy variables, with value "1" for the acquisition of spyware (*dummy_spy*), digital forensics (*dummy_for*), as well as MSS in general (*dummy_digi*), and "0" for non-acquisition, respectively.

(II) State capacity has been approximated by different variables from the V-Dem dataset. These entail estimates of territorial control by the state (*terrcont*), the professionalization of a state's bureaucracy as measured by the amount of state representatives being salaried officials (*adminren*), the importance of

[37] See also Appendix Section 11. Tables A.24-A.29.).

[38] Variables are named following this logic: "[variable abbreviation]_[year or average indicator]". Therefore, "democr_1015" refers to the democracy score averaged over the years 2010 to 2015, and "gdpcon_14" refers to the a countries GDP in 2014.

[39] Some variables had to be inversed, as their original values were coded in counter-intuitive ways (i.e., V-Dem's civil society repression variable, where low values indicate *high*, and high values indicate *low* levels of repression). These variables are highlighted in Table 2 by the column "inversed".

[40] An additional residual category, "other", was created for the acquisition of internet of things (IOT) hacking services. It is captured in *digitool*. But this only concerns one observation and has therefore not been analyzed separately.

meritocracy in administrative career advancements (*admincrit*), and a state's capacity to generate revenue through fiscal administration (*fiscap*).

(III) Financial resources are controlled for as GDP per capita at current US Dollars (*gdppc*), GDP in purchasing power parities at constant 2017 international dollars (*gdpcon*), as well as with a proxy for the allocation of government budget into the security sector (*milex*, measured as share of GDP).[41]

(IV) Regime traits mentioned in the literature entail a measure for electoral democracy (*democr*), civil liberties (*civlib*), civil society repression (*csreprss*), efforts to censor media (*medcens*), harassment of journalists (*journhrs*), as well as rule of law (*rulev*). Additionally, personalism (*person*), measured as the importance of the person of the leader, was controlled for, as the degree of regime personalization has significant effects on regime-internal dynamics (Chehabi and Linz 1998; Colgan and Weeks 2015; Peceny and Beer 2003; Wright 2010; Geddes, Wright, and Frantz 2018). These variables, then, were all taken from the V-Dem dataset.

(V) Technological capacities are operationalized with Feldstein's digital repression capacity index (*digrepcap*) which is a factor that measures a country's filtering and shut-down capacities of social media and the internet, as well as regulatory capacities for online media and communication (cf. Feldstein 2021, 299–303). It is important to note, that neither the digital repression capacity index, nor its factor components from the Digital Society Project (Mechkova et al. 2019), reflect or measure MSS.[42] Another variable included to measure technological capacity is the access to high quality education (*eduqual*). Closer to the concept of human capital, and taken from the V-Dem dataset, this allows for a more nuanced control of Palmer's hypothesized substitution effect of human capital on MSS (Palmer 2024, 289).

(VI) Infrastructural control is approximated by the legal capabilities of the state to regulate online content (*legalcap*) and a state's digital regulatory approach (*regapp*); i.e., whether it pursues a statist or a liberal,

[41] All taken from the World Bank dataset. Military expenditure was not specified in the hypotheses, but as MSS falls into the area of national security, an inclusion was warranted.

[42] This index closely captures technological capacities relevant for digital repression and surveillance, as well as the cyber capabilities that were proposed as determinant by Palmer. It avoids the issue of homogeneity, i.e., that *MSS* (*digitool, spy, foren*) might be included in the digital repression capacity index: these are conceptually distinct (Feldstein 2021, 299–303), as the factor items do not measure targeted surveillance, which is also specified by Feldstein (2021, 63; cf. also Mechkova et al. 2019).

private-sector driven one. Other variables were tested in preliminary analyzes but were discarded for conceptual reasons or unsustainably high and significant.[43]

3.5. Analysis

This section will provide (3.5.1.) a brief descriptive overview over the MSS acquisition data, and (3.5.2.) specify appropriate regression models for the analysis of MSS acquisition and digital repression capacities, before (3.5.3.) providing an overview over the models tested. The regression results are then presented for (3.5.4.) the structural determinants and their effects on MSS acquisition, as well as (3.5.5.) the effects of structural determinants on digital repression capacities. The latter analysis was warranted, as digital repression capacity was found to be the strongest and most consistently significant structural determinant of acquisition decisions. These respective results also indicate that digital repression capacities are an intervening variable between structural determinants and MSS procurement decisions.

3.5.1. Overview over mercenary surveillance software acquisitions

The dataset for this analysis consists of 179 country observations, based on the V-Dem dataset (v.13) including independent territories with more than 250,000 inhabitants. Of these 179 countries, 80 countries have acquired at least one type of surveillance software; 75 of those countries have at least one spyware in their repertoire, whereas 28 of those countries have at least one digital forensics software; 23 countries have acquired at least one of each, spyware and digital forensics. Outliers of acquisition in this dataset are the United Arab Emirate (5 spyware software, 1 digital forensics software) Burma/Myanmar (14 types of forensics software), Saudi Arabia (7 spyware, 1 digital forensics), and the United States of America (2 spywares, 11 digital forensics).[44]

[43] For a more detailed explanation, as well as an overview over *all* variables consider, see Appendix Section 7, Section 8.3. Table A.13, as well as Section 8.4. Table A.14.

[44] For a descriptive overview over the independent variables, consider Appendix, Section 8.3., Table A.13., xiv.

1 *Table 3 Overview over Variables included in the Final Analysis*

Meta-Concept	#	Variable	Variable Source Name	Interpretation	Source	inverted
Country	01	*country*	country_name	Name of the purchasing country	V-Dem	-
	02	*country_text_id*	country_text_id	Three letter ID of the purchasing country	V-Dem	-
Mercenary Surveillance Software Acquisition (MASSA)	03	*digitool*	-	Number of acquisitions (sum of spy, foren, and other)	Feldstein & Kot	-
	04	*spy*	Category of technology	Number of spywares acquired	Feldstein & Kot	-
	05	*foren*	Category of technology	Number of digital forensics acquired	Feldstein & Kot	-
	06	*dummy_didi*	-	Dummy of surveillance software acquisition ("1" purchase; "0" no purchase")	-	-
	07	*dummy_spy*	-	Dummy of spy ("1" purchase; "0" no purchase")	-	-
	08	*dummy_for*	-	Dummy of foren ("1" purchase; "0" no purchase")	-	-
	09	*other*	Category of technology	Number of other acquired neglectable as n=1	Feldstein & Kot	-
	10	*dummy_other*	-	Dummy of other ("1" purchase; "0" no purchase") neglectable as n=1	-	-
State Capacity	11	*admincrit*	v2stcritrecadm	Relevance of meritocratic criteria for career in state administration career; ~[-5,0 : 5,0], low to high	V-Dem	-
	12	*adminren*	v2strenadm	The extent of which state officials are salaried employees; ~[-5,0 : 5,0], low to high	V-Dem	-
	13	*fiscap*	v2stfisccap	The state's capacity to fund itself through tax collection; ~[-5,0 : 5,0], low to high	V-Dem	-
	14	*terrcont*	v2svstterr	The state's control over its territory; [0:100], low to high	V-Dem	-
	15	*statecap*	statecap_base_fiscal	Measuring state capacity as index; ~[-5,0 : 5,0] low to high	O'Reilly & Murphy	-
Financial Recourses	16	*gdpcon*	GDP, PPP (constant 2017 int. $)	GDP purchasing power parity in international 2016 $	WB	-
	17	*gdppc*	GDP per capita (current US$)	GDP per capita in current US$	WB	-
	18	*milex*	Military expenditure (% of GDP)	Share of military spending Interval [0:100], from low to high	WB	-
Regime Traits	19	*democr*	v2x_polyarchy	Measuring electoral democracy as index; ~[-5,0 : 5,0], low to high	V-Dem	-
	20	*civlib*	v2x_civlib	Measuring civil liberties as index; ~[-5,0 : 5,0], low to high	V-Dem	yes
	21	*csreprss*	v2csreprss	Repression against civil society organizations; ~[-5,0 : 5,0], low to high	V-Dem	yes
	22	*medcens*	v2mecenefm	Efforts by government to censor media; ~[-5,0 : 5,0], low to high	V-Dem	yes
	23	*journhrs*	v2meharjrn	Harassment of journalists; ~[-5,0 : 5,0], low to high	V-Dem	yes
	24	*rulev*	v2x_rule	Measuring the rule of law as index; [0: 1], low to high	V-Dem	-
	25	*person*	v2exl_legitlead	Measuring the importance of the person of the leader; ~[-5,0 : 5,0], low to high	V-Dem	-
Technological capacities	26	*digrepcap*	Digital Repression Capacity Index	Measuring the capacity for digital repression as index; ~[-5,0 : 5,0], low to high	Feldstein	-
	27	*eduqual*	v2peedueq	Approximating the access to high quality education; ~[-5,0 : 5,0], low to high	V-Dem	-
Infrastructural control	28	*legalcap*	v2smregcon	Approximating the legal capabilities to regulate online content; ~[-5,0 : 5,0], low to high	V-Dem	yes
	29	*regapp*	v2smregapp	Approximating the regulatory approach from low = liberal (private sector driven) to high (statist approach); ~[-5,0 : 5,0], low to high	V-Dem	yes
Infrastructure	30	*inet*	Individuals using the Internet (% of population)	Interval [0:100], from low to high	WB	-

3.5.2. Model specification

Testing the distribution of MSS, the visual investigation of the dependent variables' histograms (Graphs 3 to 5) measuring MSSA in absolute terms (*digitool*, *spy*, *foren*) refutes the assumption of normality. Likewise, the skewness and kurtosis tests support this impression.[45] This is to be expected, as the data is incident-count-based and thus more likely to follow a Poisson distribution.

However, the MSSA data violates the necessary condition for a Poisson distribution.[46] This is further substantiated after running the Pearson goodness-of-fit test, as well as a Poisson post-estimation test, indicating over-dispersion of the data.[47] The most appropriate regression model for the over-dispersed count-based MSS data is therefore a negative binomial regression model (UCLA: Statistical Consulting Group. 2021b; 2021a). For the dummy versions of the dependent variables (*dummy_digi*, *dummy_spy*, *dummy_for*), a regular logistic regression model will be used to determine likelihoods of acquisitions.

The separate analysis of the digital repression capacity (*digrepcap*) will use a regular ordinary least square regression model with robust standard errors, as the variable passes the skewness and kurtosis test.[48] Further, an OLS test-regression model with robust errors yields no pattern of the model's residuals versus its fitted values; likewise, the Breusch-Pagan and Cook-Weisber tests for heteroskedasticity yield no problematic results of the model.[49][50]

---

[45] Normality is violated at a statistically high level of significance ($p<0.01$).

[46] The mean values do not equal the respective standard deviations: $\mu_{digitool}$ = 1.1787 and $\sigma_{digitool}$ = 1.9919; μ_{spy} = 0.8268 and σ_{spy} = 1.2353; μ_{foren} = 0.3463 and σ_{foren} = 1.4388.

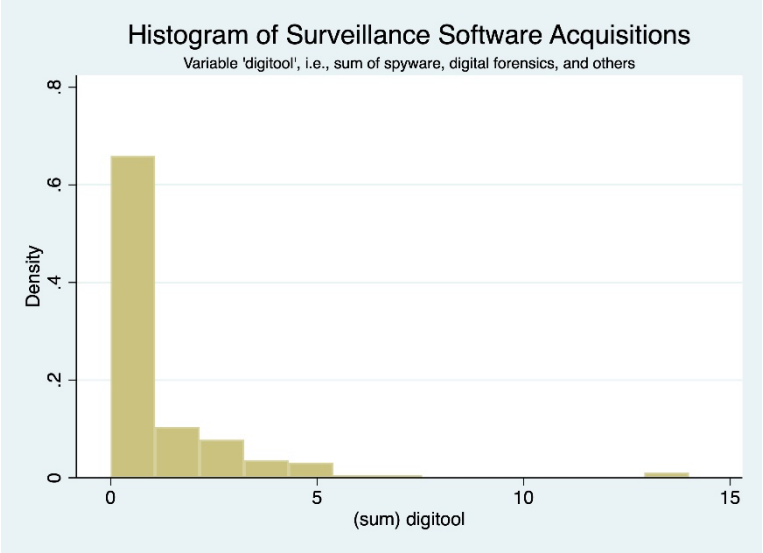
[47] Both results yield a Prob > chi2 of 0.0000, refusing the null hypothesis that a regular Poisson distribution is an appropriate fit of the MSSA data.

[48] Prob > chi^2 = 0.5081.

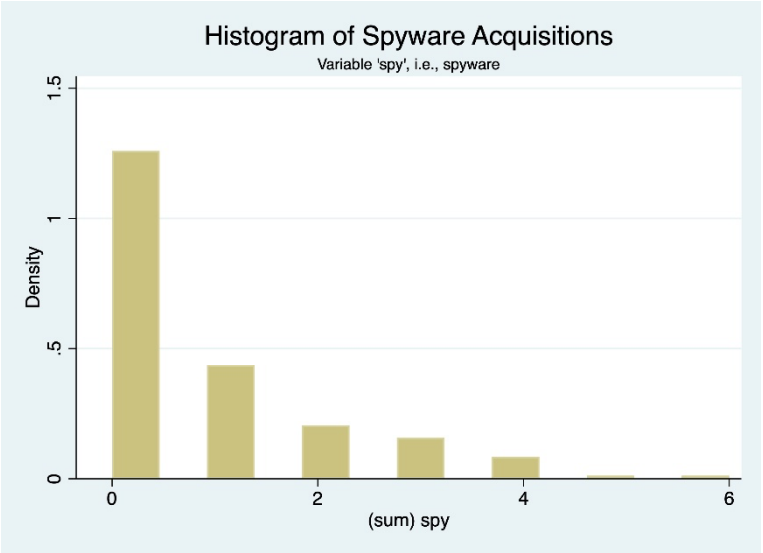
[49] Prob > chi^2 = 0.3225

[50] Consider Appendix Section 9.6. Table A.21., Section 10.1. Table A.22., as well as Section 10.2. Table A.23. for more information.

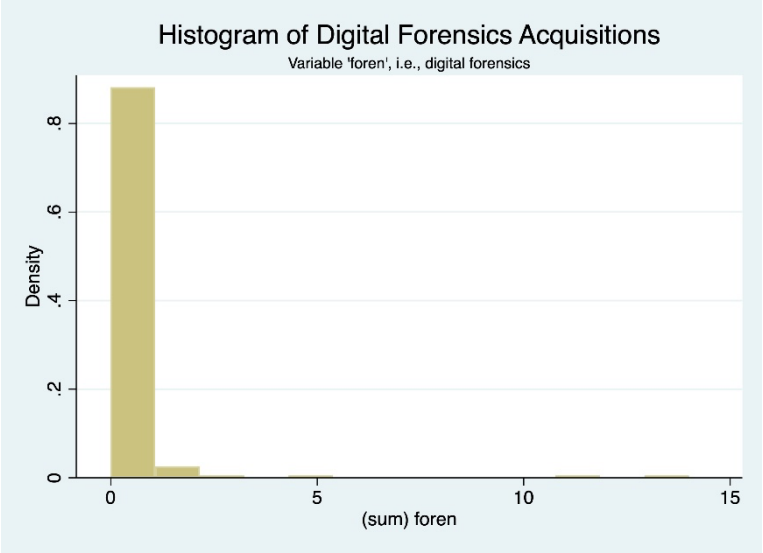
Graph 3 Histogram of Surveillance Software Acquisitions (digitool)



Graph 4 Histogram of Spyware Acquisitions (spy)



Graph 5 Histogram of Digital Forensics Acquisitions (foren)



3.5.3. Model specification

The combination of the regression models' independent variables is based on the theoretical propositions by Palmer and Feldstein, as well as the pair-wise correlations.[51] Models with different variable combinations were tested to avoid the inclusion of highly and significantly correlated variables in the same model (e.g., democracy and harassment of journalists). This approach yielded three main sets of regression models: one set (D1-D6) controlling for democracy in general (*democr*), another one (R1-R6) controlling for rule of law (*rulev*), and a third one controlling for the repressiveness of a regime (*journhrs*) and a measure for personalism (*person*) (S1-6). These three models (S, R, and D) were then used for the regressions of the dependent variables: as negative binomial regression models for the absolute acquisition numbers (*digitool, spy, foren*), and as logistic regression models for their dummy versions (*dummy_digi, dummy_spy, dummy_foren*).

In the second part of the analysis, the structural determinants were then also used as explanatory variables against digital repression capacity (*digirepacp*) as dependent variable in an OLS regression model with robust standard errors, where digital repression capacity of the year 2016 was regressed against the averaged explanatories of 2010 to 15.

3.5.4. Results for structural determinants and MSS acquisition

Table 4 to 6 present the results of the different MSS acquisition models (S1-6, D1-6, R1-6). The regression models explain a healthy 10 to 30 % of the data variation (as measured by the pseudo-R-square). Tests for multicollinearity remained negative, and the negative binomial regression models, as well as the logic models seem to be appropriate fits. After running several analyzes and different tests (cf. Appendix Section 9 & 10, p.xvii-xxvii), the main findings imply that structural determinants play a more nuanced role than the literature would suggest.

[51] Consider Appendix Section7., as well as Section 8.4. Table A.14., and Section 8.5. Table A.15. for the selection of variables and Appendix Section 8.5. Table A.15. for more detailed information on the pairwise correlation; for the correlation, a threshold of r = 0.69 was determined (cf. Dormann et al. 2013).

Table 4 Regression Results S1-6	S1	S2	S3	S4	S5	S6
Dependent Variables	dummy_digi	dummy_spy	dummy_for	digitool	spy	foren 1
Independent Variables						
Journalist Harassment *(journhrs_1015)*	0.486*	0.385	0.662	0.372**	0.329*	0.533
	(0.283)	(0.277)	(0.409)	(0.176)	(0.178)	(0.377)
Person of the Leader *(person_1015)*	-0.381*	-0.400*	0.337	-0.160	-0.182	0.148
	(0.223)	(0.219)	(0.264)	(0.129)	(0.139)	(0.244)
Digital Repression Capacity *(digrepcap_1015)*	1.722***	1.586***	1.515***	1.111***	0.988***	1.423***
	(0.369)	(0.354)	(0.491)	(0.211)	(0.206)	(0.490)
GDP (ppp, con. int. 2017 $, billion) *(gdpcon_1015_bio)*	-0.000	0.000	0.000	-0.000	0.000	-0.000
	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)
GDP p.c. (current US$, ten thousand) *(gdppc_1015_10k)*	-0.306**	-0.264**	0.070	-0.121	-0.128	-0.063
	(0.137)	(0.132)	(0.145)	(0.080)	(0.080)	(0.162)
Military Expenditure (% of GDP) *(milex_1015)*	0.148	0.098	-0.010	0.071	0.078	0.096
	(0.171)	(0.170)	(0.245)	(0.110)	(0.107)	(0.243)
Online Regulatory Approach *(regapp_1015)*	-0.384	-0.344	-0.588	-0.136	-0.179	-0.158
	(0.270)	(0.264)	(0.360)	(0.152)	(0.153)	(0.320)
Territorial Control by State *(terrcont_1015)*	0.068**	0.071**	0.044	0.006	0.015	-0.015
	(0.033)	(0.033)	(0.042)	(0.020)	(0.020)	(0.039)
Access to high quality education *(eduqual_1015)*	-0.827***	-0.776***	-1.104***	-0.379***	-0.283**	-0.775**
	(0.244)	(0.234)	(0.323)	(0.134)	(0.130)	(0.306)
Remuneration of Administration *(adminren_1015)*	-0.118	-0.168	-0.074	-0.081	-0.024	-0.216
	(0.391)	(0.384)	(0.516)	(0.236)	(0.231)	(0.510)
Fiscal Capacity of State *(fiscap_1015)*	0.428	0.288	1.057**	0.429**	0.267	0.964**
	(0.295)	(0.287)	(0.460)	(0.193)	(0.190)	(0.444)
Constant	-6.006**	-6.291**	-6.582*	-0.685	-1.709	-0.702
	(2.879)	(2.850)	(3.755)	(1.765)	(1.770)	(3.369)
Observations	132	132	132	132	132	132
Pseudo R^2	0.2810	0.2458	0.3031	0.1285	0.1141	0.1812

Standard errors in parentheses

*** p<0.01, ** p<0.05, * p<0.1

Table 5 Regression Results D1-6	D1	D2	D3	D4	D5	D6
Dependent Variables	dummy_digi	dummy_spy	dummy_for	digitool	spy	foren 1
Independent Variables						
Democracy *(democr_1015)*	-1.345 (1.561)	-0.689 (1.529)	-4.066* (2.284)	-1.636 (1.036)	-1.628 (1.038)	-3.001 (2.029)
Digital Repression Capacity *(digrepcap_1015)*	1.525*** (0.350)	1.409*** (0.340)	1.426*** (0.462)	1.022*** (0.219)	0.869*** (0.206)	1.378*** (0.490)
GDP (ppp, con. int. 2017 $, billion) *(gdpcon_1015_bio)*	0.000 (0.000)	0.000 (0.000)	-0.000 (0.000)	0.000 (0.000)	0.000 (0.000)	-0.000 (0.000)
GDP p.c. (current US$, ten thousand) *(gdppc_1015_10k)*	-0.263** (0.124)	-0.222* (0.120)	0.053 (0.144)	-0.098 (0.077)	-0.106 (0.076)	-0.066 (0.159)
Military Expenditure (% of GDP) *(milex_1015)*	0.116 (0.172)	0.059 (0.173)	0.039 (0.244)	0.072 (0.110)	0.069 (0.105)	0.125 (0.239)
Online Regulatory Approach *(regapp_1015)*	-0.318 (0.262)	-0.288 (0.257)	-0.446 (0.334)	-0.125 (0.152)	-0.207 (0.152)	-0.115 (0.310)
Territorial Control by State *(terrcont_1015)*	0.057* (0.031)	0.058* (0.031)	0.057 (0.042)	0.000 (0.019)	0.010 (0.019)	-0.005 (0.036)
Access to high quality education *(eduqual_1015)*	-0.833*** (0.234)	-0.774*** (0.223)	-1.135*** (0.312)	-0.419*** (0.130)	-0.296** (0.123)	-0.838*** (0.293)
Remuneration of Administration *(adminren_1015)*	-0.041 (0.379)	-0.106 (0.371)	0.018 (0.497)	-0.014 (0.238)	0.025 (0.230)	-0.104 (0.502)
Fiscal Capacity of State *(fiscap_1015)*	0.634** (0.321)	0.471 (0.310)	1.065** (0.503)	0.589*** (0.217)	0.456** (0.213)	1.004** (0.471)
Constant	-4.861* (2.819)	-5.223* (2.781)	-6.034 (3.832)	0.244 (1.737)	-0.845 (1.749)	-0.539 (3.245)
Observations	132	132	132	132	132	132
Pseudo R^2	0.2604	0.2237	0.2822	0.1225	0.1093	0.1760

Standard errors in parentheses

*** p<0.01, ** p<0.05, * p<0.1

Table 6 Regression Results R1-6	R1	R2	R3	R4	R5	R6
Dependent Variables	dummy_digi	dummy_spy	dummy_for	digitool	spy	foren
Independent Variables						
Rule of Law *(rulev_1015)*	-1.202 (1.245)	-0.473 (1.205)	-1.640 (1.612)	-0.100 (0.791)	-0.112 (0.808)	-0.889 (1.428)
Digital Repression Capacity *(digrepcap_1015)*	1.585*** (0.346)	1.441*** (0.332)	1.635*** (0.479)	1.166*** (0.212)	0.998*** (0.201)	1.576*** (0.512)
GDP (ppp, con. int. 2017 $, billion) *(gdpcon_1015_bio)*	0.000 (0.000)	0.000 (0.000)	0.000 (0.000)	0.000 (0.000)	0.000 (0.000)	-0.000 (0.000)
GDP p.c. (current US$, ten thousand) *(gdppc_1015_10k)*	-0.253** (0.124)	-0.219* (0.120)	0.050 (0.146)	-0.100 (0.079)	-0.107 (0.078)	-0.071 (0.166)
Military Expenditure (% of GDP) *(milex_1015)*	0.118 (0.174)	0.058 (0.173)	-0.024 (0.245)	0.069 (0.114)	0.065 (0.109)	0.085 (0.247)
Online Regulatory Approach *(regapp_1015)*	-0.298 (0.254)	-0.271 (0.248)	-0.304 (0.325)	-0.038 (0.156)	-0.117 (0.157)	0.001 (0.315)
Territorial Control by State *(terrcont_1015)*	0.060* (0.032)	0.059* (0.031)	0.063 (0.041)	0.002 (0.020)	0.012 (0.020)	-0.003 (0.037)
Access to high quality education *(eduqual_1015)*	-0.782*** (0.245)	-0.757*** (0.236)	-1.115*** (0.319)	-0.452*** (0.144)	-0.330** (0.137)	-0.829*** (0.304)
Remuneration of Administration *(adminren_1015)*	-0.016 (0.381)	-0.099 (0.372)	0.032 (0.484)	-0.042 (0.245)	-0.003 (0.236)	-0.096 (0.512)
Fiscal Capacity of State *(fiscap_1015)*	0.592** (0.287)	0.435 (0.276)	0.677 (0.413)	0.364** (0.179)	0.238 (0.175)	0.665* (0.396)
Constant	-5.207* (2.795)	-5.409** (2.739)	-7.271** (3.684)	-0.387 (1.770)	-1.527 (1.756)	-1.342 (3.316)
Observations	132	132	132	132	132	132
Pseudo R^2	0.2614	0.2234	0.2628	0.1162	0.1022	0.1652
Standard errors in parentheses *** p<0.01, ** p<0.05, * p<0.1						

Technological capacities had a consistent and significant impact, but in the direction opposite than expected. The findings contradict $H_{2.2}$ on the substitution effect between technological capacities and MSS proposed by Palmer. Technological capacities (*digrepcap*) have a consistent, highly significant, and *positive* impact on MSS acquisition ($p<0.001$): this holds for absolute acquisition numbers, the likelihood of acquisition, and all different MSS subtypes, respectively. Instead, the models substantiate Feldstein's claim, that the use and acquisition of more sophisticated surveillance technology requires sufficiently high technological capacities.

The models also support the existence of substitution effects between for financial resources ($H_{2.4}$) and human capital ($H_{2.3}$) (albeit more moderately for the former). Greater access to high quality education is significantly associated with a lower likelihood of procurement, as well as the total acquisition numbers ($p<0.01$). These results are consistent across the respective subtypes of MSS. *Ceteris paribus*, higher per capita income is also associated with lower likelihood to acquire mercenary surveillance software, and spyware in particular. However, per capita did not affect the total number of software acquired, or digital forensics more specifically.

Territorial control turned out to be the only proxy of state capacity that had a somewhat consistent and positive, albeit weakly significant effect on MSS acquisition and the likelihood to acquire spyware throughout all models (S, D, and R; significance between $p<0.05$ and $p<0.1$). Depending on the model, fiscal state capacity was positively associated with MSS acquisitions at varying degrees of significance: While it had some influence on the likelihood of MSS acquisition (insignificant in S1; $p <0.05$ in R1 and D1), it was more consistently and moderately significant for total acquisition numbers, and for digital forensics in particular ($p<0.05$). This also provides moderate support for Feldstein who suggested that state capacities are *required* in order to use sophisticated surveillance technology effectively ($H_{2.1}$). Infrastructural control, as proxied by the regulatory approach (with values from low to high representing statist to liberal approaches) did not turn out to be significant in any of the models tested. Consequently, infrastructural control as determinant for MSS acquisition is refuted in by this analysis (H_3).

Interestingly, proxies of regime traits played a marginal role in explaining both, the likelihood of MSS acquisition, as well as the total number acquired. These results also hold for the respective MSS subtypes. When controlling for personalism and harassment of journalists, the latter had a positive and weakly significant ($p<0.1$) effect on the likelihood of MSS acquisition, and a more moderately significant

and positive effect on the total acquisition number (S1-S6; $p<0.05$). Personalism, in turn, was only weakly and negatively associated with the likelihood of MSS acquisition, and of spyware in particular. In the democracy models, the electoral democracy index was only marginally important, and weakly associated with a lower likelihood to acquire digital forensics software (D1-D6; $p<0.1$). Rule of law did not play any significant role either (R1-R6). These findings, then, seem to refute the idea that regime type, or rule of law have a negative effect on MSS acquisition ($H_{1.1}$, and $H_{1.2}$); and even repressiveness has only a weakly significant positive effect ($H_{1.3}$).

Table 7 Overview on Hypotheses Tests

Variable	Predicted Effect on MSS procurement	Findings
Democracy ($H_{1.1}$)	Negative	Weakly supported
Rule of Law ($H_{1.2}$)	Negative	Not supported
Repression ($H_{1.3}$)	Positive	Moderately supported
State Capacity ($H_{2.1}$)	Positive	Moderately supported
Technological Capacity ($H_{2.2}$)	Negative	Strongly Contested – positive and significant effect on MSSA
Financial Resources ($H_{2.3}$)	Negative	Moderately supported
Human Capital ($H_{2.4}$)	Negative	Supported – consistent negative and significant effect on MSSA
Infrastructural Control (H_3)	Negative	Not Supported

3.5.5. Results for Structural Determinants and Digital Repression Capacity

Digital repression capacity consistently turned out to be the single most significant independent variable with a positive effect on the likelihood of MSS acquisition, and on total numbers acquired. Consequently, the variable was analyzed in a separate cross-sectional OLS regression models with robust standard errors, regressing the 2016 capacities against the explanatories averaged over 2010-5 (DRC1-4, Table 8 respectively). Here, structural factors played a more significant role in determining a country's capacity to digitally repress, highlighting its potential role as intervening variable between structural determinants and MSS acquisition.

Unsurprisingly, regime traits, as approximated by the electoral democracy index and the civil liberty index, had a highly significant, as well as a negative impact on digital repression capacities ($p<0.01$; in line with Feldstein 2021). Per capita income is found to have positive effect on digital repression capacities at a weak to moderate level of significance. Personalism also has a positive and highly significant impact on digital repression capacities ($p<0.01$). Likewise, a more statist regulatory approach on the online sphere, greater access to high quality education, as well as greater state capacities increased digital repression capacities at a moderate level of significance. These findings support the notion that democratic regimes are less likely to expand their digital repression capacities when compared to more autocratic and repressive regimes. Also, this supports that an expansion of the technical capacities to employ digital repression tools is associated with more repressive regimes.

Table 8 Regression Results DRC1-4	DRC1	DRC2	DRC3	DRC4
Dependent Variables	digrepcap_16	digrepcap_16	digrepcap_16	digrepcap_16
Democracy *(democr_1015)*		-2.267***	-1.369**	
		(0.443)	(0.581)	
Civil Liberties Index *(civlib_1015)*	-1.584***			
	(0.509)			
Harassment against Journalists *(journhrs_1015)*				0.099
				(0.102)
Person of the Leader *(person_1015)*	0.193***		0.127*	0.178***
	(0.065)		(0.070)	(0.063)
GDP (ppp, con. int. 2017 $, billion) *(gdpcon_1015_bio)*	-0.000	-0.000	-0.000	-0.000
	(0.000)	(0.000)	(0.000)	(0.000)
GDP p.c. (current US$, ten thousand) *(gdppc_1015_10k)*	0.055**	0.053**	0.051*	0.050*
	(0.025)	(0.022)	(0.027)	(0.030)
Military Expenditure (% of GDP) *(milex_1015)*	-0.064	-0.055	-0.046	-0.055
	(0.053)	(0.057)	(0.054)	(0.053)
Online Regulatory Approach *(regapp_1015)*	0.200**	0.234***	0.205**	0.268***
	(0.087)	(0.080)	(0.084)	(0.085)
Territorial Control by State *(terrcont_1015)*	-0.004	-0.001	-0.006	-0.009
	(0.009)	(0.008)	(0.009)	(0.009)
Access to high quality education *(eduqual_1015)*	0.123**	0.132**	0.189***	0.190***
	(0.052)	(0.051)	(0.056)	(0.060)
Remuneration of Administration *(adminren_1015)*	-0.021	-0.048	-0.023	-0.044
	(0.113)	(0.109)	(0.117)	(0.123)
Meritocracy of Administration *(admincrit_1015)*	0.375***	0.363***		
	(0.106)	(0.106)		
Fiscal Capacity of State *(fiscap_1015)*	0.226**	0.252**	0.400***	0.329***
	(0.096)	(0.109)	(0.085)	(0.078)
Constant	1.207*	1.089	0.957	0.723
	(0.634)	(0.715)	(0.745)	(0.740)
Observations	132	132	132	132
Adjusted R^2	0.416	0.403	0.355	0.322

Standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1

3.5. Interpretation

So, what are the structural determinants of public procurement of mercenary surveillance software? Based on these finding, if a country wants to possess state of the art surveillance technology, human capital does not pose a *conditio sine qua non* in this pursuit, nor do financial resources, or regime type: A lack in these resources for the development of own software can simply be compensated for by private sector providers.

Still, this substitution requires at least a sufficiently developed administrative apparatus. Surprisingly, and against the assumptions in the literature, countries with cyber capabilities, proxied by digital repression capacities are also more likely to acquire MSS, and in greater numbers.[52] Interestingly, digital repression capacities appear as an intervening variable between structural factors, such as regime types and state capacities, as well as MSS acquisition, which merits further investigation.

These results allow for several interpretations: (I) There are barely any structural factors that impair MSS acquisition. Consequently, a growing number of regimes will be in control of powerful surveillance software – either by developing these technologies themselves, or by turning to private sector providers. And (II) if a regime is expanding their digital repression capacities, they will also acquire more commercial surveillance software. (III) The acquisition patterns also hold across democracies and autocracies: When controlling for other variable, regime-type does not affect MSS acquisition. Obviously, however, this does not imply an equally malicious uses of these technologies *per se*. Qualitative differences between autocracy and democracy prevail: Autocracies continue to be more violent and repressive than democracies (cf. Feldstein 2021). And transgressions in the latter continue to be subjected to greater public scrutiny and legal consequences if abuses are detected and those responsible are identified (cf. Kość 2022; Smith 2023). And as MSS can be used for legitimate purposes, such as national security and fighting organized crime, as well as for repression, autocracies and democracies will consequently continue to acquire surveillance technologies.

However, (IV) notwithstanding qualitative regime-type differences between democracies and autocracies, this raises concerns. Unimpaired by almost any structural factors, and unaffected by regime type, private sector companies continue to be indiscriminate providers that contribute to a wider proliferation of powerful surveillance tools. And these tools have been frequently abused by politicians and governments – also in democratic contexts: In Poland, spyware was used by the PiS-government to spy on its opposition (Kość 2022); in Spain, Catalan journalists and politicians were also most likely targeted by the government (Scott-Railton et al. 2022); in Greece, Prime Minister Kyriakos Mitsotakis allegedly spied on allies and opponents alike (Smith 2023); and the USA has also been found to spy on journalists and allies

[52] As mentioned in footnote 21, the acquisition of MSS and the way digital repression capacity is measured is conceptually distinct (cf. Feldstein 2021, 63, 299–303).

(Khudayer et al. 2014; Gellman, Blake, and Miller 2013; Gellman 2020; Gunitsky 2020; Michaelsen and Glasius 2018). Additionally, and justified by a discourse of securitization, Germany, France, and other countries have been pushing for new EU-legislation that would also allow journalists to be surveilled with spyware, potentially causing chilling effects across Europe (O'Carroll 2023; Lavrilleux et al. 2023). And while transgressions are still subjected to legal prosecution in democracies, within the global context of continuous democratic backsliding (cf. Schmelzer and Karppi 2024), democratic governments today might very well purchase the surveillance tools for tomorrow's dictators, and provide the legal frameworks to (ab)use them. Consequently, and (V), the findings of this analysis highlight the necessity for more effective regulatory frameworks: (a) Concerning the commercial provision of such software (cf. Feldstein and Kot 2023a), but also (b) regarding the regime-internal frameworks that regulate the acquisition, development, use, and oversight of such technologies in democracies. Otherwise, an un- or under-regulated market of surveillance technologies runs the risk of pouring more gasoline into the fire that is the global state of democracy in the twenty-first century (cf. Schmelzer and Karppi 2024).

3.5. Outlook

Democracy is at stake, and the results of this analysis warrant an outlook on the larger context against which the acquisition patterns of surveillance software need to be understood. This context entails (I) the global political economic structures of digital technologies, as well as (II) the conceptualization and distinctions of regime-types in the twenty-first century.

(I) The systemic under-regulation of digital industries creates a permissive global economic context that incentivizes the development and commercialization of ever-more potent repressive tools (Saglam 2022; cf. also Feldstein and Kot 2023a). Consequently, tech companies that market potentially dangerous technologies like MSS are major beneficiaries of commercialized digital surveillance and are pillars of digital repression strategies worldwide. Their indiscriminate provision of potent digital repression tools does not only endanger societies of countries they are sold to; they also undermine the privacy of politicians, activists, and citizens worldwide, due to their territorially unrestricted nature (cf. Dalmasso et al. 2018; Glasius 2018). Because these companies, and their potential anti-democratic effects, are a global phenomenon (Freedom House 2019; Abramowitz and Chertoff 2018; Sherman 2019), safeguarding democracies in the twenty-first

century, requires more effective global regulatory frameworks of these industries (cf. Feldstein and Kot 2023a).

Further, the global market of commercialized of surveillance and repression deepens international structures and dynamics of dependence: the companies that provide surveillance technology are located in industrialized high-income countries, predominately in the Global North (Feldstein and Kot 2023a). As shown in this analysis, countries with lower per capita income are more likely to acquire these technologies from the private sector. If these countries acquire these technologies for autocratic purposes, tech-capital from the Global North becomes complicit in the repression of societies in lower-income countries (cf. Saglam 2022); as was the case with Germany's FinFisher and their indiscriminate sales to numerous autocracies (Reporters Without Borders 2023). If countries purchase these technologies for national security strategies, they render themselves vulnerable to the commercial providers, and to the governments of the countries these companies preside in. This can have detrimental effects on national security, as exemplified by the decision of the Israeli government to block Ukraine's acquisition of spyware from NSO Group in 2019 ahead of the Russian invasion (Bergman and Mazzetti 2022; Kirchgaessner 2022). That case also illustrates the asymmetric income-dimension of this dependence: At that time, Israel reported a per capita income of 44,452 USD, compared to Ukraine's 3,752 USD (World Bank 2024a).

(II) Digital technologies will make it harder to distinguish autocracies from democracies in the twenty-first century. Digital innovations, such as digital surveillance technologies, allow autocratic regimes in the twenty-first century to *look* more democratic and to appear less repressive than they are (Kendall-Taylor, Frantz, and Wright 2020; Schlumberger et al. 2023; Guriev and Treisman 2019). They put incumbents at an advantage vis-à-vis their population (Rød and Weidmann 2015), as there are manifold ways to control the digital infrastructures (Keremoğlu and Weidmann 2020). These incredibly powerful innovations amplify and transform authoritarian rule itself (Schlumberger et al. 2023) by facilitating fine-tuned and less obvious repression which is more powerful in controlling beliefs and behaviors of populations than analogue techniques (Ibid, 11-17).

Also, we know from contemporary cases of backsliding that democratic decay does not usually come radically overnight, as did military coups in the last century (Bermeo 2016; Freedom House 2019). Instead, these are creeping processes that manifest themselves in seemingly tolerable and insidious ways. This subtlety of backsliding will be complemented by a technologically-facilitated *calmer-looking* front of

future autocracies (Schlumberger et al. 2023, 12f). Covert surveillance technologies like the currently available MSS can have powerful chilling effects on critics and journalists, and can contribute to the consolidation of an autocracy without necessitating more visible forms of censorship or repression.

In line with the literature on hybridization (Diamond 2002; Levitsky and Way 2010; Mufti 2018; Møller and Skaaning 2010), and proponents of a convergence between digital autocratic and democratic practices (Gunitsky 2020), distinct regime classifications will thus most likely become more challenging in the years ahead. Widening the scope of legal surveillance frameworks that potentially cause chilling effects (cf. Lavrilleux et al. 2023; O'Carroll 2023) might also have detrimental effects in democracies on the quality of media freedoms, and the human right to privacy.

Therefore, a more nuanced analysis of how regimes use digital technologies, and how they regulate and controls (digital) information environments will be indispensable for the classification of democracies and autocracies. In the age of information, the access to alternative sources of information[53] (Dahl 1989, 108–14; 1982, 10–11) is an important criterion for a healthy democracy – now more than ever. These alternative sources, and the control thereof, are directly affected by digital technologies (cf. Maati et al. 2023; Schlumberger et al. 2023; Švedkauskas, Sirikupt, and Salzer 2020).

The resilience and quality of democracy might thus be further impaired by an expansion of digital surveillance and subsequent chilling effects on journalists. It is therefore paramount to (a) expand our understanding on the proliferation and effects of digital surveillance and repression technologies, as well as the relevant actors involved, and (b) to devise more effective global regulatory frameworks to safeguard democracy in the twenty-first century.

[53] To be clearly distinguished from concepts such as "alternative truths". Instead, access to alternative sources of information is to be understood as a healthy, pluralistic, fact-based information environment, where civilized disputes are based around different interpretations of and opinions on *a shared factual basis*, instead of a disinformative environment, where no shared factual basis exists, and uncivilized disputes are *based on competing and contradicting sets of facts and "alternative facts"* (i.e., lies).

4. How authoritarianism transforms: a framework for the study of digital dictatorship

Co-authored[54] with: Oliver Schlumberger, Mirjam Edel, and Ahmed Maati[55]

Published in: *Government and Opposition*, First View (online), p. 1 – 23; 03 July 2023;

doi.org/10.1017/gov.2023.20

Abstract

While digital technologies have induced profound global transformations, political scientists often lack the analytical tools to grasp their effects on politics. In particular, digitization's impact on dictatorships remains not only empirically understudied, but seriously under-conceptualized. How do new technological possibilities affect autocratic politics? This contribution starts from the inner logic of authoritarianism rather than from technical innovation. It first maps the ways in which autocrats employ various digital technologies to maintain power. This helps us identify seven core areas where dictatorial politics are transformed by the use of new tools. We delineate the key characteristics of these areas of change and conclude that, in their sum, technologically induced transformations significantly alter the nature of dictatorship if and when it is digitized.

[54] All authors contributed equally to this article. Ahmed Maati and Mirjam Edel developed the initial scope of the article, Oliver Schlumberger sharpened the theoretical focus on the study of authoritarianism, and Koray Saglam concretized the theoretical framework of technologically induced transformations on the political sphere. Writing, revising, and finalizing the article was done at equal parts.

[55] Acknowledgements. We would like to thank Erica Frantz, Marlies Glasius, Joseph Wright, Andreas Schedler, Nils Weidmann, Maria Josua, Žilvinas Švedkauskas and Chonlawit Sirikupt for valuable comments on previous versions of the text, and Victoria Wang for great research assistance.

4.1. Introduction

The digital revolution's massive impact on politics is undisputed. From tech giants such as Google's or Cambridge Analytica's disruptive political influence to China's 'Great Firewall', evidence abounds that digitization fundamentally changes social textures, political practices and sometimes outcomes.[56] But while some scholars view digitization as a threat to democracy and others see its potential as a prodemocratic tool for mobilization (among many others, see, e.g. Boehme-Neßler 2020; Gil de Zúñiga et al. 2010; Hindman 2009; Howard and Hussain 2011; Zuboff 2019), the impact of the digital on authoritarianism has been studied far less than its impact on democracy (notable exceptions are discussed below).

It is common wisdom that in modern dictatorships, rulers 'must contend with the omnipresent threat of overthrow' (Frantz 2018, 104).[57] But while it is well established that dictators aim at perpetuating power,[58] it is far less clear how to fully grasp the political impact of digitization in such authoritarian environments of power maintenance, and how this might change the overall face of authoritarianism. We address this gap by presenting an analytical framework for the study of digital dictatorship that helps us better understand how digital technologies influence political processes and outcomes under

[56] We distinguish between digitization as the technical process of an electronification of communication, information, and control; and digitalization as the processes this technological change triggers on the social, economic and political levels. Digitalization, then, refers to the broader effects caused by an ever-widening use of digital technologies (Urbach and Röglinger 2019). 'Digital technologies' comprise all technologies that produce or process digitized information. They differ qualitatively from analogue technologies in three ways: (1) they are reprogrammable; (2) the information they produce, and process are in universally machine-readable formats; and (3) digital technologies are self-referential in their innovativeness, i.e., digital innovations require digital devices (Yoo, Henfridsson, and Lyytinen 2010).

[57] We use dictatorship, like autocracy, as a generic term to refer to any non-democratic political regime. Below, we follow Linz, who defines 'authoritarianism' by four characteristics: (1) limited, non-responsible political pluralism; (2) absence of large-scale political mobilization from above (except in some specific circumstances), with political apathy instead; (3) absence of an elaborate guiding ideology, but with mentalities instead; (4) an exercise of political rule within 'formally ill-defined, but actually quite predictable' limits (Linz 1975, 264). For an empirical definition of totalitarianism, see Friedrich and Brzezinski (1956).

[58] Obviously, this assumption only approximates reality as humans always pursue more than one goal at any one point in time. But in authoritarianism research, it has proven useful to take the dictator's quest for regime survival and power maintenance as a starting premise.

authoritarianism, and how these transformations make digitized 21st-century dictatorship distinct from the ways authoritarianism has traditionally been viewed. Future research should hence not only examine changes in authoritarianism, but also the macropolitical regime type dimension (changes of authoritarianism).

4.2. A new framework for analysis: why and how?

After initial euphoria about digitization's democratic potential, more and more contributions now examine how autocrats instrumentalize digital technologies. Gerasimos Tsourapas (2020) and Steven Feldstein (2021) hint at digitally enabled domestic and transnational repression, while Sergei Guriev and Daniel Treisman (2019) describe how 'informational autocrats' base their rule on the manipulation of information (instead of on terror or ideology). Seva Gunitsky (2015) focuses on how social media help autocrats bolster legitimacy and gain more accurate information about their population, thereby acquiring some of the functions routinely ascribed to autocratic elections. Espen Rød and Nils Weidmann (2015) demonstrate how the internet is used as a 'repression technology' in autocracies, and Xu Xu (2020) finds that increased digital surveillance leads to more targeted repression, which in turn reduces the dictator's costs of co-optation. Others have studied the impact of new technologies on variables such as regime duration or the likelihood of protests (Frantz, Kendall-Taylor, and Wright 2020; Kendall-Taylor, Frantz, and Wright 2020; Maerz 2016, 201).

These are important contributions, and we still need more comparative and case-based empirical studies. Yet, there is a growing awareness that this emerging literature, its merits notwithstanding, lacks the theoretical embeddedness necessary to systematically relate findings about the usage of digital technologies (1) to the strategic ends of authoritarian regimes, and (2) to the transformational political effects of such new technologies. Nor does studying individual aspects of digitization necessarily tell us whether and in what respect the nature of authoritarianism transforms.

This latter question is pertinent as it remains unanswered because existing research has not operated on the level of abstraction that would allow to confer a locus to each of the contributions within the emerging broader research agenda. While Eda Keremoğlu and Nils Weidmann (2020) rightly lament the lack of a theoretically embedded framework for analysis, our contribution provides just that. Thus, this article neither represents another piece of empirical research nor does it provide a comprehensive literature

review of the emerging field. Rather, we provide a framework that enables us to better assess how digital technologies influence political processes and outcomes in autocracies.

In contrast to the recent suggestion to structure the field according to which techniques dictators employ – that is, by focusing on the new epiphenomenon of the digital (Keremoğlu and Weidmann 2020) – we hold that the link between the digital and the dictator needs to be analyzed from the other end, that is: to start from what we know about dictatorship. Only by considering the dictator's overarching logic of power maintenance that guides policies can we comprehend why and to what effect dictators[59] employ what means to stay in power. Unlike a tool-centred approach, the holistic perspective adopted here enables scholars to make statements about what exactly is changing in the nature of politics on a political (not technical) level. On that basis, it can also stimulate theory-building by linking new observations to existing knowledge about autocracies. By starting from the logic of authoritarian rule, digitization becomes clear as an intervening variable rather than being mistaken for an independent in some causal vacuum. The goal is thus to white-balance new technological developments with authoritarianism as classically defined by Juan Linz (1964; 1975); the starting point for structuring the field thus needs to be 'seeing like an autocrat', not 'seeing like a technocrat'.

We first outline the dictator's agenda of power maintenance on a meta level. This step is based on, but does not explicitly review, the vast recent literature on authoritarianism.[60] Most generally, dictators want: (1) to be informed as perfectly as possible, that is to know about what their societies and elites (i.e. their 'subjects')[61] do or plan; (2) to influence their subjects' behavior to achieve compliance so that it does not threaten their rule; and (3) to manipulate their subjects' beliefs so that their rule appears legitimate – which,

[59] While authoritarian regimes are not monolithic, and no individual always controls everything, 'dictator' is a placeholder that refers to the regime elite's perspective as a collective actor.

[60] For a good recent overview, see Schlumberger and Schedler (2020).

[61] Our framework encompasses all domestic actors who can pose threats to authoritarian regimes. Throughout this article, we use the term 'subjects' to refer to both societal/mass actors as well as to representatives of the (politically relevant) elites (PRE). For a fuller discussion see note 12.

if successful, is automatically conducive to (2).[62] Second, we move down to the meso level of technological innovation to empirically identify and categorize the new digital tools in the hands of dictators while simultaneously linking them to the latter's agenda of power maintenance. Finally, we white-balance these first two steps and thereby identify seven core areas of political (as opposed to technical) change. We claim that these areas of transformation may be constitutive (though not necessarily exhaustive) for the emerging research agenda on digital dictatorship.[63] Each of these areas is classic in the comparative study of politics and contains at least one original hypothesis to invite fresh scholarly debate in what has become a major new field of research.

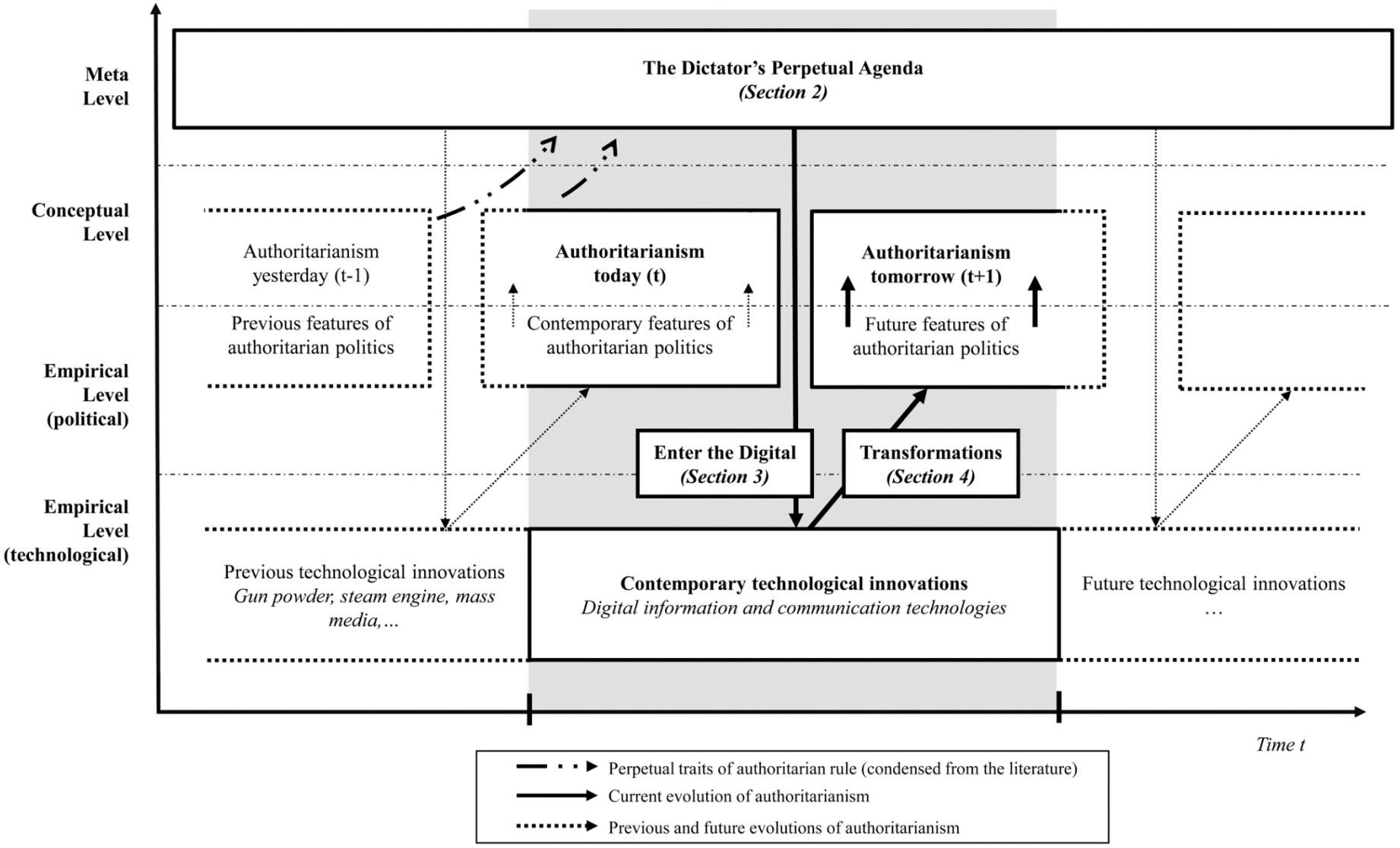
In sum, autocracies will be digitally transformed in ways that likely go beyond a mere 'authoritarian upgrading' (Heydemann 2007) or incremental modifications of authoritarian practices.[64] Rather, we witness changes on the conceptual level of regime characteristics. The idea that technology can be a defining element of political rule is not new. Carl Friedrich and Zbigniew Brzezinski (1956), for instance, defined totalitarianism as, inter alia, monopolistic control over mass media, a feature peculiar to modernity. This nexus between (autocratic) political rule and technological requisites that condition the former is important because certain regime types cannot exist without specific technologies. We argue that today we witness no less than such a technologically induced transformation of political rule in authoritarianism. As such, this is not unique, but it is historic (see boxes 'technological innovation' in Figure 5 below).

[62] Some might argue that, logically, beliefs are ahead of behavior as the former leads to the latter, but for the dictator to organize compliance, the former is much more ambitious and difficult to achieve; we therefore discuss the three goals in the order mentioned above.

[63] While we do acknowledge the importance of the international dimension of digital dictatorship, and while our analytical frame also facilitates future explorations into that dimension, it is beyond the scope of this article to include it systematically here.

[64] What Heydemann refers to as 'upgrading' has brought about incremental change in the past and concerns the invention of new tactics or strategies. In contrast, what we refer to here as qualitative, transformative change involves not only new strategies but also the accessibility and broad employment of new technology and impacts on both regime policies and the very nature of regimes. We also visualize this in the bottom part of Figure 1.

Figure 5 The argument (source: Schlumberger et al. 2023, 4)



4.3. The dictator's perpetual agenda: power maintenance

The following builds on broad and largely uncontested insights that research on authoritarianism has unearthed, rather than on any particular theoretical approach or school of thought, because the aim is to provide a general framework for analyzing digitized and digitizing dictatorship with global applicability. Theoretically, the stability of authoritarian regimes has been convincingly analyzed as based on legitimacy, repression and co-optation (Gerschewski 2013). But most research on authoritarianism rests on a yet more general implicit assumption: the dictators' desire to retain power – and in order to retain power, dictators need to eliminate threats, real or perceived.[65] To that end, they seek to control their subjects through various strategies, ranging from openly coercive strategies, positive and negative (material and non-material) incentives for compliance, divisive tactics, propagandistic rhetoric, ideology or intimidation, to name but a few.[66]

[65] One actor-centred rational-choice strand of literature (such as, e.g., Acemoglu, Robinson, Bueno de Mesquita, Przeworski or, in the study of dictatorship, Svolik) has modelled contentious actor constellations in dictatorships as a 'dual threat' to leaders: a horizontal threat from politically relevant elites, and a vertical threat from societal actors ('masses'). The assumption then is that leaders would use distinct strategies to counter each. Yet, this modelling of only three actors (leader–elite–masses) seems simultaneously too little differentiated and not encompassing (see also Schedler 2013, 34–35). As indicative evidence suggests, many (if not most) digital strategies of power maintenance such as, e.g., full-range real-time surveillance, are applied similarly to both elites and masses.

However, the main reason why we do not follow this particular actor-centred approach is that such constellations are not the same across all dictatorships. If a regime 'determines who has access to political power, and how those who are in power deal with those who are not', then such constellations by definition cannot be assumed to be uniform across regime types and subtypes, and indeed empirically, they differ in important respects not only across regime subtypes, but also across time, space, motivations, militancy, group identity, coherence etc.

Because our framework aims at applicability to all regime subtypes, we must avoid delving into the meso level of various possible actors, their varying constellations and the respective threats that emanate from them in this contribution. We thus choose to not follow the view of a 'dual threat', but instead build our analytical framework by following Gerschewski's broader approach, which, moreover, allows us also to incorporate structural rather than only actor-related factors.

[66] On democratic leaders entertaining similar desires and on authoritarian practices in democracies, see note 16.

One can now link the classical pillars of legitimation, repression, and co-optation to general authoritarian objectives: co-optation and repression directly stem from the objective of influencing behavior. Aspirations to generate legitimacy originate from dictators' desires to influence the beliefs of their subjects. To pursue their agenda, autocrats thus need to do three things: they must (1) know about potential threats, rivals, grievances and the effectiveness of their strategies. To address threats, they need (2) to influence the behavior of their subjects; and, simultaneously, (3) to influence their beliefs.[67]

First, dictators need to gather as much information as possible on subjects in order to recognize threats. To control and manipulate behavior and beliefs effectively, accurate knowledge about who potential challengers are and what they plot is essential. Knowing (what people think, do, or plan) is thus a basic requisite that logically precedes the control and manipulation of behavior and beliefs. Most 'strategies of knowing' focus on identifying opponents and finding out what they do or plan. Strategies to assess prevailing beliefs more accurately traditionally include elections as 'opinion barometers'. Once information is available, incumbents dissect, analyze, and interpret it to respond appropriately to challenge(r)s.

To pre-empt threats, incumbents directly influence people's behavior. Most prominently, they do so through repression: by restricting unwanted activities physically or legally, or by raising the costs of contention. Repression thus entails negative incentives and sanctions. But autocrats also set positive incentives for compliance by offering avenues of co-optation to selected groups. Divide-and-rule strategies combine positive and negative incentives. They aim at fragmenting potentially threatening opponents so that competing groups keep each other at bay. Thereby, dictators can prevent or eliminate threats but sometimes they act too late or inexactly – which hints at another important path to control behavior.

Less open than directly controlling and manipulating behavior, but potentially more effective, is to control narratives that shape subjects' beliefs. By altering and controlling narratives, authoritarian regimes render the populace oblivious to its oppression. In academic terms, such manipulation intervenes in the causal chain and in turn causes behavioral changes. Ideally, orders become unnecessary when compliance becomes voluntary. Nobody contending for power would reduce the costs of repression and, ultimately, of power

[67] These three components of the power-maintenance agenda are interrelated and, in part, even endogenous to one another. Nonetheless, for the purpose of this article, we treat them as distinct, non-hierarchized elements of power maintenance.

maintenance. In an autocratic utopia where all people always believed the regime's narratives, coercive apparatuses would be superfluous.

We differentiate between 'constructive' and 'destructive' means to influence beliefs and opinions. First, the construction of narratives occurs in two forms: either governments create and perpetuate narratives themselves (through propagandistic speeches, state-owned media etc.) or they promote pre-existing narratives by selectively sharing content. By promoting a certain picture of reality, such as by granting pro-regime news more coverage in regime-controlled media, autocrats can marginalize undesired narratives. But they also actively engage in campaigns that produce false 'news' and 'alternative facts' that deliberately create regime-orchestrated (untrue) narratives. Second, incumbents have 'destructive' means to marginalize undesired information and counter-narratives: the production and proliferation of content is restricted via censorship of the various media. If it has already spread, unwanted information is discredited in public statements and regime-controlled media, or their producer (e.g., an opposition group or army general) is defamed to render the source untrustworthy (Table 8).

Table 8 The dictator's agenda (source: Schlumberger et al. 2023, 6).

Control subjects					
Know		**Influence beliefs**		**Influence behavior**	
Collecting information	Processing information	Constructive: through creation and promotion of narratives	Destructive: through discrediting and censoring narratives	Negative incentives and sanctions (mostly repression)	Positive incentives (mostly cooptation)

4.4. Enter the digital

Dictators remain, as always, interested in controlling their subjects, but digitization provides them with a plethora of new opportunities to pursue their goals of knowing, influencing beliefs and influencing behavior.[68] Contrary to others, we explicitly broaden the view beyond the 'internet' and 'social media'.

[68] Actors in democracies, too, engage in digitally enabled authoritarian practices (cf., e.g. Glasius 2018c). But in democracies, control and surveillance are structurally constrained by basic civil liberties (privacy rights), in combination with political guarantees such as an independent judiciary (rule of law). While authoritarian practices in democracies

Digital technologies also include advanced digital devices and programs that, assisted by automatized machine-learning, allow for digitization, analysis, and response by the regime. This section provides a comprehensive screening of the digital techniques most commonly used by dictators and illustrates their respective – often multiple – purposes; we thereby show how they relate to the dictator's power-maintenance agenda.

4.4.1. Techniques to know

These are digital techniques for gathering and analyzing information. While we separate the two analytically, they are usually employed iteratively: the analysis of information usually leads to better collection and vice versa.[69]

2.4.1.1. Gathering information

Dictators use four sets of digital techniques to collect information: (1) obtaining user data from service providers, for example through respective legislation; (2) installing additional hardware (data probes, surveillance cameras and other eavesdropping devices) in public spaces, on terminal devices or on the infrastructure such as national gateways;[70] (3) obtaining data directly from users, either through deceptive means or by users voluntarily revealing information through interaction with specific digital applications (e.g. entertainment services, emails or websites) or through interaction with official government websites; and (4) malware and hacking.

First, internet service providers (ISPs) are subject to local laws and forced to provide data to authorities if requested. This applies to all countries, but in most autocracies, legal processes are not

constitute flaws of the system, they are integral to the modus operandi of dictatorships. Consequently, in democracies, scandals such as the one in 2018 with Cambridge Analytica or the NSA in 2013 result in public debates, new legislation for data protection and/or lawsuits.

[69] This is particularly visible in face-recognition technology that simultaneously collects and analyzes information.

[70] Gateways are entry points that connect devices outside a network with devices inside a national network and facilitate their communication.

independent of the dictator's power-maintenance agenda, and privacy rights remain unenforceable. Data thus acquired contain basic information, such as the frequency of visits to specific websites, but can be more detailed if the service provider uses hardware data probes (see below). Information is also requested from international companies such as Facebook, which argues that it 'responds to government requests for data in accordance with applicable law and [its] terms of service'. Between January and June 2019 alone, Facebook responded positively to over 85 data requests by authoritarian regimes, among them Jordan (Facebook 2019a).

Second, hardware eavesdropping components are implanted in digital devices such as smartphones to surveil the in- and outbound traffic of that device. These hardware components are either designed specifically for surveillance (e.g., spy microchips) or manipulated to also serve the purpose of surveillance, for example when sim cards and GPS locators are used to collect information about users' locations and activity. Data probes are hardware components that are installed on national internet cables connected to government-owned servers. They screen all internet traffic passing through the national network and store all thus surveilled internet data on large government servers to be later analyzed by computer programs. Russia uses such probes as part of its surveillance program SORM-3 (Lewis 2014).

Third, autocrats also deceive users through phishing campaigns to steal their identities, such as login credentials for social media, email or bank accounts. State officials send links that direct users to fake websites that resemble legitimate or known ones. Entered usernames and passwords are then stored on a government server.

Moreover, dictators have also learned how to incentivize users, that is, to either force users to accept specific cookie settings or browser certificates and actively share their personal and/or device information, or by luring them, sometimes via private companies that subsequently share the data they collect with autocratic regimes, into voluntary sharing such information. For example, the Kazakh regime attempted to force all internet users to install a government browser certificate that allows the government to see the interaction between digital devices and websites unencryptedly (Mozilla 2019). By digitizing government services, governments can create centralized data banks of their citizens that digitally code all bureaucratic steps that individuals take and, in extreme cases, record every daily action of targeted individuals. These are also data sources that are used – for example, in Chinese provinces where social credit systems have been implemented to inform a digitally assisted assessment of subjects from the standpoint of the Chinese regime

(Kostka and Antoine 2020; Xu, Kostka, and Cao 2022).[71] Online entertainment programs on social media can also be used to gather information.

Fourth, malware and hacking are the most sophisticated and intrusive techniques of data gathering. Spyware collects information from users' devices and sends it to a government server. One infamous example is a program named Pegasus. The Israel-based NSO Group Technologies claims that it sells the program exclusively to law-enforcement agencies (Kenyon 2019). Unsurprisingly, CitizenLab reports that various authoritarian regimes have used the program to target political dissidents. Like other malware programs, Pegasus copies files from the victims' device and sends them via the internet to a server accessible to the surveillance agency. It is also able to delete files and to destroy the infected device. Without the user noticing, malware programs can switch on cameras and microphones on end-user devices, turning them into live spying machines (Cannings et al. 2017)

2.4.1.2. Analyzing information

Authoritarian regimes analyze information with computer programs that can access, sort and analyze the vast amount of data gathered. Some software, such as SolarWinds NetFlow Traffic Analyzer, is commercially available. The capacity of such analysis programs to process data is impressive, and opaque, as the algorithms produced and sold to dictatorships – also by Western companies – are often dual-use technologies. Algorithms developed for identifying cancer cells, for instance, can also be used for face recognition.

[71] These systems are operated on a provincial level and include private and public operators with varying degrees of sophistication and extent – all ultimate authority to control private sector operations, however, lies with the regime. Other than in Western contexts where Google and other large companies could be said to de facto control access to the data they collect, ultimate 'allocation of values' in places like China is firmly in the hands of the top regime elite, not of any private company. Moreover, it is clear that the Chinese regime is working hard to integrate and streamline hitherto separate systems of assessing individuals' behavior (Drinhausen and Brussee 2021). This bears fruit, as could be seen, for instance, during the COVID pandemic when police-operated 'talking drones' were used across various provinces to, first, digitally identify, and second, directly address subjects through the drones, telling them to wear face masks or to stay at home (cf., e.g, D'Amore 2020).

Second, regimes also program social media bots to analyze, detect and collect content that regimes deem critical. These algorithms can spot, screen and report critical posts, pages, and users, but are also used for additional purposes in digitized dictatorships (more below).

Finally, autocrats use techniques that are not particularly 'digital' to analyze 'big data'. Innovations in psychometrics have allowed Cambridge Analytica to analyze data gathered from over 50 million Facebook users to – among other things – craft personalized voting campaigns. The analysis relied on Facebook profile information, including 'likes' to specific pages and posts, to create personality profiles.

4.4.2. Techniques to influence behavior

New ways of collecting and analyzing information are not ends in themselves, but they allow the autocrat to decide on the choice of digital (and non-digital) techniques to influence behavior.

2.4.2.1. Digital repression

While dictators routinely use digitally collected information to repress subjects in the offline world (Kendall-Taylor, Frantz, and Wright 2020, 108), this section focuses on techniques of digital repression – that is, techniques of repression targeting digital devices or platforms, regardless of whether this extends to the offline world or not.

Dictators use two techniques to repress digitally. First, they deny users access to online services such as social media profiles, personal or corporate websites or specific communication platforms. Authoritarian regimes utilize their jurisdiction over service providers and pressure international companies to block or delete specific accounts, services, or websites. Alternatively, autocrats can deny access to websites and services by blocking access to their IP addresses from within national borders, or digitally attack specific websites in so-called denial-of-service (DOS) attacks.[72] Russia, for instance, domestically blocked Telegram after the latter had refused to provide the state with all encrypted conversations (Dans 2018).

[72] Internet bots repetitively and simultaneously connect to the victim's server and thereby bring down the whole service by exhausting its capacity, as China did against Telegram during the 2019/20 protests in Hong Kong.

Second, dictators target specific individuals and organizations with malware computer programs that destroy devices or steal sensitive data (e.g., private photos) to repress opponents across borders. Malware programs often overlap with surveillance programs (spyware), which also have a transnational reach. A case in point is, again, Pegasus, which has been used to destroy subjects' digital devices outright.

2.4.2.2. Digital co-optation

The most prominent examples in this area are China's social credit systems. In provinces where such systems are in place, citizens' scores are tied to a virtual account for each person.[73] The score reflects the gross evaluation of an individual's activities. Information surveilled and analyzed includes offline behavior through public surveillance cameras in combination with face recognition, but also online behavior that is comprehensively surveilled because clients are forced to use accounts that are tied to their individual social credit account. This score, in turn, not only reflects behavior, but also determines behavior, as certain privileges must be earned, such as bank credit (including terms and conditions like interest rates), permission to travel internationally, permission to fly, permission to access social media, and even to access the internet as such (Drinhausen and Brussee 2021; Kostka and Antoine 2020; Xu, Kostka, and Cao 2022). The range of positive incentives for compliant behavior is thus very broad and includes most of what subjects consider modern life (Data Justice Lab 2020, gives a complete list). It is true that these systems are not yet implemented across all Chinese provinces equally and coherently; they still require human agency, and do not (yet) result in one coherent central data set that could be analyzed in real time. Yet, the existing systems demonstrate the technical capacities that autocrats can utilize for surveillance and for granting or

[73] China, by far the most advanced digital dictatorship with its social credit systems, delineates a conceivable ideal type – and thus is a suitable example when contemplating trends. Note that we do not claim that all dictatorships, including China, are able or willing to fully establish such an ideal type. Still, the ambition to control, surveil and manipulate digitally is present in virtually all dictatorships that experiment with the purchase and development of digital power-maintenance tools. While China highlights the current scope of tools available to the digital dictator, other dictatorships rather install piecemeal digitization and so far focus on specific dimensions they deem particularly important for their own survival. Likely, we will see different 'digital profiles' emerge among the universe of digitizing dictatorships. Our illustrations here stem from across the world to ensure that our framework and conclusions are not based on any particular case.

withholding rights and privileges (Drinhausen and Brussee 2021). As to its effects, thus, it makes sense to conclude that in the eyes of the subject, it is the political leadership who grants the benefits of modern life and for which it can expect gratitude and compliance in return – while they can be withdrawn from ungrateful subjects.

4.4.3. Techniques to influence beliefs

2.4.3.1. Pro-regime propaganda

One way to establish pro-regime narratives digitally is to use traditional propaganda techniques on government-owned websites. Apart from the important information-gathering function discussed above, another reason why authoritarians digitize public services is that e-governance can not only carry propaganda messages, but also serves to promote a legitimizing image of advanced regime performance (output legitimacy). By advancing e-governance, autocracies legitimize their rule by painting a digital façade of participation and responsiveness (Maerz 2016). Unsurprisingly, thus, authoritarian regimes invest particularly heavily in e-governance – but for reasons very different from international donor intentions. Another way is to employ social media bots to create and spread pro-regime narratives. These bots pretend to be humans on social media. They comment, like, post and share content. Russia, China and the Middle East are but some of the locations where 'bot armies' are extensively used to spread regime propaganda (cf. Jones 2022; Oxford Internet Institute 2021).

As Russian interference in the 2016 US elections demonstrated, target audiences of digital propaganda campaigns are not exclusively domestic. National and international digital disinformation campaigns include the creation of fake news through bots or trolls (humans who create content of the aforementioned sort) not only to influence opinions and beliefs, but also to instil scepticism about truth more generally.

Censorship and discreditation

One core feature of authoritarianism is the restriction of 'access to alternative sources of information'.[74] Digital technologies allow autocrats to censor online content more effectively and less expensively than manual censorship. Digital censorship includes, first, the cooperation of online service providers to remove content and pages deemed critical by the regime and, second, the direct blocking of websites, as happened to Wikipedia in Turkey because it had informed about corrupt government officials. Third, bots also censor online content. These algorithms can be programmed to automatically detect and block webpages that contain critical keywords or content. The Chinese Great Firewall combines numerous algorithms to filter and block critical content automatically (Arthur 2012).

Social media bots can also be programmed to defame and discredit opponents, as well as to influence news coverage. Bahrain, for instance, employed such bots during the 2011 uprisings to 'troll' posts and pages of political opponents (Jones 2019).

The most drastic digital censorship is to shut down the internet altogether, regionally, or nationally, to prevent international audiences from getting information about regime crackdowns on opposition. When, in 2019/2020, the Iranian regime killed over 1,000 people in a crackdown on demonstrations, it was hardly covered by international media, nor did it trigger political reactions as it was conducted during an ordered internet shutdown.

As with information gathering and processing, dictators' capacities to control national and substantially influence international public discourse have vastly increased with digitization; accordingly, so have their abilities to influence what their subjects believe.

Trade-offs between the various strategies where the use of one might undermine the other have existed before digitization and continue to exist. But such trade-offs seem to be ameliorated by digitization in various ways. For instance, while one might think that more effective censorship of public discourse would deprive regime leaders from useful information, the opposite seems more likely because, while

[74] Note that this is one of Dahl's 'eight institutional guarantees' in his definition of polyarchy (Dahl 1971, 3).

'public' discourse is censored, digital technologies enable rulers to access potential dissidents' private discourses on all levels of electronic and offline communication.[75]

4.5. Transformations of political dynamics in authoritarian regimes

We now discuss how digital tools affect the dictator's perpetual agenda. Only when viewed against the backdrop of literature on authoritarianism does it become clear, however, that many of the integral elements of authoritarianism are affected by digitization. If we understand 'political regime' as 'the formal and informal organization of the centre of political power, and of its relations with the broader society' (Fishman 1990, 428), digital transformations affect not only the 'three pillars' of 'authoritarian stability' (Gerschewski 2013), but important core features of how regimes form, are composed and institutionalize, including state–society relations. Their effects thus transcend incremental enhancements of existing dictatorial ruling strategies and capacities.

This section discusses seven key areas where digitization transforms authoritarianism because of regimes' unprecedented abilities to collect and analyze information about subjects, and to influence the latter's beliefs and behavior. For each, we provide testable hypotheses on how politics is transformed by the dictatorial use of digital tools. While these areas of transformation are not necessarily exhaustive, they are common fields in research on authoritarianism. Their discussion helps in assessing more precisely on what level and to what extent political transformations occur due to technological innovation, and how this influences the overall face of dictatorship.

4.5.1. New elite actors and partially reconfigured regime composition

Operating the new tools requires higher levels of technical expertise from regime agents. Domestically, new 'cyber elites' are already emerging (see also transformation 2, below), while, at least in the short run, regimes also rely on foreign commercial services to install, maintain, and operate their tools. Some of the traditional

[75] Moreover, as one anonymous reviewer suggested, technological innovation can also bring synergy effects such as in China, where regime-initiated discourse influences belief formation in ways conducive to citizens' willingness to voluntarily provide private information and comply with surveillance policies.

elites' importance will decline because digital technologies increasingly assume their tasks. Simultaneously, the more digitized autocracies become, the more cyber elites will gain in influence. For instance, directors of security services' surveillance directorates, formerly in command of huge bodies of informants, may be marginalized as the collection and real-time analysis of big data are performed by self-learning algorithms, the administration of which the old guard of elites cannot perform due to lack of digital expertise. Fewer and very differently qualified personnel are now needed in extremely sensitive positions, and such new elites may also be recruited internationally (see also transformation 7 below). Agents of digital repression, co-optation and propaganda already occupy a prominent place in newly installed institutions (more below). Beyond such formal positions, elites are also reshuffled in more informal and secret positions. In any case, these reconfigurations in the composition of, and power dynamics within, autocratic elites can impact authoritarian politics in important ways. Changes in the relative importance of some elites and changes in elite circles that can access and control information might impact intra-elite composition and coordination, and possibly create new challenges to the rulers (e.g. principal–agent issues).

So far, little research has examined these changes, nor how they fit into existing theories of autocratic elite coordination, formation, or recruitment. It remains for future research to investigate the sociopolitical and economic ramifications of such changes to elite composition/configuration in authoritarian regimes – especially since some major works on authoritarianism view elite coordination and power dynamics as pivotal in understanding the politics of authoritarian regimes (stability).

4.5.2. Institution-building and -reconfiguration

Large data-gathering and data-analyzing techniques can reduce or erode previous functions of more traditional dictatorial political tools. For instance, public opinion is continuously screened and known by dictators when they employ sophisticated data analysis programs. Rulers then no longer need to rely on elections as a barometer of public opinion, and we concur with Gunitsky (2015, 43) that with a 'potential substitute for unfair elections', such institutions lose part of their function.

When autocratic institutions change functions as dictatorships digitize, it represents important institutional shifts. We therefore expect autocracies competent in digital surveillance to rely less on elections for finding out about their population's political preferences. Such losses of function could lead us, prima

facie, to assume a decrease in the frequency or importance of elections in authoritarianism, but they also serve purposes other than testing regime popularity.[76]

Digital capabilities can also supplant existing dictatorial tools. Enhanced surveillance capacities enable autocrats, in combination with bot armies and other defamation and control instruments, to better predict voting behavior. If Cambridge Analytica became infamous for digitally distorting democratic elections, it would be naive to assume that autocrats would not apply similar strategies to influence and control votes at home. The electoral process hence becomes more predictable for authoritarians and yet less promising for oppositional forces. This might motivate autocrats to rely even more on elections for generating legitimacy and could thus lead to an increase in their frequency or centrality. The increasing popularity that pseudo-democratic elements such as referenda enjoy among modern autocrats seems to point in this direction.

Institutional change beyond elections includes, for instance, new political institutions established as reaction to technological change. Examples are the 2013-founded Chinese 'Cyberspace Administration' that reports directly to the president (Polyakova and Meserole 2019, 3), the Iranian 'Cyberspace Supreme Council', established in 2012 and staffed mostly with security personnel (Reporters Without Borders 2020), or the various bodies for supervising new processes of e-governance that most autocracies have recently established, and which are staffed, inter alia, with the above-mentioned new cyber elites. As discussed above, e-governance not only enhances autocrats' 'performance legitimacy' but also enables them to engage in 'imitative institution-building' when they establish democratic-looking façades (Albrecht and Schlumberger 2004). Yet, imitative institution-building might become less important in digital dictatorships. We therefore hypothesize (a) the emergence of new, now functionally necessary dictatorial institutions, and (b) a change in the nature, functions and potentially also shape of existing 'imitative' institutions' that mimic their democratic counterparts.

[76] On why dictators hold elections when results are known ex ante, see, e.g. Gandhi and Przeworski (2006).

4.5.3. The intension of political rule: reconfigured state-society relations

While the consequences of a new digital public sphere are debated (Schäfer 2016), the distinction between the public and private spheres becomes blurred. Where private activities, preferences and conversations increasingly take place digitally, regime capacities to penetrate private life increase. The more the private takes place online (e.g., via social media or messenger services), the more it becomes at least susceptible to 'publicization', and ultimately part of the public sphere.

The depth to which society can now be digitally penetrated is unprecedented, and the intensity of 'knowing' and, subsequently, manipulating beliefs and behavior exceeds even what 20th-century dictators could have dreamed of. Big data analyzes give incumbents the power of real-time mass surveillance and, simultaneously, of targeting an almost unlimited number of individuals more specifically. This leads to a thorough reconfiguration of state–society relations: whereas rulers remain in opacity, subjects become more transparent than ever. Oppositional activity is often detected in the planning stages before it occurs – because incumbents know.[77] In many dictatorships, incumbents now implement tools of digital surveillance to pre-empt open contestation. With digital surveillance perfected, we will hence see fewer mass demonstrations.

Some argue societies would counteract by likewise acquiring digital skills and thus creating new challenges to autocrats (Hobbs and Roberts 2018). Yet, this view fundamentally ignores the qualitative imbalance in power resources between societies and dictators in which the asymmetry between the two allows the latter not only to control but also to determine the digital possibilities of societal forces. While opposition movements do have learning capacities, these invariably depend on the regime-installed hardware to which access is controlled by incumbents, and on the regime's monopoly to control access to software. Ultimately, therefore, opposition is thus much more restricted and has fewer opportunities to coordinate than before digitization. This point has been empirically confirmed in a large-n study by Weidmann and Rød (2019, chapters 5 and 6), who call it the 'protest-reducing effect of internet technology'

[77] This does not mean that no errors occur. Apart from human miscalculations, certain types of errors are innate in the digital tools themselves (e.g., misidentification of individuals by recognition software). Yet, such errors become fewer through machine learning in self-optimizing systems.

(Weidmann and Rød 2019, 155). It is our framework that explains the causes behind that increasing imbalance.

While it is still too early to predict exactly how contentious politics will further evolve, this is one central theme to understand state–society relations in 21st-century dictatorships. What is certain today is that digital techniques have empowered authoritarian incumbents much more than their societal opponents. While popular movements have been able to make use of digital techniques to mobilize, such opportunities vanish rapidly as authoritarians become more digitally capable than most still were in the 2000s and 2010s when the room for online contention was still large. In the 2019 Hong Kong protests, the Telegram-based organization among participants was highlighted. But it was only in combination with a new type of offline protest tactic ('be like water') that authorities had a hard time in handling protesters. This is just one example of how activities in the online and offline world blend. Such innovative crossings are likely to become more prevalent in the future, as might be opponents' tactical withdrawal into the analogue world when digital surveillance becomes omnipresent (as long as there are physical spaces that are not covered by real-time facial recognition and CCTV). Clandestine acts of resistance then likely outpace open political opposition or visible activism.

4.5.4. The reconfiguration of coalitions and micro-steered co-optation

New tools of digital co-optation alter the ways of authoritarian coalition-building. Co-optation of either particularly loyal followers or of would-be opponents has now become much more individualized. Traditionally, different collectivities (i.e., classes, segments or elite groups) are both the building blocks and main beneficiaries of authoritarian coalitions and their welfare provision (Eibl 2020; Slater 2010). E-governance and social credit systems individualize both the criteria for inclusion into authoritarian social pacts and the benefits of social welfare. Instead of including or excluding societal segments, incumbents can target specific individuals based on their (online) behavior as 'social-credit scores can determine the results of applications for personal loans, jobs, visas, and more' (Qiang 2019, 59). Given this ability to fine-tune inclusion and exclusion independently of group identities, regime coalitions as well as the relationship between different elite segments might look different in the future.

Even basic citizenship rights become contingent on subjects' 'well-behavior' (theoretical reflections: Heydemann 2020). We expect the widespread use of reward–punishment systems such as China's social credit system to affect the ways authoritarian coalitions evolve and are sustained. For some regimes, such systems will reduce the costs of rule by narrowing down the group of beneficiaries as exclusive benefits (and costs) can be delivered with surgical precision to the intended individual recipient instead of to larger groups. Other regimes might diversify their coalitions to include individuals from different societal segments rather than by co-opting larger groups. This may increase loyalty and leader–elite-cohesion, thus further reducing threats to the regime (see transformation 3 above). We assume that resource-rich authoritarian regimes might tend to keep previous elite coalitions intact whereas resource-poor autocracies might narrow down such coalitions more quickly.

4.5.5. The frequency, forms and targeting of repression

With the spread of bots, digital attacks and malware, authoritarian regimes enjoy an unprecedented ability to know about their population, censor information and destroy opponents' digital devices. This allows digitized dictators to fine-tune and target repression. First, the regimes' ability to know enables them to better identify threats and employ repression with surgical precision, as Feldstein (2021) convincingly illustrates. Second, regimes can censor and destroy regime-critical content more easily, more systematically and more precisely. We discussed Bahrain's use of social media bots to censor critics as well as China's Great Firewall. Such measures enable the targeting of specific critical content instead of enacting bans of entire social media, let alone a total internet shutdown (a Syrian routine in the 2000s). Furthermore, as India and South Africa, albeit democracies, demonstrate, regimes are today able to shut down the internet or to throttle the bandwidth in a very targeted manner (Farries 2019, 13), which effectively blocks avenues for opponents' coordination.

The consequences of such repression deserve closer attention. Intuitively, more targeted repression seems to reduce both its undesired side-effects and its costs (Feldstein 2021) and would increase regimes' willingness to repress. Yet, we also noted that autocrats today better pre-empt opponents from gathering and even coordinating. The International Network of Civil Liberties Organizations reports the extent to which the governments of Kenya, Russia and Hungary use digital surveillance to curb protests before they

are even called for (Farries 2019, 8) – which in turn helps avoid the large-scale repression that would be necessary if such protests materialized. When domestic mass contention becomes thus less frequent (transformation 3), so does potential international damage to the regimes' legitimacy. Dictators increasingly 'shy away from overt and highly visible forms of coercion and turning to subtler techniques that are less likely to spark outrage and condemnation' (Frantz 2018, 120), and the cause for that might well lie in the vastly increased levels of 'knowing' that allow for more targeted repression, if necessary at all.

4.5.6. Legitimacy and informational agnosticism

In the analogue age, readers had a choice between, say, the state's official gazette and alternative newspapers that could deviate from the regime's official narrative within 'accepted lines'. Readers were usually aware of whose voice they were exposed to. Digital tools to influence beliefs fundamentally blur this distinction between pro-regime and regime-critical information sources because nongovernmental information channels are systematically infiltrated (Kelly et al. 2013, 4). Information looks as if it is derived from a diversity of sources while in fact it consists of different regime-initiated discourses. For incumbents, it is not necessary to allow only one voice to speak. They just need to sow enough disinformation to make the opposition appear slightly less legitimate than the regime.[78] For example, during the 2011 Bahraini uprising, social media bots retweeted and posted pro-regime narratives without officially belonging to the regime (Jones 2013, 78–79). Even before bots became ubiquitous, Russia initiated and financed private 'brigades' to change online narratives (Polyanskaya, Krivov, and Lomko 2003). The Chinese regime forges 448 million social media comments a year to 'distract the public and the change the subject' away from controversial political issues (King, Pan, and Roberts 2017).

With regimes creating and disseminating their own 'truths' through, among other things, social media, dictators have drastically expanded their capacity not only to obscure the origin of news and narratives, but also to render citizens structurally unable to identify the source of 'information' they consume or to judge its trustworthiness. Thus, confounded subjects cannot know what news to trust nor whether rulers protect or manipulate them. Deeply manipulated rationales of knowing lead to equally distorted

[78] We thank Marlies Glasius for hinting this point to us.

rationales of obedience – which might, in turn, transform how the Weberian belief in legitimacy itself is garnered.

Moreover, ignorance about who stands where leaves potential dissidents within masses and elites uncertain about their relative strength, rendering collective action less likely. This is a qualitative break from anything seen in earlier times, and it might become the tool to create almost perfect ignorance about truth and falsehood. As psychologists have demonstrated since the 1960s, this pushes subjects not only into a state of ignorance about reality, but into political apathy and carelessness about the origin of the news they are fed. Mutually exclusive narratives translate into a general suspicion against media, even in democracies. Such authoritarian practices intentionally work against the very concepts of truth and reality; among subjects, they create not only an informational gap, but also informational agnosticism. This is particularly frightening because 'access to alternative sources of information' (Dahl 1971, 3) is a core requisite for democratic contestation. Where citizens are unable to discern the very source of their information, they lack the prerequisites of forming an independent opinion. We hypothesize, therefore, that digitized authoritarians will successfully broaden the base of those who buy their narratives and yet more successfully marginalize critics. The decisive point is not whether citizens are convinced of the truthfulness of regime narratives. The uncertainty instilled upon society is enough for most to not engage in searching for truth because 'truth', under these conditions, cannot be known anyway.[79] This enhances the dictator's ability to manipulate beliefs while simultaneously decreasing prospects for democratization.

4.5.7. The extension of political rule: the transnational reach of power

Digitized dictatorship changes the features and the scope of political rule, both in its intension (see transformation 3), but also in its extension. The latter becomes clear when we look at what traditionally constituted national borders. All three 'pillars of stability' (Gerschewski 2013) today routinely transgress

[79] This psychological effect is long known. Saloojee and Dagli (2000, 903–4), for instance, report on collusion within the US tobacco industry in the 1950s when reports about smoking as a health hazard emerged. In an internal memo, the colluders strategized, 'doubt is our product. Spread doubt over strong scientific evidence and the public won't know what to believe …. It's enough to foster and perpetuate the illusion of controversy in order to muddy the waters.'

borders much more quickly and at less cost than ever before, adding a transnational dimension to the transformations discussed under transformations 4 to 6.

A case in point is the remote surveillance of opponents abroad: agents are no longer needed to spy on exiled opposition leaders. The case of London-based Saudi satirist Almasarir exemplifies this.[80] In many cases, this digitally enhanced capacity to know, in turn, enhances the capacity to physically repress in the offline world and instils fear among regime critics. Some question whether this successfully silences all critics (Pan and Siegel 2020; Roberts 2020), but empirics suggest that the existing power gap between dictators and their critics increases to benefit the former (King, Pan, and Roberts 2013; see transformation 3 above). Azeri journalist Khadija Ismayilova was secretly filmed in her home and blackmailed with the material before it was spread online, ultimately leading to her arrest (Reporters Without Borders 2018, 10). The unprecedented ability to surveil critics anywhere intimidates exiled opposition. Rwandan deputy Faustin Rukondo, targeted by a WhatsApp Pegasus attack in 2019, felt 'paranoid and scared' (Tidy 2019). We hypothesize that authoritarian regimes, alongside increasing transnational surveillance capacities, also increase their capacities to repress targets abroad.

Digital tools of repression thus enable autocrats to better target and silence even exiled opponents (Dalmasso et al. 2018). Rukondo was not only internationally surveilled, but the same Pegasus malware also destroyed files on his mobile phone (Tidy 2019). Private Russian agencies directly tied to the president orchestrate troll armies that attack targets worldwide, as with Finnish journalist Jessikka Aro or during Emanuel Macron's campaign for the French presidency in 2017 (Reporters Without Borders 2018, 23–24). State-sponsored online harassment and hate speech against critics are also well documented (Michaelsen 2020) and acknowledged by international organizations such as the European Council.

Beyond surveillance and repression, co-optation also increasingly occurs transnationally. One example is the recruitment of international tech experts of questionable ethics, often hired on a one-off basis, but sometimes also lured into long-term contracts with autocracies. Different from the international advisers whom dictators have always had, such experts are located at the most sensitive points of domestic security infrastructures, which could result in ramifications on the inner dynamics of authoritarianism.

[80] Saudi security forces had hacked Almasarir's phone with the Pegasus spyware. For similar cases, see Middle East Monitor (2019).

Furthermore, rulers' efforts at legitimizing their hold on power increasingly target not only a domestic audience, but international ones too. Alongside elaborate disinformation campaigns through traditional state-controlled international media (such as Russia Today or Sputnik News), new media have been particularly successful in spreading favourable 'news' about autocracies abroad. This allows dictators to paint a positive picture of their regimes to domestic and international audiences alike. The international delegitimization and defamation of rivals and adversaries are closely related. Dictatorial great powers such as Russia perceived the world to be in a state of cyber war about (mis-)information even before the war in Ukraine, aiming at internal and external legitimation (the 'Gerassimov Doctrine'). However absurd the 'news' that troll firms disseminate might seem, they likely find followers who multiply their messages and create echo chambers so that uncertainty about truth is propelled even beyond
national borders.

Taken together, then, digitization significantly transforms the political process in various dimensions.[81] Each of these areas awaits more systematic empirical research that we hope to encourage by the discussion and hypotheses presented here. Overall, we can safely state that digitization makes autocracies faster in their responses to threats, quicker and more targeted in both surveillance and repression, and more versatile in the creation of tailor-made 'truths' for targeted audiences – in brief: authoritarianism on steroids. All this points to what Steven Heydemann (2007) called 'authoritarian upgrading'. But the whole can be more than the sum of its components. We are convinced that the combined weight of these transformations amounts to more than just changes in degree. By contrast, we argue that above and beyond the discussed transformations of the political process – that is, in the sphere of politics – we also witness transformations that affect regime type – that is, polity. We conclude this article by suggesting that digitization produces a kind of political rule that, while dictatorial, also differs in important respects from authoritarianism as classically defined.

[81] These seven areas can interact: new or altered forms of repression potentiate the transnational reach of authoritarianism; new cyber elites can dilute or highlight the importance of different security agencies (institutions), and reconfigured regime coalitions surely affect state–society relations and contentious politics, which in turn impacts on forms of repression, and so on. Digital technologies' ability to simultaneously serve several elements of dictators' perpetual agenda gives dictators an edge in steering these interactions to their favour.

4.6. A technologically induced transformation of authoritarian politics

Condensed from the existing literature on authoritarianism, but in contrast to most contributions on digitized dictatorships, we started our argument from the 'dictator's agenda' in studying dictatorships instead of from the technological side. Proceeding thus enabled us to treat digital innovation in ruling techniques as the intervening variable it is. Technical innovation provides autocrats with new tools – tools they not only embrace but actively develop in order to better pursue their political goals, and which strongly impact on the way autocratic politics work. Thus, while the goals of authoritarianism remain constant, the means by which dictators pursue them are fundamentally transformed in ways that rapidly increase dictators' capabilities of controlling, surveilling and manipulating the attitudes and behavior of their societies – despite all societal or oppositional efforts to the contrary. This is because resources available to societal forces are to a large extent determined by regimes' exclusive power over hardware and regulations that circumscribe the availability of digital means of resistance available to oppositional forces.

The seven core areas of transformation identified above can be understood as an analytical frame that helps both in locating current and encouraging future research within the broader field of digitized dictatorships, and in identifying areas where future research is particularly desirable. But change might not stop here: the combined impact of these transformations leads to profound changes not only to the process of how authoritarian politics – including politics aimed at authoritarian stability – functions, but in consequence also to the very nature of authoritarianism. Far from a distant techno-sceptical dystopia, the Chinese case demonstrates just how different from authoritarianism as traditionally defined (cf. Linz 1964; 1975) new, digitized autocracies can already look today. While, for reasons that go beyond the scope of this contribution, we do not share Larry Diamond's (2019) view of a 'postmodern totalitarianism' on the horizon, empirical trends in the direction of a more total than ever control and surveillance are evident. Further research should therefore not only focus on transformations in authoritarian politics, but also broaden the view and include the possible transformation of authoritarianism as a distinct regime type as well.

5. Information doubt and decay: how digitization spurs democratic decay

Co-authored[82] with: Ahmed Maati, Mirjam Edel, Chonlawit Sirikupt, and Oliver Schlumberger[83]

Published in: *Democratization*, online, p. 1 – 21; 07 Aug 2023; doi.org/10.1080/13510347.2023.2234831

Abstract

The amount of information available to citizens due to global digitization and new technologies is unprecedented. However, in established democracies where access to alternative sources of information is guaranteed and educational levels are high, we witness a rise in attitudes and actions that threaten democratic foundations. Some citizens succumb to misinformation that has led them down the path of radicalization and violence; others withdraw completely from political life. How do we explain these developments? Building on democratic theory and the concepts of informational learned helplessness and selective exposure, we introduce a theoretical framework that connects digitization and digital technologies to attitudes and behavior that threaten democracy even before democratic decay manifests. We argue that AI-assisted digital technologies expose societies to an abundance of contradictory information, limit citizens' ability to assess their trustworthiness, and reinforce the tailored dissemination of misinformation. We present the US and Germany as empirical plausibility probes that show how these features drive some citizens towards informational agnosticism, which results in depoliticization and political apathy. Others might become misbelievers who display negative attitudes towards democracy and/or engage in anti-democratic actions. Our probe offers an initial empirical illustration that provides a basis for further systematic investigations of digital technology's effects on democracy.

[82] All authors contributed equally to this article. Ahmed Maati and Koray Saglam developed the initial scope of the article, Chonlawit Sirikupt focused on the empirical plausibility probes, Koray Saglam concretized the political economic theoretical framework. Oliver Schlumberger and Mirjam Edel sharpened the arguments link to democratic theory. Koray Saglam and Oliver Schlumberger proof-read the article and sharpened the overall coherence of the article. Writing, revising, and finalizing the article was done at equal parts.

[83] The authors would like to thank Jelena Cupac, Hendrik Schopmans, and Irem Tuncer-Ebetürk from the Berlin Social Science Center for their helpful comments. The authors would also like to thank Žilvinas Švedkauskas, research assistant Victoria Wang, and all participants of the Chair's research colloquium.

5.1. Digitization, Information, and democratic decay

Democratic theory has long stressed the centrality of information for the proper functioning of democracy (Dahl 1971, 3) When governments restrict access to information, citizens lack a fundamental requisite to meaningful participation and informed decision making. Free access to information has, therefore, been theorized to be conducive rather than detrimental to democracy (Carpini and Keeter 2002, 131). But while digitization and artificial intelligence (AI) have exponentially expanded access to varieties of information, they have also posed threats to democracy in different places (Tucker et al. 2018). From the UK's Brexit referendum to mob lynching in India, these developments have aggravated trends of what scholars have termed "democratic regression", "erosion", "backsliding", "de-democratization", or "authoritarianization".[84]

We know that digital technologies and AI contribute to misinformed attitudes and anti-democratic behavior. In this contribution, we propose an analytical framework that provides the hitherto missing link between digitization and AI on the one hand and such attitudes and behavior on the socio-psychological level on the other. We suggest an integrated framework for analyzing the origins of democratic decay that starts not with misinformation and anti-democratic behavior, but with where these dispositions stem from. In doing so, we highlight political agnosticism and apathy as symptoms of the digital transformation that have important ramifications for democracy.

Digitization and AI-assisted technologies increase citizens' costs of identifying reliable information which can cause states of selective exposure (Stavrositu 2014; Stroud 2008)[85] and informational learned helplessness (ILH) (Nisbet and Kamenchuk 2021).[86] This induces citizens to either become misinformed

[84] A plethora of terms has been invented to refer to this phenomenon. While aware of these debates, we do not seek to settle them here; rather, we agree with Gerschewski that all these terms are "broadly defined as a loss in democratic quality," all the while acknowledging that measurement of such decay is, again, debated (cf., i.a., Diamond and Morlino 2005, for an overview of discussions on this topic). In the following, we refer to the said phenomenon as democratic decay.

[85] In short, "selective exposure" refers to individuals choosing information sources consonant with their worldview.

[86] In contrast to the Russian case they study, however, reference to ILH in democracies refers to citizens' unavoidable exposure to contradictory information.

or politically apathetic. We link misinformation and political apathy back to elements of democratic theory and political regime theory to explain why and how they pose dangers to democracy. To be sure, the variables that determine the resilience of any given democracy to such threats are manifold, and it is beyond the scope of this contribution to examine them in depth. While these variables determine whether only some modest decay or a full-fledged breakdown of democracy will occur, this is not our focus.[87] Instead, we aim to complete the explanatory chain that links AI and digitization more broadly to the phenomena of democratic decay by showing how technology creates psychopolitical dispositions among citizens; these dispositions can, even if not immediately, become a manifest danger to democratic regimes up to the point of democratic breakdown.

While the breakdown of trust in the possibility that truth is knowable can lead to extremism (Gowen 2018), anti-democratic violence, and political disengagement (Wardle and Derakhshan 2017, 10; Wenzel 2019, 1987–88), research does not holistically capture technology's influence on the emergence of attitudes and behavior that put democracy under stress. Scholars have also explored isolated instances (e.g., electoral processes and outcomes) in which misinformation[88] harms specific democratic elements or procedures (Švedkauskas, Sirikupt, and Salzer 2020; Allcott and Gentzkow 2017; Tucker et al. 2018; Benkler, Faris, and Roberts 2018, 341–49). However, these works remain concentrated on isolated aspects of technology and/or individual elements of democracy, thereby ignoring the larger causal chain. From a systemic perspective, digitally induced democratic decay cannot be reduced to the realms of elections, disinformation, or misbelief, despite the relevance of these realms for democracy. Others have used a "deliberative systems"

[87] We do not seek to explain regime-level outcomes that may (and empirically do) differ quite dramatically between cases such as Russia, Hungary or Turkey (where democracy was abolished altogether during the past two decades), or Poland, the US or Brazil (where a tangible erosion of democratic quality is undisputed despite the fact that these cases may still qualify as democracies), and, third, cases such as France, Germany, or Sweden (where we identify "stress factors" such as significant parts of the populace falling prey to misinformation or political apathy even though a decline in the quality of democracy cannot (yet) be measured). By contrast, we seek to establish a more comprehensive causal argument which, because of its comprehensiveness, will allow us to identify dangers and threats to democracy way before current measurement systems of democratic quality would detect them.

[88] While misinformation and disinformation both refer to false or misleading information, disinformation is characterized as "nonaccidentally misleading information" intended to deceive people. Misinformed citizens can further share such information without having the intent to deceive (cf. Fallis 2015).

approach to theorize and examine how disinformation threatens democracy by inducing "anti-deliberative effects" (McKay and Tenove 2021). We concur with these scholars that it is important to specify "which democratic goods are at risk from disinformation, and how they are put at risk" (Ibid: 703) and to consider systemic interactions (Pond 2020). However, beyond specific narratives of misinformation and technical elements like social media algorithms, it is necessary to systematically link the numerous elements of the epiphenomenological level of digitization back to democratic theory and political regime theory to confidently assess whether threats to democracy emerge, and to determine whether they are systemic or ephemeral.

We identify three features inherent to digitized information production, dissemination, and consumption that have transformed citizens' information environment. Section 2 shows how these traits cause a cognitive dissonance that can (1) make parts of the population agnostic about the very existence and relevance of "facts", (2) predispose other parts of the population to become misinformed through selective exposure to information that fit their pre-existing ideas; others (3) bear the higher transaction costs of verifying information to resolve the dissonance.15[89] Section 3, then, explains how such attitudes and the resulting behavior endanger democracy by linking them to democratic theory. Section 4 empirically validates our analytical framework through a plausibility probe into the 2021 US Capitol Hill riots and the 2020 anti-COVID protests at the German Reichstag. While such a probe is not a rigorous hypothesis test, it does provide anecdotal evidence and illustrates our claim about how digitization facilitates misbelief and, subsequently, anti-democratic behavior, or agnosticism and political apathy. While our article suggests a novel and more comprehensive causal chain, only further research will be able to verify such claims through more rigorous empirical testing. Yet, in our view, it is high time that an integrated view and explanation of how democratic decay actually starts and comes about is proposed at all, so that it can be put under closer scrutiny by the scholarly community. A discussion of the implications of our findings for future research on how digital processes may cause decay or breakdown concludes this contribution, together with a call for

[89] We do not intend to provide a universal definition of, or engage with philosophical debates about, "truth" and "falsehood." This would merit discussions that go beyond our scope. Our goal is rather to theorize and show the link between digitization, misinformation, and democratic decay. To illustrate this link, we examine obvious cases of misinformation and falsehoods.

establishing more fine-grained early-warning systems that alert us to threats to democracy we cannot measure adequately so far – precisely because we have been lacking an explanation that comprehensively links digitization to democratic decay.

5.2. How digitization transforms citizens' information environment

Three features of digital technologies affect the nature of information and how citizens consume them: (1) abundance of contradictory information; (2) decreasing ability of consumers to assess its truthfulness; and (3) AI-assisted algorithmic targeting of users with personalized content. These developments occur because of lagging public oversight over the digital sphere that is amplified by political-economic dynamics by which commercial interests (ab)use the still largely unregulated digital space. Together, they transform the informational environment that can lead citizens to embrace misinformation or become doubtful of the existence of truth altogether.

First, digital technologies magnify the abundance by which contradictory information reaches citizens (Feldstein 2021, 3–4). While increasing the pervasiveness of information, they also diversify narratives by simultaneously turning information consumers into information producers. Users not only have a myriad of choices to express and share their preferences, but they are also able to alter the content of the information they disseminate, forward, or re-post (Ibid: 4). This results, first, in Chinese-whispers effects and, second, in the impossibility of identifying the original source of information. Consequently, unprecedented amounts of contradictory accounts of reality overwhelm citizens. Social media platforms' strategies to generate ever more user data to target consumers with fine-tuned appealing narratives exacerbate that trend (cf. Zuboff 2019).

Before the digital revolution, citizens were better able to identify the origin of information, which made it easier to evaluate its reliability and sincerity. By contrast, when information is created and disseminated by many users on numerous digital platforms, it becomes harder (and often impossible) for them to identify its sources. Furthermore, digital image and audio processing technology have immensely enhanced the sophistication of fabrications and, therefore, thwarted citizens' abilities to distinguish reality from fabrication. Competitive market mechanisms incentivize tech companies to design cutting-edge products, which further enhances the technical possibilities of creating AI-assisted deep fakes that help

legitimize fringe beliefs. It is, therefore, not surprising that Europeans state that "helping citizens to better identify disinformation" is the most important public measure authorities should take against the spread of falsehood (Vaccari and Chadwick 2020; European Commission 2020, 54). Digital technologies thus lower the costs of access to information, but counterintuitively, dramatically raise the transaction costs of being correctly informed; they subject wide segments of society to unprecedented difficulties in assessing the accuracy of contradictory information to which they are exposed.

Third, AI-based, self-learning algorithms provide users on digital devices with targeted content. This aggravates both the likelihood of believing misinformation and, depending on the design and purpose of the algorithm, an abundance of contradictory information: Some algorithms promote controversial content, misinformation, and conspiracy beliefs that have led to political polarization and even calls for violence (Dean 2021; Ross Arguedass et al. 2022). Citizens thus experience a psychologically and emotionally challenging overkill of contradictory claims to "truth". Other algorithms, however, rely on the "familiarity effect" and promote content consonant with worldviews that resonate in users' close circles of family and friends – which ultimately contributes to an increase in (mis-)information and facilitates the emergence of the so-called "filter bubbles" (Swire, Ecker, and Lewandowsky 2017, 1948–49).

These three features inherent to digitized information environments are structurally reproduced as digital technologies become commodified products and services designed to generate profits (cf. Saglam 2022). Social media platforms and websites generate revenue through donations, subscriptions, advertisements, and data mining – which all depend on traffic.[90] To increase traffic, platforms routinely employ affirmative or polarizing algorithms, or a mix thereof – irrespective of adverse socio-political outcomes (Dean 2021).

Massive quantities of information, algorithmic targeting, and a reduced ability to assess truthfulness appear most prevalent on social media, where lies spread faster than truths (Vosoughi, Roy, and Aral 2018,

[90] Traffic includes frequency, interaction intensity, and a number of interactions with online content. More traffic means more data to collect and sell, more precise targeting, greater ad revenues, and a greater likelihood that users will subscribe or donate. See also Martin Kenney and John Zysman (2016), as well as Shoshana Zuboff (2019).

1147). However, they pervade the entire digitized information environment,[91] including devices like smartphones that use algorithms for data mining and usage maximization. These are designed to incentivize users to participate in the pluralized information environment by constantly producing and disseminating content. Thus, digitization profoundly changes how citizens are confronted with information. An AI-assisted targeting of individuals with abundant contradictory information of unclear origin can produce fundamental doubts about what is true, what can be trusted, and whether (objective) facts even exist.

Psychologically, constant exposure to contradictory information creates "cognitive dissonance" – a state where humans constantly experience cognitively (and often also emotionally) stressful contradictions (Festinger 1957). There are different possible reactions to this state: (1) Citizens succumb to ILH, i.e., they repeatedly experience an inability to access harmonious, non-contradictory information, which drives them to believe that all information are contested. To these citizens, truth appears not to be knowable or existent, which results in informational agnosticism. To resolve this dissonance, agnostics take the "exit option" and refrain from forming and expressing any opinions, or even from staying informed, which can result in apathy and ignorance.

Citizens can (2) attempt to harmonize dissonance by selectively exposing themselves to one version of discourse. Influenced by traffic-maximising machine-learning algorithms that filter available information based on user preferences, however, this group might fall prey to belief in misinformation and retreat into "echo chambers": "Regardless of how obscure the information we are consuming, as long as it supports pre-existing ideas and does not challenge our beliefs, we are prone to accept it" (Meyer and Böswald 2022, 13). Lastly, individuals might (3) bear the higher transaction costs of verifying information to resolve the dissonance; this constitutes a third, residual category of "the resilient" which is, however, explicitly not the focus of this article.

[91] Non-social media platforms like Spotify or Netflix use similar techniques to increase user traffic, commodify data, and share it with third parties (cf. Zuboff 2019).

5.3. Why informational agnostics and misbelievers endanger democracy

Deduced from our theoretical framework, we identify two groups whose sentiments and behavior threaten democracy: (1) the informationally agnostic and (2) misbelievers. These psychological and attitudinal consequences of digitized information environments threaten democracy before democratic decay becomes visible.

As ILH has been documented to result in apathy (Nagel 2005), ignorance about political matters can be expected to facilitate de-politicization, turning citizens into informational agnostics: When confronted with overwhelming amounts of contradictory narratives, citizens who renounce from consuming (political) information altogether not only become agnostic on an attitudinal level but also display apathy as a form of political behavior. While Bond and Messing lack the causal step of ILH in between that we have introduced, they have, like Nagel, "consistently found that exposure to disagreement [on one's social network] depresses engagement and [political] participation" (Bond and Messing 2015, 75).

Crucially, de-politicization and political apathy are one of four characteristics that Linz uses to define authoritarianism as a non-democratic regime (Linz 1975, 264) Some research has also found that they contribute to democratic decay (Berelson, Lazarsfeld, and McPhee 1986, 314; Huntington 1975, 114). In fact, democratic theory highlights the centrality of citizens' participation in the deliberation process to generate input legitimacy for a healthy democratic system (Dahl 1971), and informed decision-making as an integral element of democratic citizenship (Dahl 1982, 10–11; 1989, 108–14). Healthy democracies depend on citizens' participation (Neubauer 1967, 1002); even more so amid a global democratic decay in which safeguarding democratic norms and practices as is paramount (Levitsky and Ziblatt 2018).

Consequently, informational agnostics as non-participants thereby not only undermine the potential of input legitimacy generation. They are also unlikely to defend democracy or mobilize against proponents of democracy-threatening narratives or actions, as they have concluded that they cannot know what is right. Unlike "misbelievers", agnostics are not part of the polarized but have withdrawn from politics; they feel that neither what they do matters, nor can they change anything. While they might remain engaged with their personal and family lives, they share little interest in public and political affairs. Hence, informational agnostics tend no longer to have an opinion regarding the desirability of democracy. This decrease in diffuse

public support for the democratic political system can endanger the system's sustainability (Easton 1975).[92] While agnostics may return to become part of the informed citizenry in the mid- to long-run, digital technologies make it more likely that agnostics turn into misbelievers since digital media has made it more difficult to distinguish between inaccurate and accurate information (Nisbet and Kamenchuk 2021, 576).

Citizens overwhelmed by the abundance of contradictory information might also embrace misinformation as their new truth. They resolve the stress of cognitive dissonance by embracing information that affirms preconceived worldviews and ignoring contradicting accounts – even if that entails embracing lies and ignoring facts.

While informational agnostics constitute a more silent threat to democracy, misbelievers pose a more direct one in several ways: While access to alternative sources of information is one institutional minimum for democratic rule (Dahl 1982, 10–11; 1989, 108–14), selective exposure to misinformation and counterfactual narratives subverts the reasoning behind democratic participation. Misbelievers are, therefore, likely to vote for anti-democratic parties and candidates based on inaccurate information. While their political participation might be procedurally democratic (e.g., voting), it defies the spirit of democratic participation that envisions participation based on accurate information regarding political choices, and it can produce an impetus for anti-democratic forces that ultimately aim to dismantle democratic institutions.

Second, misbelievers can develop a deep suspicion or even aggression towards dissonant information and its proponents whom they perceive as confounders who aggravate dissonance. This suspicion and aggression can result in misbelievers denying their political opponents' legitimacy as fellow citizens, and in extreme cases, in their stylization as enemies of the state who had best be jailed or killed. Misbelievers thus harbour attitudes that can translate into anti-democratic insurgencies (Levitsky and Ziblatt 2018, 23). This is aggravated by anti-democratic actors that tactically gear misinformation towards undermining democratic institutions and manipulate citizens to mistake democracy for dictatorship. Evidence from cases like Thailand, Germany, and the US show that citizens can be mobilized against democracy if they mis-perceive it be dictatorial, fraudulent, unresponsive, or corrupt; they ironically seek to "save" the "real" democracy by trying to overthrow an elected democratic government (Sinpeng 2021, 165–

[92] For a recent empirical confirmation of the argument see Christopher Claassen (2020).

66; Volk 2021, 13; DFR Lab 2021; Leuker et al. 2022). While anti-democratic attitudes need not per se lead to anti-democratic actions, scholars highlight the importance of pro-democratic attitudes for the functioning of democracies (Teorell and Hadenius 2006; Welzel and Inglehart 2019, 126). If pro-democratic attitudes are important for democracy to flourish, then digital technologies' role in the spread of anti-democratic attitudes has direct consequences for democracy.

Third, confirmation bias induced by online selective exposure jeopardizes social cohesion and exacerbates polarization (Lawrence, Sides, and Farrell 2010). Additionally, through their algorithms, social media platforms (e.g., Youtube, Facebook, and Twitter) might also facilitate radicalization (Camargo 2020). Radical anti-democrats aggravate these radicalization processes by using mainstream social media to funnel their targets towards even less regulated websites and "alternative" social media platforms (e.g., BitChute, Gab, Minds, Parler or Telegram) to generate funds and followers and to circumvent public scrutiny (Andrews and Pym 2021). Ex-president Trump's Truth Social, when released in 2022, immediately topped the US social media downloads in Google's Playstore and Apple's Appstore (E. Palmer 2022).

Even seemingly apolitical misinformation profoundly affects the overall information environment of citizens. For instance, nearly half of Americans believe that dinosaurs still exist (SWNS Staff 2021). Such misinformation contributes to what scholars have called the "post-truth era" where people believe in starkly different accounts of reality (Suiter 2016). This deepens epistemic divides that extend far beyond the political sphere while reinforcing existing political divides about societal challenges, the best solutions, and whether to trust scientific accounts. Thus, seemingly apolitical questions are politically relevant in processes preceding democratic decay (Lipset 1959, 83; Mouffe 1999), especially since misinformation continues to influence how people think even after they have been corrected (Ecker et al. 2022).[93]

In divided societies, crises of democracy are more likely to emerge (Linz 1978, 28), and if polarization looms large, democracies are in danger (Dahl 1971, 105; Sartori 1976, 132–44). Scenarios like "gridlock and careening" or "democratic erosion or collapse" are then enabled (McCoy, Rahman, and Somer 2018). This is not only because new cleavages underlying polarization emerge (Ibid), which pushes the democratic party system toward the brink of "nonworkability" (Sartori 1976, 144), but also because citizens'

[93] The impact this has on contentious political issues can hardly be overestimated (e.g., whether the 2020 elections were "stolen" is a claim that more than half of Republican Party members still believe two years later).

orders of preferences transform as societal trust declines. Here, electoral choices come in again: Beyond making poor choices due to misinformation, high polarization prompts voters to "trade democratic principles for partisan interests" (Crimston, Selvanathan, and Jetten 2022). Thus, when polarization and misinformation collectively induce citizens to perceive that the social fabric has broken down, they are more likely to support authoritarian leaders (Lijphart 1999, 275).

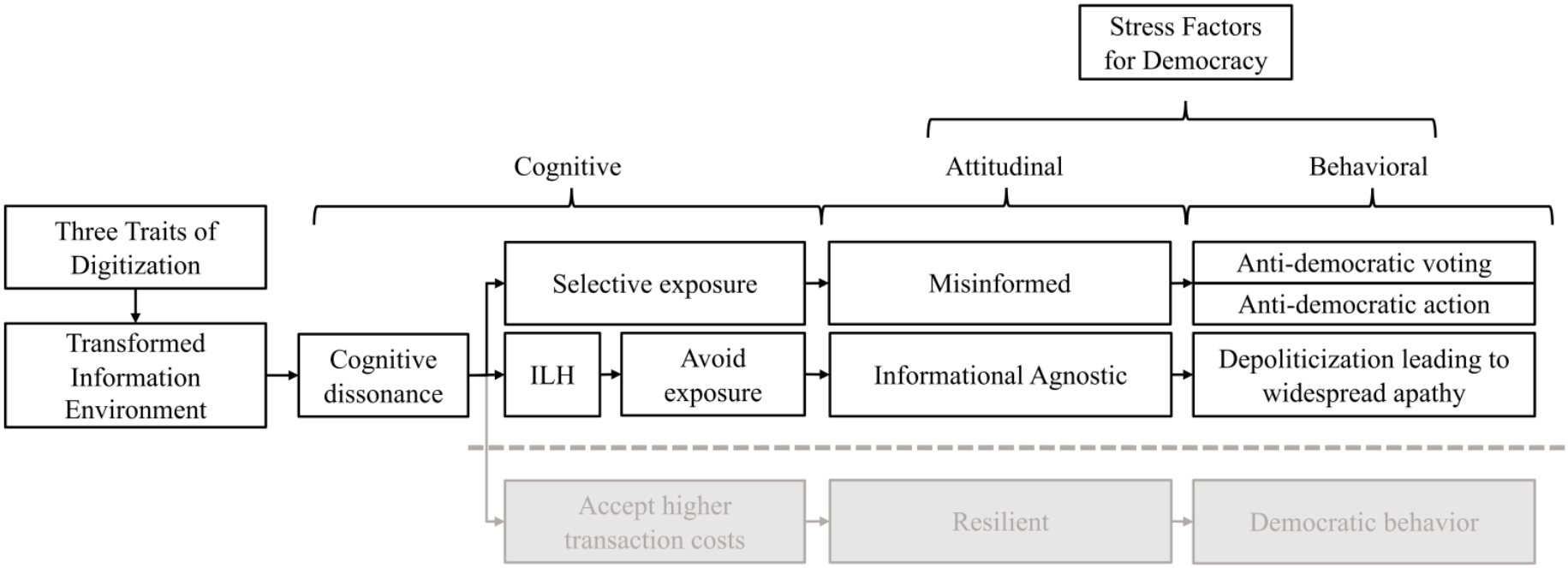
We have now proposed a complete causal chain that links the effects of digital technologies to political attitudes and their associated behavior, as well as their broader impacts to democratic decay, respectively; Figure 6 visualizes this causal chain. With the help of anecdotal evidence from two recent examples of anti-democratic protests that challenged two established democracies, we probe the plausibility of our theorized mechanisms.

5.4. Our Cases: US and Germany

Our theoretical sketch of these pathways is likely to apply in the context of a transformed informational environment at this level of abstraction, bearing in mind cross-country variations in specific structural and sub-structural conditions. Comparing the US and Germany is an important analytical exercise for several reasons. While both are established, wealthy, and representative federal democracies that have a highly educated citizenry that enjoys unfettered access to information, they are, within the universe of liberal democracies, different cases in terms of institutional arrangements, regulation of freedom of speech, digital platform regulations, and media gatekeeping mechanisms.

First, as far as democratic subtypes are concerned, majoritarian systems like those of the US are likely to foster the dominance of identity-based politics. In contrast, proportional representation systems that exist in Germany lead to more inclusive coalitions that temper partisan hostility.58 Second, while the American doctrine of free speech places immense faith in the ability of the individual to discern the truth where he sees it, the German approach necessitates interventions in fostering a tradition of civility and a polity of responsible citizens (Kommers 1980, 685). Third, Germany's digital regulatory framework compels social media companies to remove hate speech and other illegal content whereas American laws provide them with thorough protection from third-party liability, as well as a general allowance for platforms to take down content voluntarily (Scheurman 2022, 418).

Figure 6 Causal link between digitization and democratic decay (source: Maati et al. 2023, 8)



Fourth, Germany's public media enjoys significantly more public funding than the US' highly commerce-driven media landscape, which plays a key role in containing the spread of bias that aggravates ideological extremity and partisan conflict (Benkler, Faris, and Roberts 2018, 22). Finally, and arguably due to the differences, both countries witnessed different degrees of democratic decay (International IDEA n.d.).

Despite these critical differences, very similar mechanisms challenge democracy in both cases. Specifically, AI-assisted digital communication technologies fuelled doubtful attitudes and anti-democratic actions in both countries. In the US, protestors stormed Capitol Hill on January 6, 2021, over misinformation surrounding voter fraud. Similarly, Germans who opposed the government's COVID policies stormed the Reichstag on August 29, 2020. While German anti-COVID protests were more diverse than Capitol riot protests, their common denominator is a growing portion of misinformed citizens who renounce "diffuse support" for democracy (Easton 1975, 444–47). In addition, both cases show signs of digitally aggravated apathy. In the US, one-third of eligible voters did not vote in the 2020 presidential elections (Chamie 2021). In Germany, noncompliance with the government's public health measures was linked to people who gave up on consuming information about COVID (Siebenhaar, Köther, and Alpers 2020, 4–6).

A plausibility probe helps establish whether our framework is valid based on the extent to which it accounts for apparent empirical phenomena.[94] Using a plausibility probe, we seek to provide an initial, non-exhaustive empirical illustration of how features inherent to digitization aggravate selective exposure and ILH, which, in turn, influence beliefs and behavior dangerous to democracies. Our probe, therefore, seeks to provide an initial, non-exhaustive empirical illustration of the socio-psychological impacts that digital technologies have at the attitudinal and behavioral level before decay or breakdown becomes visible at the political regime level. The outcomes at the focus of our analysis are anti-democratic insurgencies, negative attitudes towards democratic institutions, and political apathy.[95]

[94] A plausibility probe is an intermediary step between hypothesis generation and hypothesis testing that allows scholars to explore the suitability of a particular case(s) as a vehicle for theory development (Levy 2008, 3).

[95] We used primary and secondary sources in English and German to support our probe. These include archives of digital media and statements by protesters, news reports, and scholarly works. We also used opinion surveys about

Concretely, we employ four qualitative indicators drawn from our framework to help guide our probe: (1) tailored dissemination of contradictory information to citizens with similar beliefs via recommendation algorithms; (2) the presence of self-organized users and groups on social media platforms who shape algorithmic processes by actively producing and disseminating misinformation; (3) the presence of citizens who selectively expose themselves to tailored online misinformation to gain subjective certainty. Their consumption of contradictory information are expressed via doubts towards official information in favour of dubious non-official sources of information that form a basis for subsequent engagements in anti-democratic actions (e.g. refusal to comply with decision-making processes and norms governing representative democracies and issuing threats of armed violence against elected officials and state representatives); and (4) the presence of citizens who express a sense of helplessness in navigating the abundance of contradictory information. In contrast to the misbelievers, helpless citizens disengage altogether from forming concretely defined beliefs.

5.4.1. From "Stop the Steal" to the steps of the Capitol

On January 6, 2021, a mob of 2,000-2,500 supporters of former US president Donald Trump stormed the Capitol building in Washington, DC as they sought to overturn President-elect Joe Biden's victory in the 2020 presidential elections. The rioters comprised of hyper-partisan pro-Trump activists, QAnon conspiracy theorists, the neo-fascist Proud Boys, unlawful militias (e.g. Oath Keepers), and ideological travellers of the far-right (DFR Lab 2021). This blatant physical violation of American democracy was not a spontaneous reaction to Trump's call but an incremental process in which its origin bear traces to digital technologies that underpin the transformed informational environment. Specifically, the combination of an abundance of contradictory information about official election results, difficulties in identifying truthful accounts, and algorithmic targeting paved the way for a militant offline mass of misbelievers.

Facebook and the digital technologies that power its platform were central to the spread of misinformation. In 2016, the company's internal studies revealed that its algorithms and prioritization of

citizens' perceptions of the 2020 US presidential elections and belief in COVID-related conspiracy theories in Germany.

user engagement exacerbated political polarization, such as by recommending a user to join QAnon - a baseless online fringe-turned- mainstream conspiracy theory that proclaimed Trump's divine role to save the world from an evil cabal of paedophiles (Zadrozny 2021). Despite warnings before the elections (Martin 2022, 230), Facebook's algorithms continued to recommend QAnon pages to old and new users (Frenkel 2020). While Facebook eventually paused its recommendations engine, it started to lift some of these control measures following the elections (Timberg, Dwoskin, and Albergotti 2021).

These algorithmic processes amplified what became the "Stop the Steal" narrative that consisted of three underlying arguments: (1) the expansion of mailed ballots created an opportunity for Democrats to engage in massive voter fraud; (2) Trump won the election and; (3) Trump was within his right to challenge the result and not concede, and even further, Republican legislatures and governors in states where Biden won should use their power to appoint pro-Trump electors (Drutman 2021). When Biden's victory became clear on November 7, the narrative, coupled with the Trumpists' Big Lie tale (a term that is borrowed directly from Hitler's 1925 book Mein Kampf), grew in coordination with Trump's failed legal efforts to "stop the count" of legitimate votes in various states (DFR Lab 2021).

The escalations among various far-right movements that culminated in the Capitol riots were linked to these algorithmically-driven filter bubbles that sustained a groundswell of selective online engagements with the Stop the Steal narrative. These processes did not mitigate polarization but hardened the viewpoints of many Americans who had already embarked on a path to radicalization (Ibid). One Facebook group started by Tea Party activists Amy and Kylie Kremer, which peddled unsubstantiated accusations that the Democrats made false copies of ballots and tricked Arizona Trump supporters into using sharpies to invalidate their votes, attracted more than 360,000 members just a day after the election (Tolan 2021). Initially, Facebook took "limited or no action" against election delegitimization movements and only began removing them once they already gained traction (Mac and Frenkel 2021).

Ultimately, these online dynamics facilitated anti-democratic protests notwithstanding the protesters' professed intentions to "save" US democracy from a perceived corrupt political establishment. Even before January 6, smaller but provocative Stop the Steal rallies had already mushroomed around the country, mostly in states with contested election results (Ibid). Moreover, Jacob Chansley (the "QAnon Shaman" who became the face of the riot) is an example of how digitized informational environments can

exacerbate selective exposure tendencies that result in anti-democratic behavior. On the day of the riot, he remarked,

I realized that doing my own research brought me more information than listening to the news ever could. Once I stopped allowing the news to make up my mind or my narrative for me, I grew exponentially ... I was able to take the information that I was absorbing and apply it to my activist routine (Channel 4 News 2021, 4).

Other misbelievers who developed anti-democratic attitudes but did not physically partake in the Capitol violence can also exacerbate processes that make democratic decay visible. While many Americans rejected the claims and propositions related to Stop the Steal, Republican voters supported all elements of the narrative in significant numbers (Drutman 2021). Furthermore, election misinformation can confuse citizens and place them at the crossroads of either becoming misbelievers or informationally agnostic citizens. Following the elections, 10% of Americans were unsure if Trump should publicly acknowledge Biden as the legitimate president (Griffin and Quasem 2021).

Beyond selective exposure, the effects of digital technologies can also influence ILH, which increases the risk of political apathy that quietly harm democracies: about 68% of US adults said the 2020 elections were a significant source of stress in their lives (Safai 2020). Furthermore, there were indications of apathy as false claims of a stolen election became widespread. Lending initial support to our theorization that informationally agnostics retreat from information consumption to reduce costs associated with information verification, a Pew Research Center poll indicated that one-third of US respondents said that they heard "a little" about January 6 (Gramlich 2020).

5.4.2. From COVID scepticism to the steps of the Reichstag

The COVID-19 pandemic is the first global health crisis that has played out in the digital era where online falsehoods can quickly go viral. The proportion of Germans who saw COVID misinformation several times a day rose from 9% in June 2020 to 17% in February 2021 (Leuker et al. 2022, 11). While digital technologies and social media help keep people safe and informed, they also enable and amplify an "infodemic" where an abundance of contradictory information causes citizens to doubt their governments' public health measures (World Health Organization 2020). The mainstreaming of major pandemic-related conspiracy

theories that originated from fringes of the internet were, in fact, linked to digital and AI-assisted technologies that power social media platforms (Dwoskin 2020).

One of the major COVID conspiracy narratives that managed to penetrate the European online sphere with the help of these technologies is "ID2020". It accused Microsoft and Bill Gates of employing the pandemic as a pretext for implanting microchips to control citizens (Thomas and Zhang 2020, 2). Given that algorithms promote divisive content, high engagements by conspiracy users shaped these algorithms in ways that steered vulnerable users towards this narrative in the aftermath of the outbreak in late 2019 (Ibid: 6). By May 2020, ID2020 became one of the key terms on Twitter (Ibid: 12). Though traces of ID2020 first emerged at anti-COVID protests in the US, they also trickled their way into the German context. Between March and July 2020, around a quarter of German adults believed that Gates had more power than the government and had bought the WHO (Friedrich Naumann Stiftung 2020). In May, a famous vegan chef claimed that the federal government tried to forcibly plant mind-control chips into its citizens at the behest of Gates (Kirschbaum 2020). One doctor also accused Gates of striving for ""pharmacological" world domination" (Das Versteckspiel, n.d.).

As ID2020 made its round on Twitter, the core tenets of QAnon evolved into an umbrella conspiracy that started to embrace anti-COVID narratives. Here, algorithmic targeting continued to amplify narratives that appealed to anti-vaccination and anti-lockdown users (Wong 2020). On Youtube, recommendation algorithms contributed to a "conspiracy boom" that included QAnon (Faddoul, Chaslot, and Farid 2020). These algorithmic processes facilitated the "trans-nationalization" of QAnon into the German online sphere, which attracts the second largest number of followers after the US despite stronger media gatekeeping mechanisms (Barker 2020). A number of German users were able to adapt such alt-right themes and narratives to their context and, aided by recommendation algorithms, pushed the conspiracy theory downstream. After conspiracy ideologue Oliver Janich created the first major Germanlanguage video on QAnon in November 2017, the video reached 90,000 views (Holnburger, Tort, and Lamberty 2022). Though Youtube modified its algorithms in early 2019 (Dwoskin 2020), another German-language QAnon YouTube channel, Qlobal-Change, amassed over 17 million views by September 2020 (Barker 2020).

These effects consequentially shaped anti-democratic attitudes and, in extreme cases, mobilized anti-democratic actions against the German government. The protests that transpired on August 29 in front of the Reichstag were motley crew of Querdenker ("lateral thinkers" who are sceptical and oppose the

government's COVID measures), anti-vaxxers, Q-Anon conspiracy theorists, far-right extremists, and ordinary citizens (Brady 2020). Around 300 of these protesters stormed the building before the police eventually dispersed them. Though the violators were a subset of the 30,000 people who attended the mostly non-violent demonstration that day, digitally induced cognitive dissonance was a key driver behind their anti-democratic behavior (Ibid). The presence of QAnon signs and a portrait of Trump during the rally, as well as images of protesters chanting and promoting anti-Gates slogans such as "Don't give Gates a chance" (Euronews 2020), suggest that selective exposure to online misinformation about COVID, which was reinforced by algorithmic targeting of QAnon and ID2020 content on social media, induced a misguided belief amongst protesters and sceptics that their resistance was against a supposed "COVID dictatorship" (Brady 2020; Forsa Institute 2021, 4).

Although the storming of the Reichstag represented the most visible attack on German democracy and foreshadowed what was to come for the US several months later, digitally-induced cognitive dissonance also played a quieter role in shaping anti-democratic attitudes prior to the incident. Shortly after the first nation-wide lockdown in March 2020, over 25% of Germans believed there was something else behind the pandemic than what was officially announced (Maas 2020, 27–28). Moreover, one study highlighted a positive correlation between Germans who use social media to inform themselves and the rise in pandemic-related conspiratorial beliefs, which suggests the potential of algorithmic targeting to reinforce selective exposure to misinformation (Ibid: 29). Ten percent of Germans reportedly started to believe in a global conspiracy, mostly in connection to Gates (Ibid: 28). Separate from anti-democratic attitudes and actions, signs of apathy associated with ILH also surfaced. Many Germans found distinguishing between news and fake news on the virus difficult (Friedrich Naumann Stiftung 2020). As conspiratorial narratives continued to spread, a YouGov poll in September 2020 provided further empirical evidence for our probe: 11% of the respondents did not know what to think about them, suggesting a degree of detachment that is in line with our theorization that because they cannot know what is right, informationally agnostic citizens withdraw from information consumption to minimize cognitive dissonance (Suhr 2020).

5.5. Conclusion

Global democracy indices such as Freedom House, Polity, or the Bertelsmann Transformation Index tell us that democracy is globally in retreat, but the jury remains out on at least two important questions: The first is about the concrete causal mechanisms that underlie democratic decay as a domestic process. The second is to understand the reasons behind variations in the extent and nature of decay in different contexts, i.e.: Why do some democracies crumble more quickly and substantially than others?

This article contributes to the first debate. We argue that three features inherent to digitization alter the information environment of citizens; we illustrate how this contributes to spreading attitudes and behavior that put stress on, and thus constitute a threat to, democracy. While our case studies empirically illustrate that these characteristics of digitization leave citizens vulnerable to misinformation and apathy, we have also drawn on established knowledge in democratic theory to show how misbelief and apathy threaten the foundations of democracy. We thus provide a novel theoretical approach of how global digitization, widespread misinformation, and challenges to democratic rule are interconnected.

These causes we hypothesize and illustrate empirically usually precede the adverse effects on democracy as measured by existing democracy indices and are hardly captured by the latter. This means: The state of democracy as numerically measured by commonly used indicator systems might seem identical in two given cases; yet, immanent threats of the sort discussed previously may have built up in one case but not in another with identical values on "democracy"–because they are not made visible by existing indices. Thus, equal levels of stress or threats to democracy need not automatically result in similar levels of democratic decay. A diverse range of variables – apart from the ones discussed previously – can be assumed to contribute to the robustness or fragility of democratic regimes when faced with significant stress.[96] Here again, the cases of the US and Germany might provide a helpful comparison to uncover the variables resulting in varying degrees of decay.

Yet, the paramount issue for scholars, but also for democratic policymakers, would be to pay attention to stress on, and threats to, democracy before existing indices can make them visible as a manifest

[96] Some of which may likely be found in the literature on democratic consolidation such as in, e.g., Wolfgang Merkel's "Embedded and Defective Democracies" (2004).

decay or breakdown of democratic institutions and/or procedures. We call for the development of more fine-grained instruments to be able to better assess and potentially quantify such latent stress (and for democratic decisionmakers to devise policies to safeguard democracy). This emergent research agenda would also benefit from two additional endeavours. First, because informationally agnostic citizens are far less visible than misbelievers, more research is required on the formers' size, motivations, and on possible ways to turn them back into informed citizens despite the challenging information environment. Second, the analytical framework we proposed should be subjected to more systematic testing: While our plausibility probe does provide some preliminary empirical illustrations that seem to support our claims, it must not be mistaken for a rigorous effort at falsification.

Beyond complementing ongoing debates on digital technologies and democratic decay by providing much-needed theory-building and proposing concrete causal mechanisms at play, this contribution thus also offers a potentially fruitful outlook for policy-makers and academics to further discuss strategies and policies to promote societal resilience to anti-democratic trends in the digital age – politically by, e.g. enhancing information literacy or regulatory oversight over algorithmic targeting; academically by further testing our proposed mechanisms and by operationalizing the link between digitization and anti-democratic attitudes and behavior through the development of more fine-grained tools for measurement than the ones currently available.

6. Conclusions (Framework Paper)

6.1. Democracy at risk…

With a relational understanding of digital technologies and focusing on their transformative effects they have on political regimes, the findings of this research paint a bleak picture of the digital information age: In the twenty-first century, democracy is "in retreat" (Freedom House 2019) – for twenty consecutive years as of now (Karppi and Hopkins 2024). And based on the research presented in this thesis, the role of supposed digital 'liberation technologies' (cf. Diamond and Plattner 2012) are not to be underestimated in this regard.

As presented in chapter 5 (cf. Maati et al. 2023), democracies are struggling with new information environments that overwhelm citizens with contradicting information, misinformation, and heightened transaction costs of information verification. Citizens that are unable or unwilling to bear these higher costs can have detrimental effects on democracies: overwhelmed individuals run the risk to either become informationally agnostic and politically apathetic; or they might even fall prey to misinformation and conspiracy beliefs. Both outcomes can have detrimental effects on a democracy. As democracies rely on an informed and engaged citizenry (Dahl 1982, 10f; 1989, 108ff), misinformed citizen can be mobilized by populists and engage in anti-democratic mobilization. Examples of these developments manifesting in violent incidents have grown in number – be it the attempted storm of the German parliament in 2020, the insurgency on Capitol Hill in Washington on January 6th, 2021, or the attack on the Brazilian congress in 2023. In turn, informational agnostics that have become politically apathetic will not stand in the way of such political forces to defend the democratic institutions against dismantlement by such anti-democratic populist forces.

Unsurprisingly, then, conspiracy narratives are reaching a wide audience: in a representative survey from 2022, almost every fifth US American was either unsure whether the earth was flat, or even fully convinced that it was (nine and ten percent respectively; Hamilton 2022). Likewise, twenty-eight percent were either unsure or sure that the COVID-19 vaccinations implant micro-ships into the human body (nineteen and nine percent, Ibid). In Germany, twenty-three percent think that it is most likely true that 'hidden powers' are 'secretly controlling the world' – and eight percent are fully convinced by that (Neu

2023). Such conspiracy narratives usually draw the conclusions, that the government, the media, and other secret powers are in cahoots together to pursue malevolent plans and are not to be trusted.

The spread of such conspiracy beliefs and similar misinformation can perpetuate a vicious cycle of declining public trust in institutions and a wider spread of such narratives. In many democracies, these conspiracies fall on fertile ground, as societal trust in institutions has been steadily declining. For the United States, for example, a long-term Gallup survey reflects this alarming development across different kinds of institutions: Public trust has declined for almost all socially and politically relevant institutions, with the exception of the military which was able to even slightly increase its trustfulness in the eyes of the American population (Gallup 2024, see Table XX for an overview). As societal confidence in the congress, the supreme court, and the presidency, as well as traditional media steadily erodes, conspiracy narratives that insinuate these institutions to be involved in secret and malevolent plans further undermine these democratic foundations. This phenomenon of rising distrust in public political and social institutions is also paralleled by developments in other democracies, such as Germany (Faus et al. 2019), as well as across the countries of the European Union (Eurofound 2022).

Table 9 Public confidence in institutions (source: author's compilation based on Gallup 2024).

Institution	**Trust in 1973** (or specified otherwise)	**Trust in 2023**
Church / organized religion	65%	32%
Supreme Court	45%	27%
Banks	60%**	26%
Public Schools	58%	26%
Newspaper	39%	18%
Congress	42%	8%
Television News	46%***	14%
Organized Labor	30%	25%
Presidency	52%*	26%
Police	52%***	43%
The Medical System	80%*	34%
The Criminal Justice System	17%***	17%
Big Business	26%	14%
Military	58%*	60%

Trust: Share of respondents that trust these institutions "a great deal" or "a lot".

Note: 1973 was chosen as earliest year available, 2023 as latest year available; where availability was restricted, the earliest year available is displayed, with *=1975, **=1979, and ***=1993.

Papaioannou, Pantazi, and van Prooijen (2023) substantiate these concerns regarding the growing popularity of conspirative narratives, public institutional trust, and their detrimental effects on democracies. Their large-N study analyzes conspiracy beliefs and political convictions, and they found that the conviction of conspiracy narrative was as a strong and significant predictor for the support of autocracy. Rejection for democracy and democratic ideas was explained with this explanatory in representative samples from the United States and Greece (Ibid).

Chapter 5 of this thesis therefore provides a timely contribution to the study of misinformation and democratic decay. It proposes the theoretical framework that links the technical and political economic characteristics of digital technologies to changes in the information environment and the subsequent outcomes in beliefs and behavior of citizens. Against the backdrop of declining public institutional confidence, the chapter highlights the urgency to act if democracy is to prevail in the twenty-first century. To foster democratic resilience, it is paramount to devise more effective campaigns that combat misinformation and conspiracy narratives, and reestablish trust in public institutions. Likewise, new regulatory frameworks of the digitized information environment are required that strikes the balance between freedom of speech and freedom from misinformation.

6.2. … autocracy on the rise…

Just as democracy is under pressure worldwide, authoritarianism is resurging on a global scale (Repucci and Slipowitz 2022). In 2021, eight out of ten persons worldwide lived under a regime that was considered partly-free or not free, up from five out of ten in 2005 (Ibid, 4). And digital technologies play a central role in this development (Shahbaz 2018; Funk, Shahbaz, and Vesteinsson 2023; Shahbaz and Funk 2019): As chapter 4 presented, autocrats around the world can now pursue the perpetual autocratic agenda of power maintenance with new digital tools and strategies that provide them with unprecedented abilities to know about their subjects and potential challenges to their incumbency (Schlumberger et al. 2023). New ways to control beliefs and behavior of their subjects, and the transnational reach of digital instruments will cause far-reaching transformation of authoritarianism in the twenty-first century. Manipulation and repression will become more subtle, allowing for new (also transnational) legitimation and repression strategies, and the

emergence new state-society relations; new regime coalitions and elite compositions will impact on regime dynamics and institution-building.

These developments of digital authoritarianism manifest in two main dimensions: for one, regimes resort to these technologies to consolidate and control subjects *within* their territory (Yayboke and Brannen 2020). Here, more efficient and subtle repressive techniques assisted with evermore sophisticated technologies make it ever more challenging for people to hold these autocratic regimes accountable for transgressions and human rights violations – a task that is already daunting without potentially omniscient rulers.

Further, autocrats are also applying these technologies and their expertise *outside* of their own territories (Ibid). In line with chapter 5, autocrats seek to undermine democracies: For one, by fragmenting and distorting the information environment they undermine the credibility of democratic institutions, and engineer their misinformation campaigns to support anti-democratic political forces. This ultimately undermines institutional trust and interferes with the electoral process (Švedkauskas, Sirikupt, and Salzer 2020; Blake 2020; McCabe 2019; Tennis 2020). Further, autocrats are also undermining the prospects of democracy by providing powerful surveillance technology and necessary expertise to governments of all traits, democracies and autocracies alike (Chestnut Greitens 2020; Mozur, Kessel, and Chan 2019). With a growing number of instances where also governments in democracies have been found to resort to illicit surveillance of political opponents (Kość 2022; Scott-Railton et al. 2022; H. Smith 2023; Kayali 2023), chilling effects further erode the confidence and ability of critics to hold their governments accountable, with detrimental effects for democracy (cf. O'Carroll 2023). Together, this exposes a growing number of people to authoritarianism, bet it within autocratic regimes, or abroad, where manipulation and surveillance from external actors also subject citizens in democracies to forms of digital authoritarianism.

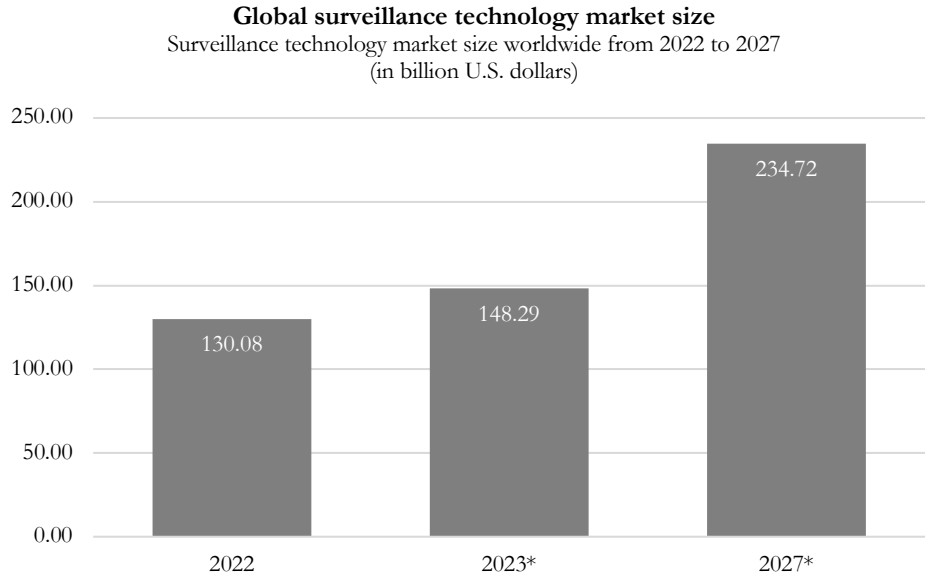
The bourgeoning literature on autocracy in the twenty-first century is only beginning to grasp the full scope of digital authoritarianism, and new areas of research continue to emerge. Digital technologies put autocrats at an advantage vis-à-vis their subjects (Rød and Weidmann 2015), but it remains unclear what kind of effective opposition strategies are available to opponents under digital authoritarianism. To understand patterns of contestation, a more nuanced understanding of how autocrats use these technologies is warranted. While some research is starting to clarify factors that determine choices of digital strategies and tools (cf. Feldstein 2021; Saglam forthcoming) much is to be explain, such as what type of autocrats

rely on which technologies and strategies; what circumstances affect the choice or combination of different tools available; and how effective are these strategies.

6.3. … and companies profiting.

The phenomena of digital authoritarianism and digitally intensified democratic decay, as well as digital technologies themselves, have distinct political economic ramifications that perpetuate these developments, as regimes are not the only relevant actors (chapter 3 and 2, i.e., Saglam 2022; and forthcoming, respectively). The systemically underregulated political economy of digital technologies creates ample incentives for tech-companies to market ever more potent digital goods and services, irrespective of the social and political externalities they might cause (Saglam 2022). This creates markets for commercialized electoral manipulation, as well as for targeted digital surveillance and repression. Companies involved in this market allow regimes, that have insufficient human or financial capital to develop their own sophisticated surveillance technology, to simply turn to private-sector companies as cost-efficient alternatives (Saglam forthcoming).

Graph 6 Global surveillance technology market size, 2023 and 2027 projected (source: Borgeaud 2023)



And this market is lucrative: in 2022, it stood at 130 billion US dollars, and it is projected to grow by another 58 percent between 2023 and 2027 (Borgeaud 2023; see also Diagram 1). As the market size grows (Ibid),

and regulation remains ineffective (Feldstein and Kot 2023a), more companies can be expected to enter into competition with one another and to provide ever more sophisticated and potent surveillance technologies at better prices.

Consequently, the threshold to acquire digital surveillance becomes significantly lower as it becomes cheaper and more affordable to purchase them, even for low-income countries. In 2016, the New York Times reported that, based on leaked internal documents of NSO Group, the Israeli spyware company offered to hack ten smartphones for 65,000 US dollars each, plus a 500,000 US dollars set up fee (Perlroth 2016). From internal documents of the now dissolved German spyware company FinFisher, we know that these prices can even be undercut (Nordic Monitor 2022).

With a wider proliferation of these surveillance technologies due to numerous affordable providers, a secondary demand is triggered. Even countries that could develop their own in-house solutions, or that do not even have intentions to use such software, might turn towards the private sector nevertheless: As a growing number of countries acquire commercial surveillance software, more countries might deem it necessary to protect themselves against this technology. This, then, necessitates these countries to acquire and analyze these products to stay up to date with the most recent versions on the market and find more powerful ways to counter them.

Together, then, this thesis provides substantial theoretical and empirical research on the transformative impact of digital technologies on politics and political systems in the twenty-first century. It lays out the perilous situation of democracies that struggle to strike a balance between regulation of online content and freedom of speech; it presents a compelling framework of new ways that authoritarianism will manifest in the new millennial; and it illuminates the political economic structures that – without any foreseeable effective international regulatory framework of these technologies – will perpetuate these developments for the foreseeable future.

6.2. Dependence, convergence, and classification

These findings highlight two main points for further investigation. First, if contextualized against the broader political economic context, the substantiate the perception of perpetuating dependencies and vulnerabilities between industrialized and industrializing countries (Mayer and Lu 2022; World Economic

Forum 2022, 45ff). This can be illustrated along two dimensions, the supply-side, as well as the demand-side. Second, the findings of this thesis also raise questions of (a) how digital technologies allow autocrats to rely on new and more sophisticated ruling techniques; and (b) how democracies appear to be increasingly challenged by a myriad for internal- and external dynamics that undermine core-institutions, and, at times, appear to also resort to digitally enabled illiberal practices. Together, some observers interpret these developments as convergence in practices (Gunitsky 2020). But even from a more nuanced perspective, it becomes increasingly challenging to classify regime types using conventional definitions or cursory hallmarks for classification. Consequently, the findings of this thesis also highlight the necessity to reconsider the conceptual role of information control and information environments in defining democracies and authoritarian regimes in the twenty-first century.

6.2.1. Perpetuating dependencies, internalizing profits, and socializing externalities

The political economy of digital technologies does not emerge on a blank canvas, *ex machina* so to speak. Instead, digital innovations are products and services developed and marketed within the capitalist mode of production with a profit intention. As such, their political economy is inherently embedded in wider structures of global dependence (cf. Santos 1970; Wallerstein 2004; Prebisch 1950; and Singer 1950), and reinforces them. Digitization is producing new vulnerabilities and dependencies across the globe. However, if one is to refer to Wallerstein's (2004) terminology of center, semi-periphery and periphery, countries of the center are affected to a lesser degree by dependencies, whereas countries of the (semi-)periphery are affected much more drastically.[97] This can be exemplified along two main dimensions, the demand and the supply side.

[97] This loose reliance on Wallerstein's framework of centre, semi-periphery and periphery simply serves only to illustrate the main argument and highlight some general patterns to contextualize the findings of this thesis against the greater backdrop of global political economic dynamics. The intention is not to negate the more nuanced intricacies of global political economic dependencies that the research of the past decades have produced.

6.2.1.1. The demand-side: importing vulnerability

Digitization is continuously expanding, and it has become an integral element of the globalized economy, as well as a requirement for economic integration. Consequently, regimes of all traits pursue digital technologies for various reasons, ranging from civilian purposes to security and combating organized crime, all the way to targeted surveillance, manipulation, and digital repression. However, by continuously integrating digital infrastructures, countries are also reproducing existing dependencies, and render themselves open to new vulnerabilities (Mayer and Lu 2022; World Economic Forum 2022, 45ff; Mussington 2021).

These new vulnerabilities also affect countries of the center. While global tech-capital continues to be located in countries of the center (cf. Companies Market Cap 2024), new economic ties with providers of digital infrastructure components also create new challenges. For one, externally provided digital technologies and infrastructures can always serve as a backdoor for other third parties. In 2020, the Chinese tech company Huawei was found to be able to access mobile networks around the world by integrating hidden entry points for third parties (Pancevski 2020). The company produces mobile devices but also provides digital infrastructure components around the world. In Italy, for example, the company could access the data traffic of millions of its clients through a backdoor of their internet routers they provided to Vodafone (Lepido 2019). Likewise, encryption chips from the Chinese company Hualan, blacklisted by the US Commerce Department for its suspicious ties to the Chinese military, "[…] have ended up deep inside sensitive Western information networks […]" (Greenberg 2023), raising concerns about the integrity of these networks (Ibid).

For countries of the periphery and the semi-periphery, however, these new vulnerabilities pose far greater challenges due to their limited technological and financial capacities to adequately protect themselves against potential intrusions; but also due to their limited political levers to sanction such transgressions by other foreign powers. Digital technologies and infrastructures have become a matter of economic integration and prosperity. Countries with limited resources are then not only required to keep up with advancing digitization, but also to keep up with digital arms race and the development of defensive cyber capabilities – aggravating the scarcity of their already strained capacities. As a consequence, less developed

countries of the (semi-)periphery are more vulnerable to hackers, digital extortion, and external digital intrusion (Russu 2022; cf. also World Economic Forum 2022, 45ff; EIT Digital 2021; Mussington 2021).

But the political economy of digital technologies does not only aggravate dependencies concerning continued economic integration and the protection from external intrusion. The also concern external national security strategies. Digital technologies can enhance the abilities of national intelligence agencies to gather critical information in the prevention of terrorist attacks and countering other imminent threats. If countries do not possess the ability to develop such digital intelligence tools on their own, their entire national security strategy can become contingent on the decision of external providers which might be companies or other countries – with potentially detrimental outcomes.

A case in point is Ukraine. Five years after the Russian invasion of Crimea, Luhansk and Donetsk, and amidst rising tensions prior to the second invasion in 2022, Ukraine sought to purchase the potent Pegasus spyware from the Israeli NSO Group for its national intelligence services in 2019 (Bergman and Mazzetti 2022b; Kirchgaessner 2022). While the software itself would not have prevented the attack, it could have provided the intelligence services with crucial information ahead of the full-scale invasion by Putin's army. Yet, fearing deteriorating relations with Russia, the Israeli government intervened and prevented the transaction (Ibid).

Another example in this regard was the interference of Elon Musk in shutting down the internet access of Ukraine's army during a critical counter-operation against the Russian occupation (Nazzaro 2023). With the full-scale invasion, and the breakdown of internet networks along the front line, the Musk's Starlink satellites provide critical infrastructure necessary for defending and reinstating Ukraine's sovereignty. However, with Musk's decision to not only turn off the internet service during a critical operation, but to tolerate the Russian army's usage of these services in this unlawful war of aggression (Guardian Staff 2024), potentially prolonged the war and further jeopardizes what is left of Ukraine's sovereignty and national security. These are but a few instances of how new digital technologies and advancing digitization is recreating existing dependencies and producing new vulnerabilities for countries that rely on external providers.

6.2.1.2. The supply-side: profiting from misery

The supply-side of these technologies highlight how these dependencies and vulnerabilities are capitalized on by companies, as well as by the countries in which they preside. These companies are predominately located in countries of the center and semi-periphery. This, in turn, produces a dynamic, where profits and market value accrue to the companies of industrialized and more wealthy countries, whereas externalities in the form of dependencies, vulnerabilities, polarization and violence are simply socialized around the world.

Measured by market capitalization, 799 out of the 950 largest tech companies listed publicly are located in the Global North; 514 alone in the United States (Companies Market Cap 2024). Out of the 2.638 trillion US dollars in market capitalization, 2.398 trillion accrue to the Global North (Ibid). This pattern also holds for companies that operate in the market of commercialized surveillance technologies (cf. Feldstein and Kot 2023a): companies like FinFisher, NSO Group or HackingTeam are located in high-income democracies in the Global North, such as Israel, Italy, and Germany (Ibid). These companies generate billions in market value and profits but socialize the political and socio-economic externalities around the globe. Industrialized countries are beginning to experience the negative effects of algorithms that polarize societies and translate into real-life conflicts (e.g., Martin 2022; Duell 2021; Hagey and Horwitz 2021) and other concerning outcomes that are caused by digitized information environments (cf. Maati et al. 2023).

However, the socio-economic and political externalities of digital technology industries have more dire consequences for societies in countries of the periphery and semi-periphery that are already more vulnerable (cf. Scheck, Purnell, and Horwitz 2021; see also Kassem 2023; Wallerstein 2004). One example entails the outsourcing of content moderation, training algorithms, and the review of appeals on social media platforms which are yet to be completely taken over by artificial intelligence algorithms. These tasks have been relocated to countries such as India or Kenya (Parent and McQue 2023; Bhalla 2023; Pilling and Murgia 2023). In these positions, employees are exposed to disturbing imagery, ranging from racism to graphic displays of torture, death, and sexualized violence, ultimately jeopardizing the mental health of those exposed to these contents, causing traumas and depression (McIntyre, Bradbury, and Perrigo 2022; Parent and McQue 2023; McKay and Tenove 2021; Parent and McQue 2023; Bhalla 2023).

More drastic examples of externalities entail lethal political violence, as in India, where Facebook tolerated the spread of religious hate-speech to not jeopardize profits; this ultimately spiraled into

Islamophobic mobilization with deadly consequences (Purnell and Horwitz 2021). Despite the awareness of its employees, Facebook was found to be unable or unwilling to effectively address instances were human trafficking rings relied on the platform to target vulnerable women in the Middle East; or where armed Ethiopian militias where inciting ethnically motivated violence; Mexican drug-cartels could even use the advertisement mechanism to disseminate gruesome pictures to recruit new members; instead, the company focused on making the platform safer and more appealing in higher-income countries (Scheck, Purnell, and Horwitz 2021).

This pattern of profit internalization and externality-socializing is also resembled by the global market of commercialized surveillance software: While citizens of industrialized high-income countries have also been targeted by their governments with the help of commercial spyware, such as in the cases of Poland, Hungary, Greece, or Spain (Walker 2021; Kość 2022; H. Smith 2023; Scott-Railton et al. 2022), consequences of the use of such surveillance technology has been much more gruesome, even lethal in the (semi-)peripheral countries: Spyware was instrumental in the murder of Jamal Khashoggi (Kirchgaessner 2021a); it was used to facilitate forced disappearances and torture in Egypt (Tesquet 2017), and massacres of protestors in Sudan (Teloglou et al. 2022). And while civilians, journalists, and critics are spied on with this technology and subsequently killed, the companies that indiscriminately provide this technology rake in the profits. If one is to further study the full impact digital technologies have around the word, it becomes inevitable paramount to incorporate develop a critical theoretical framework of the digital political economy.

6.2.2. Democracy and autocracy in the twenty-first century

In the digital age, dictatorships look 'calmer' even though they are not less repressive or 'more demcoratic' (Kendall-Taylor, Frantz, and Wright 2020, 110ff; Rød and Weidmann 2015; Schlumberger et al. 2023, 13ff). New and more subtle ways to coopt, repress, and manipulate provide contemporary autocrats with the means to preempt mass mobilization, to target repression more precisely, to generate more effective pro-regime narratives and to undermine the effects of counter-narratives (Ibid). Likewise, governments and politicians in democracies are also increasingly using digital technologies for illiberal purposes (Gunitsky 2020; Bradshaw and Howard 2017). While qualitative differences between autocracies and democracies prevail, and democratic governments continue to be exposed to greater scrutiny and judicial prosecution if

transgressions become public (cf. Kość 2022; H. Smith 2023), it is still warranted to reflect on the questions of regime-convergence and conceptual reconsiderations, as well as the safeguards required to protect democracy in the new millennium.

6.2.2.1. Convergence and classification

In autocracies, manipulation, cooptation, and repression has become more subtle thanks to digital innovations. Consequently, elections have become potentially less threatening for dictators, as new strategies are available to further tilt the playing field more effectively to the advantage of the autocrat, creating the possibility of more frequent and 'liberal-looking' elections in autocracies (Schlumberger et al. 2023, 11f). Less threatening elections, in turn, could result in an increase of in frequency, and a more 'liberal look' (Ibid), which could make it even more challenging to classify whether a regime is authoritarian or democratic, causing similar conceptual challenges as regime hybrids (cf. Diamond 2002; Levitsky and Way 2002; 2010; Møller and Skaaning 2010; Collier and Levitsky 1997; Merkel 2004), i.e., regimes that are not 'fully' democratic, or polyarchies (Dahl 1971), but also not as 'fully' autocratic as Spain under Franco (Linz 1964).

But greater challenges in classifying regime types not only emerge from the way autocracies are affected by digital innovations. Digitized democracies also add to these conceptual challenges, as the illiberal use of new technologies has also found its way into democratic regimes (Gunitsky 2020), where a growing number of politicians rely on digital manipulation and digitally disseminated misinformation to further their own agenda (Bradshaw and Howard 2017; Feldstein 2021, 14f). This undermines the capabilities of citizens to make well-informed decisions and their ability fully participate in the democratic process; which, in turn, has detrimental consequences for the quality of democracy (cf. Maati et al. 2023).

Likewise, politicians and governments in democracies have resorted to digital surveillance software to spy on political opponents, journalists and activists in democracies, such as Poland, Hungary, Greece, or Spain (Walker 2021; Kość 2022; H. Smith 2023; Scott-Railton et al. 2022). Just like autocracies, democracies are purchasing sophisticated surveillance technology, either from private market providers (Saglam forthcoming) or from other countries, such as China (Chestnut Greitens 2020, 1). As France (Kayali 2023), and Britain (Clarke 2024) have expanded their surveillance laws, Germany and other European countries push EU-wide legislation that would allow to also legally target journalists (Lavrilleux et al. 2023; O'Carroll

2023). These developments have a dire impact on the freedom of speech and the functioning of the media as fourth estate; especially through the chilling effects they create (O'Carroll 2023). This trend also coincides with growing, even lethal risks that journalists across the EU find themselves exposed to (Reporters Without Borders 2023a; 2023c), and an increasing number of defamation lawsuits that are targeted against journalists and used to undermine critical reporting (Zappulla and Simon 2023).

While verdict still stands out, whether these developments, together, resemble what Gunitsky (2020) terms a "convergence" between democracies and autocracies, these trends *do* highlight the challenges of classification. But they also shed light on potential remedies to address these challenges: As autocracies have the means to appear more liberal than they are, and a growing number of actors in democracies also resort to digital technologies for illiberal purposes, information environments and how they are regulated will prof to be a crucial hallmark to distinguish democracies from autocracies in the twenty-first century.

This is not necessarily a new insight – there is still wine in old bottles: Robert Dahl has highlighted the importance of an informed and engaged citizenry for a healthy and functioning democracy (Dahl 1998, 38ff; 1982, 10f; 1989, 108ff). However, what he termed "access to alternative sources of information" (Dahl 1971, 3ff) is probably better expressed by how he put it later as "enlightened understanding" (Dahl 1998, 38): In the digital age, probably nothing is more readily available, and more detrimental to democracy nowadays than "*alternative*" sources of information; and by that I mean outlets that disseminate misinformation, AI-generated deep fakes, and other "alternative facts"(in refernce to Kellyanne Conway's infamous statement as adviser to former US President Trump; cf. Associate Press 2017).

In the twentieth century, alternative information sources in the form of uncensored media that provided a factual perspective on events that might contradict regime narratives were indeed a crucial element in contesting autocratic ruling structures, as well as for healthy democracies. Ironically, it is the overwhelming flood of (partly contradicting and wrong) information that now poses a challenge to healthy democracies in the twenty-first century. Therefore, in order to ensure the ability of citizens to gain an "enlightened understanding" (Dahl 1998, 38), this information cacophony needs to be reigned in and combine the protection of freedom *of speech* with a protection of freedom *from misinformation*.

6.2.2.2. Safeguarding democracy

In the age of digital information, nothing is more important with regards to politics, political systems, and power, than information itself; or freely after Frank Herbert "Those, who control information, control the universe."[98] The way that rulers regulate the flow and control of information will become the most central hallmark in determining whether a regime can be classified as an autocracy or a democracy. And to protect democracy in the twenty-first century, several key objectives must be achieved within the coming years.

(I) The legal protection of journalists and media must become more effective. Growing distrust in traditional media sources, fueled by digitally disseminated fake news and conspiracy narratives, has started to translate into open violence against journalists (cf. Jacobsen 2020), making it easier for autocrats to repress free media. This also entails to counter the weaponization of defamation lawsuits against journalists to undermine free and critical media (Zappulla and Simon 2023).

(II) Companies involved in the sectors of information and communication technologies need to be subjected to more effective regulatory frameworks, as information and data have become elements of central importance in critical infrastructures. Be it the commercialization of private user data (Deibert 2019; Zuboff 2019), the selling of surveillance technologies (Feldstein and Kot 2023b; Saglam forthcoming), or the provision of digital infrastructures (Mussington 2021; Saglam 2022): the Janus-faced nature of digital technologies manifests increasingly in the form of negative social, economic and political externalities – at times even with lethal consequences. Safeguarding democracies thus requires reigning in the companies responsible for, and profiting from, these externalities and hold them accountable to the political and social outcomes caused by their products and services. While the EU's Digital Services Act is a first step in the right direction, critics highlight terminological ambiguities and loop holes that leave substantial room for improvement (Turillazzi et al. 2023; Scott 2024).

(III) The status and importance of personal information and data, and the human right to privacy, requires greater recognition and safeguarding – now more than ever. With the advent of generative artificial intelligence, immeasurable amounts of private user data are used to train newer and more capable algorithms that are already now beginning to displace labor (Schwab 2016a). The same data, that also generates billions

[98] The original quote from *Dune* (1965): "He, who controls the spice, controls the universe."

a in profit for tech-companies today (Zuboff 2019; Deibert 2019). But even beyond the pure monetary and economic aspects, the political value of privacy and the sanctity of personal information in democracies is not to be underestimated. Otherwise, the advancing encroachment on our privacy, and accelerating technological advances will continue to shrink the analog and un-surveilled space of opinion-formation and -exchange. This will inevitably also subject more and more citizens to the chilling effects of perpetual and ubiquitous surveillance. Ultimately, this would risk a future where, as George Orwell wrote in *1984*, "If you want to keep a secret, you must also hide it from yourself."

7. References

If not indicates otherwhise, all online sources have last been accessed on April 29th, 2024, by 13:00.

Abramowitz, Michael, and Michael Chertoff. 2018. "The Global Threat of China's Digital Authoritarianism." Washington Post. November 1, 2018. https://www.washingtonpost.com/opinions/the-global-threat-of-chinas-digital-authoritarianism/2018/11/01/46d6d99c-dd40-11e8-b3f0-62607289efee_story.html?utm_term=.8515635cf1fe.

Aho, Brett, and Roberta Duffield. 2020. "Beyond Surveillance Capitalism: Privacy, Regulation and Big Data in Europe and China." *Economy and Society* 49 (2): 187–212. https://doi.org/10.1080/03085147.2019.1690275.

Albrecht, Holger, and Oliver Schlumberger. 2004. "'Waiting for Godot': Regime Change Without Democratization in the Middle East." *International Political Science Review* 25 (4): 371–92. https://doi.org/10.1177/0192512104045085.

Alghamdi, Noha S., and Saeed M. Alghamdi. 2022. "The Role of Digital Technology in Curbing COVID-19." *International Journal of Environmental Research and Public Health* 19 (14): 8287. https://doi.org/10.3390/ijerph19148287.

Allcott, Hunt, and Matthew Gentzkow. 2017. "Social Media and Fake News in the 2016 Election." *Journal of Economic Perspectives* 31 (2): 211–36.

Altmeppen, Thomas, and Mirjam Edel. 2017. "Disentangling the State-Regime Nexus." *Comparative Democratization* 15 (1): 6–10. https://connect.apsanet.org/s35/wp-content/uploads/sites/26/2017/10/2017_15_1.pdf.

Amnesty International. 2021. "Massive Data Leak Reveals Israeli NSO Spyware Used to Target Activists, Journalists, and Political Leaders." NGO. Amnesty International. July 18, 2021. https://www.amnesty.org/en/tech//en/latest/news/2021/07/the-pegasus-project/.

Anand, Nikhil, Akhil Gupta, and Hannah Appel. 2018. *The Promise of Infrastructure*. SAR Advanced Seminar Titles. Durham: Duke University Press.

Andrews, Frank, and Ambrose Pym. 2021. "The Websites Sustaining Britain's Far-Right Influencers." Bellingcat. February 24, 2021. https://www.bellingcat.com/news/uk-and-europe/2021/02/24/the-websites-sustaining-britains-far-right-influencers/.

Arthur, Charles. 2012. "China Tightens 'Great Firewall' Internet Control with New Technology." The Guardian. December 14, 2012. http://www.theguardian.com/technology/2012/dec/14/china-tightens-great-firewall-internet-control.

Associate Press. 2017. "'Alternative Facts' Remark Tops 2017 List of Notable Quotes." Associate Press. December 12, 2017. https://apnews.com/article/df148be22a484e8b8c04406320bd961a.

Bakir, Vian. 2020. "Psychological Operations in Digital Political Campaigns: Assessing Cambridge Analytica's Psychographic Profiling and Targeting." *Frontiers in Communication* 5 (September): 67. https://doi.org/10.3389/fcomm.2020.00067.

Bannikova, Kateryna, Petro Fryz, Nadiia Voronova, Nadiia Voronova, Andrii Bondarenko, and Liudmyla Bilozub. 2023. "Digital Transformations in Culture and Art: New Opportunities and Challenges." *Revista Amazonia Investiga* 12 (61): 348–58. https://doi.org/10.34069/AI/2023.61.01.35.

Barker, Tyson. 2020. "Germany Is Losing the Fight Against QAnon." Foreign Policy. September 2, 2020. https://foreignpolicy.com/2020/09/02/germany-is-losing-the-fight-against-qanon/.

Barry, Ellen. 2018. "Cambridge Analytica Whistle-Blower Contends Data-Mining Swung Brexit Vote." The New York Times. March 27, 2018. https://www.nytimes.com/2018/03/27/world/europe/whistle-blower-data-mining-cambridge-analytica.html.

BBC. 2021a. "Jamal Khashoggi: All You Need to Know about Saudi Journalist's Death." BBC. February 24, 2021. https://www.bbc.com/news/world-europe-45812399.

———. 2021b. "Pegasus: Who Are the Alleged Victims of Spyware Targeting?" BBC. July 22, 2021. https://www.bbc.com/news/world-57891506.

Beckett, Lois. 2017. "Trump Digital Director Says Facebook Helped Win the White House." The Guardian. October 9, 2017. https://www.theguardian.com/technology/2017/oct/08/trump-digital-director-brad-parscale-facebook-advertising.

Benjakob, Omer. 2022. "The NSO File: A Complete (Updating) List of Individuals Targeted With Pegasus Spyware." Haaretz. January 20, 2022. https://www.haaretz.com/israel-news/tech-news/MAGAZINE-nso-pegasus-spyware-file-complete-list-of-individuals-targeted-1.10549510.

Benjakob, Omer, and Josh Breiner. 2022. "Police Use NSO's Pegasus to Spy on Israelis Without Warrant, Report Says." Haaretz. January 18, 2022. https://www.haaretz.com/israel-news/police-used-nso-s-pegasus-to-spy-on-israelis-without-court-order-report-says-1.10546407.

Benkler, Yochai, Robert Faris, and Hal Roberts. 2018. *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. 1st ed. Oxford: Oxford University Press. https://doi.org/10.1093/oso/9780190923624.001.0001.

Bensoussan, Alain, Renaud Fabre, Louki-Géronimo Richou, Lucille Colin, and Marie Blanquart, eds. 2018. *The Digital Factory for Knowledge: Production and Validation of Scientific Results*. London: Wiley-ISTE.

Bentzen, Naja, and Tristan Krause. 2021. "EU-US Explainer: Regulation of the Digital Sector." Policy Briefing PE 696.179 – July 2021. Washington, DC: European Parliamentary Research Service / European Parliament Liaison Office in Washington DC. http://www.europarl.europa.eu/unitedstates/en/eplo-resources/eu-us-explainer-regulation-of-the-digital-sector.

Béranger, Jérôme, and Roland Rizoulières, eds. 2021. *The Digital Revolution in Health*. Hoboken: ISTE Ltd / John Wiley and Sons Inc.

Berelson, Bernard, Paul F. Lazarsfeld, and William N. McPhee. 1986. *Voting: A Study of Opinion Formation in a Presidential Campaign*. Midway reprint ed. Midway Reprint. Chicago: University of Chicago Press.

Bergman, Ronen, and Mark Mazzetti. 2022a. "The Battle for the World's Most Powerful Cyberweapon." The New York Times. January 28, 2022. https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html.

———. 2022b. "Israel, Fearing Russian Reaction, Blocked Spyware for Ukraine and Estonia." The New York Times. March 23, 2022. https://www.nytimes.com/2022/03/23/us/politics/pegasus-israel-ukraine-russia.html.

Bermeo, Nancy. 2016. "On Democratic Backsliding." *Journal of Democracy* 27 (1): 5–19. https://doi.org/10.1353/jod.2016.0012.

Bhalla, Nita. 2023. "Mental Trauma: African Content Moderators Push Big Tech on Rights." The Japan Times. October 16, 2023. https://www.japantimes.co.jp/business/2023/10/16/tech/african-content-moderators-big-tech/.

Bhuiyan, Johana. 2022. "Spyware Targets Uyghurs by 'Masquerading' as Android Apps." The Guardian. November 10, 2022. https://www.theguardian.com/world/2022/nov/10/spyware-targeting-ugyhurs-android-apps-report.

Blake, Jedidiah. 2020. "Russian Interference in U.S. Elections: How to Protect Critical Election Infrastructure from Foreign Participation." *Public Contract Law Journal* 49 (4): 709–34.

Bloomberg, Jason. 2018. "Digitization, Digitalization, And Digital Transformation: Confuse Them At Your Peril." Economic News. Forbes. April 29, 2018. https://www.forbes.com/sites/jasonbloomberg/2018/04/29/digitization-digitalization-and-digital-transformation-confuse-them-at-your-peril/#432c9bbd2f2c.

Boehme-Neßler, Volker. 2020. *Digitising Democracy: On Reinventing Democracy in the Digital Era - A Legal, Political and Psychological Perspective*. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-34556-3.

Boehnke, Olaf, and Carlo Zensus. 2022. "The Global Story of Election Interference." Israel Public Policy Institute. April 14, 2022. https://www.ippi.org.il/the-global-story-of-election-interference/.

Bogaert, Koenraad. 2018. *Globalized Authoritarianism: Megaprojects, Slums, and Class Relations in Urban Morocco*. Globalization and Community 27. Minneapolis: University Of Minnesota Press.

Bogart, Dan. 2022. "Infrastructure and Institutions: Lessons from History." *Regional Science and Urban Economics* 94 (May): 103626. https://doi.org/10.1016/j.regsciurbeco.2020.103626.

Bond, Robert, and Solomon Messing. 2015. "Quantifying Social Media's Political Space: Estimating Ideology from Publicly Revealed Preferences on Facebook." *American Political Science Review* 109 (1): 62–78. https://doi.org/10.1017/S0003055414000525.

Borgeaud, Alexandra. 2023. "Surveillance Technology Market Size Worldwide 2027." Statista. December 19, 2023. https://www.statista.com/statistics/1251839/surveillance-technology-market-global/.

Bradshaw, Samantha, and Philip N Howard. 2017. "Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation." Working Paper No.2017.12. Computational

Propaganda Research Project. Oxford: University of Oxford. http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdf.

Brady, Kate. 2020. "Thousands Turn out in Berlin to Protest Coronavirus Measures." Deutsche Welle. August 29, 2020. https://www.dw.com/en/thousands-turn-out-in-berlin-to-protest-coronavirus-measures/a-54756290.

Bruff, Ian. 2014. "The Rise of Authoritarian Neoliberalism." *Rethinking Marxism* 26 (1): 113–29. https://doi.org/10.1080/08935696.2013.843250.

Bruff, Ian, and Cemal Burak Tansel. 2019. "Authoritarian Neoliberalism: Trajectories of Knowledge Production and Praxis." *Globalizations* 16 (3): 233–44. https://doi.org/10.1080/14747731.2018.1502497.

Brunsdon, David. 2023. "Examining Predator Mercenary Spyware." HYAS Labs. October 23, 2023. https://www.hyas.com/blog/examining-predator-mercenary-spyware.

Cadwalladr, Carole. 2020. "Fresh Cambridge Analytica Leak 'Shows Global Manipulation Is out of Control.'" The Observer. January 4, 2020. https://www.theguardian.com/uk-news/2020/jan/04/cambridge-analytica-data-leak-global-election-manipulation.

Camargo, Chico Q. 2020. "YouTube's Algorithms Might Radicalise People – but the Real Problem Is We've No Idea How They Work." The Conversation. January 21, 2020. http://theconversation.com/youtubes-algorithms-might-radicalise-people-but-the-real-problem-is-weve-no-idea-how-they-work-129955.

Cambridge Analytica. 2020a. "Cambridge Analytica - Select 2016 Campaign-Related Documents." Databank. Internet Archive. September 28, 2020. http://archive.org/details/ca-docs-with-redactions-sept-23-2020-4pm.

———. 2020b. "Campaign Related Documents w. Redactions -1." Leaked Internal Company Documents. https://archive.org/details/ca-docs-with-redactions-sept-23-2020-4pm/page/n9/mode/2up.

Cannings, Richard, Jason Woloz, Neel Mehta, Ken Bodzak, Wentao Chang, and Megan Ruthven. 2017. "An Investigation of Chrysaor Malware on Android." *Google Online Security Blog*. April 3, 2017. https://security.googleblog.com/2017/04/an-investigation-of-chrysaor-malware-on.html.

Carpini, Michael X Delli, and Scott Keeter. 2002. "The Internet and an Informed Citizenry." In *The Civic Web*, edited by D. Anderson and M. Cornfield, 129–53. Lamham: Rowman & Littlefield Publishers. https://repository.upenn.edu/handle/20.500.14332/1838.

Caruso, Loris. 2018. "Digital Innovation and the Fourth Industrial Revolution: Epochal Social Changes?" *AI & SOCIETY* 33 (3): 379–92. https://doi.org/10.1007/s00146-017-0736-1.

Chamie, Joseph. 2021. "Who's Not Voting in America?" The Hill. July 7, 2021. https://thehill.com/opinion/campaign/561886-whos-not-voting-in-america/.

Channel 4 News. 2021. "Meet the 'QAnon Shaman' behind the Horns at the Capitol Insurrection." January 21, 2021. https://www.youtube.com/watch?v=trB06rINhKI.

Chehabi, Houchang E., and Juan J. Linz, eds. 1998. *Sultanistic Regimes*. Baltimore: Johns Hopkins University Press.

Chestnut Greitens, Sheena. 2020. "Dealing with Demand for China's Global Surveillance Exports." Global China - Assessing China's Growing Role in the World. Brookings. https://www.brookings.edu/articles/dealing-with-demand-for-chinas-global-surveillance-exports/.

Claassen, Christopher. 2020. "Does Public Support Help Democracy Survive?" *American Journal of Political Science* 64 (1): 118–34. https://doi.org/10.1111/ajps.12452.

Clarke, Laurie. 2024. "Britain's Got Some of Europe's Toughest Surveillance Laws. Now It Wants More." Politico. January 3, 2024. https://www.politico.eu/article/uk-bulking-up-spying-regime-breakneck-speed/.

Colgan, Jeff D., and Jessica L.P. Weeks. 2015. "Revolution, Personalist Dictatorships, and International Conflict." *International Organization* 69 (1): 163–94.

Collier, David, and Steven Levitsky. 1997. "Democracy with Adjectives: Conceptual Innovation in Comparative Research." *World Politics* 49 (3): 430–51. https://doi.org/10.1353/wp.1997.0009.

Collins, Keith, and Gabriel J.X. Dance. 2018. "How Researchers Learned to Use Facebook 'Likes' to Sway Your Thinking." The New York Times. March 20, 2018. https://www.nytimes.com/2018/03/20/technology/facebook-cambridge-behavior-model.html.

Companies Market Cap. 2024. "Largest Tech Companies by Market Cap." Companies Market Cap. April 19, 2024. https://companiesmarketcap.com/tech/largest-tech-companies-by-market-cap/.

Confessore, Nicholas. 2018. "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far." The New York Times. April 4, 2018. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

Coppedge, Michael, John Gerring, Carl Henrik Knutsen, Staffan I. Lindberg, Jan Teorell, David Altman, Michael Bernhard, et al. 2023. "Varieties of Democracy Dataset Version 13." https://doi.org/10.23696/vdemds22.

Coppedge, Michael, John Gerring, Carl Henrik Knutsen, Staffan I. Lindberg, Jan Teorell, Kyle L. Marquardt, Daniel Pemstein, et al. 2023. "V-Dem Varieties of Democracy Methodology." V–13. Gothenburg, Sweden: University of Gothenburg. https://v-dem.net/data/the-v-dem-dataset/.

Coskun, Gülcin Balamir. 2021. "Turkey's New Internet Law and Its Effects on Freedom of Media." *Reset Dialogues*. July 12, 2021. https://www.resetdoc.org/story/turkey-internet-law-freedom-media/.

Couldry, Nick, and Ulises Ali Mejias. 2019. *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*. Culture and Economic Life. Stanford, California: Stanford University Press.

Crimston, Charlie R., Hema Preya Selvanathan, and Jolanda Jetten. 2022. "Moral Polarization Predicts Support for Authoritarian and Progressive Strong Leaders via the Perceived Breakdown of Society." *Political Psychology* 43 (4): 671–91. https://doi.org/10.1111/pops.12787.

Currier, Cora, and Morgan Marquis-Boire. 2014. "Leaked Files: German Spy Company Helped Bahrain Hack Arab Spring Protesters." The Intercept. August 7, 2014. https://theintercept.com/2014/08/07/leaked-files-german-spy-company-helped-bahrain-track-arab-spring-protesters/.

Dahl, Robert Alan. 1971. *Polyarchy: Participation and Opposition*. Repr. New Haven: Yale University Press.

———. 1982. *Dilemmas of Pluralist Democracy: Autonomy vs. Control*. New Haven: Yale University Press.

———. 1989. *Democracy and Its Critics*. New Haven: Yale University Press.

———. 1998. "Chapter 4 - What Is Democracy?" In *On Democracy*, 35–43. New Haven & London: Yale University Press.

Dalmasso, Emanuela, Adele Del Sordi, Marlies Glasius, Nicole Hirt, Marcus Michaelsen, Abdulkader S. Mohammad, and Dana Moss. 2018. "Intervention: Extraterritorial Authoritarian Power." *Political Geography* 64 (May): 95–104. https://doi.org/10.1016/j.polgeo.2017.07.003.

D'Amore, Rachael. 2020. "'Yes, This Drone Is Speaking to You': How China Is Reportedly Enforcing Coronavirus Rules." Global News. November 2, 2020. https://globalnews.ca/news/6535353/china-coronavirus-drones-quarantine/.

Dans, Enrique. 2018. "The Kremlin Vs. Telegram: What's Really Going On With The Messaging Service In Russia?" Forbes. April 19, 2018. https://www.forbes.com/sites/enriquedans/2018/04/19/the-kremlin-vs-telegram-whats-really-going-on-with-the-messaging-service-in-russia/.

Das Versteckspiel. n.d. "Feindbild Bill Gates / 'Gib Gates Keine Chance.'" ['Enemy Image Bill Gates / "Give Bill Gates No Chance'"]." Das Versteckspiel. Accessed April 2, 2024. https://dasversteckspiel.de/die-symbolwelt/verschwoerungsmythen/feindbild-bill-gates-gib-gates-keine-chance-343.html.

Data Justice Lab. 2020. "Data Harm Record." Data Justice Lab. 2020. https://datajusticelab.org/data-harm-record/.

Data Reportal. 2022. "The Latest Facebook Statistics: Everything You Need to Know." DataReportal – Global Digital Insights. May 11, 2022. https://datareportal.com/essential-facebook-stats.

Dean, Jason. 2021. "The Facebook Files." The Wall Street Journal. October 1, 2021. https://www.wsj.com/articles/the-facebook-files-11631713039.

Deibert, Ronald J. 2019. "The Road to Digital Unfreedom: Three Painful Truths About Social Media." *Journal of Democracy* 30 (1): 25–39. https://doi.org/10.1353/jod.2019.0002.

Deutsche Welle, Deutsche. 2021. "German Police Secretly Bought NSO Pegasus Spyware." Deutsche Welle. September 7, 2021. https://www.dw.com/en/german-police-secretly-bought-nso-pegasus-spyware/a-59113197.

DFR Lab. 2021. "#StopTheSteal: Timeline of Social Media and Extremist Activities Leading to 1/6 Insurrection." Just Security. February 10, 2021. https://www.justsecurity.org/74622/stopthesteal-timeline-of-social-media-and-extremist-activities-leading-to-1-6-insurrection/.

Diamond, Larry Jay. 2002. "Thinking About Hybrid Regimes." *Journal of Democracy* 13 (2): 21–35. https://doi.org/10.1353/jod.2002.0025.

———. 2019. "The Road to Digital Unfreedom: The Threat of Postmodern Totalitarianism." *Journal of Democracy* 30 (1): 20–24. https://doi.org/10.1353/jod.2019.0001.

Diamond, Larry Jay, and Leonardo Morlino, eds. 2005. *Assessing the Quality of Democracy*. Johns Hopkins University Press. https://doi.org/10.56021/9780801882869.

Diamond, Larry Jay, and Marc F. Plattner, eds. 2012. *Liberation Technology: Social Media and the Struggle for Democracy*. A Journal of Democracy Book. Baltimore, Md: Johns Hopkins University Press.

Digital Society Project. 2024. "Digital Society Project." Digital Society Project. 2024. https://digitalsocietyproject.org/data/.

Dixon, Robyn. 2021. "Russia's Surveillance State Still Doesn't Match China. But Putin Is Racing to Catch Up." Washington Post. August 17, 2021. https://www.washingtonpost.com/world/europe/russia-facial-recognition-surveillance-navalny/2021/04/16/4b97dc80-8c0a-11eb-a33e-da28941cb9ac_story.html.

Dormann, Carsten F., Jane Elith, Sven Bacher, Carsten Buchmann, Gudrun Carl, Gabriel Carré, Jaime R. García Marquéz, et al. 2013. "Collinearity: A Review of Methods to Deal with It and a Simulation Study Evaluating Their Performance." *Ecography* 36 (1): 27–46. https://doi.org/10.1111/j.1600-0587.2012.07348.x.

Drinhausen, Katja, and Vincent Brussee. 2021. "China's Social Credit System in 2021: From Fragmentation towards Integration." China Monitor. Mercator Institute for China Studies (MERICS). https://merics.org/en/report/chinas-social-credit-system-2021-fragmentation-towards-integration.

Drutman, Lee. 2021. "Theft Perception." Democracy Fund - Voter Study Group. June 2021. https://www.voterstudygroup.org/publication/theft-perception.

Duell, Mark. 2021. "Facebook's Algorithm 'Promoted Toxic and Hateful Content.'" Mail Online. October 26, 2021. https://www.dailymail.co.uk/news/article-10132759/Facebooks-algorithm-promoted-toxic-hateful-content.html.

Dwoskin, Elizabeth. 2020. "Misinformation about the Coronavirus Is Thwarting Facebook's Best Efforts to Catch It." The Washington Post. August 19, 2020. https://www.washingtonpost.com/technology/2020/08/19/facebook-misinformation-coronavirus-avaaz/.

Easton, David. 1965. *A Framework for Political Analysis*. Englewood Cliffs, New Jersey: Prentice Hall, Inc.

———. 1975. "A Re-Assessment of the Concept of Political Support." *British Journal of Political Science* 5 (4): 435–57. https://doi.org/10.1017/S0007123400008309.

Eaton, Tim, Paolo Gerbaudo, Mohamed Ben Moussa, Marc Owen Jones, Juliette Harkin, and Hussein Ghrer. 2013. "The Role of Social Media in the Arab Uprisings - Past and Present." Edited by Maha Taki and Lorenzo Coretti. *Westminster Paper in Communication and Culture* 9 (2): 1–115.

Ecker, Ullrich K. H., Stephan Lewandowsky, John Cook, Philipp Schmid, Lisa K. Fazio, Nadia Brashier, Panayiota Kendeou, Emily K. Vraga, and Michelle A. Amazeen. 2022. "The Psychological Drivers of Misinformation Belief and Its Resistance to Correction." *Nature Reviews Psychology* 1 (1): 13–29. https://doi.org/10.1038/s44159-021-00006-y.

Eibl, Ferdinand. 2020. *Social Dictatorships: The Political Economy of the Welfare State in the Middle East and North Africa*. Oxford: University Press.

EIT Digital. 2021. "European Digital Infrastructure and Data Sovereignty - a Policy Perspective." EIT KIC publications. Brussels: European Institute of Innovation and Technology - EIT Digital. https://eit.europa.eu/library/european-digital-infrastructure-and-data-sovereignty.

Eurofound. 2022. "Trust in Institutions Continues to Fall in EU, despite Declining Unemployment and Phasing out of Pandemic Restrictions." Eurofound. July 7, 2022. https://datawrapper.dwcdn.net/oABpV/6/.

Euronews. 2020. "'Sturm auf Reichstag': Nazi-Flaggen und QAnon-Anhänger in Berlin." Euronews. August 30, 2020. https://de.euronews.com/2020/08/30/nazi-flaggen-und-qanon-anhanger-bei-corona-protesten-in-berlin.

European Commission. 2020. "Attitudes towards the Impact of Digitalisation on Daily Lives." European Union. March 2020. https://europa.eu/eurobarometer/surveys/detail/2228.

———. 2022. "Data Protection in the EU." Text. European Commission - European Commission. 2022. https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en.

Fabre, Renaud, Quentin Messerschmidt-Mariet, and Margot Holvoet. 2016. *New Challenges for Knowledge: Digital Dynamics to Access and Sharing*. Information Systems, Web and Pervasive Computing Series. London : John Wiley & Sons, Inc.

Facebook. 2019a. "Requests For User Data." Facebook Transparency. 2019. https://transparency.facebook.com/government-data-requests/country/JO/jan-jun-2019.

———. 2019b. "Direct Link to Download Leaked Facebook Internal Documents and Emails Secret (PDF 628Mo)." Reddit. November 7, 2019. https://www.reddit.com/r/privacy/comments/dst6se/direct_link_to_download_leaked_facebook_internal/.

Faddoul, Marc, Guillaume Chaslot, and Hany Farid. 2020. "A Longitudinal Analysis of YouTube's Promotion of Conspiracy Videos." arXiv. http://arxiv.org/abs/2003.03318.

Fallis, Don. 2015. "What Is Disinformation?" *Library Trends* 63 (3): 401–26. https://doi.org/10.1353/lib.2015.0014.

Farries, Elizabeth. 2019. "Spying on Dissent: Surveillance Technologies and Protest." Geneva: International Network of Civil Liberties Organizations (INCLO). https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwi974Hs0b31AhWLy6QKHVSqAKoQFnoECAwQAQ&url=https%3A%2F%2Fwww.inclo.net%2Fpdf%2Fspying-on-dissent-Report_EN.pdf&usg=AOvVaw1mGMnfN8C7yATYTTHH4sxg.

Faus, Rainer, Tom Mannewitz, Simon Storks, Kai Unzicker, and Erik Vollmann. 2019. "Schwindendes Vertrauen in Politik Und Parteien Eine Gefahr Für Den Gesellschaftlichen Zusammenhalt?" ["Diminishing Trust in Politics and Parties: A Threat to Social Cohesion?"]." Gütersloh: Bertelsmann Stiftung. https://www.bertelsmann-stiftung.de/fileadmin/files/Projekte/Gesellschaftlicher_Zusammenhalt/ST-LW_Studie_Schwindendes_Vertrauen_in_Politik_und_Parteien_2019.pdf.

Feldstein, Steven. 2019a. "The Global Expansion of AI Surveillance." Working Paper. Washington, DC: Carnegie Endowment for International Peace. https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final.pdf.

———. 2019b. "The Road to Digital Unfreedom: How Artificial Intelligence Is Reshaping Repression." *Journal of Democracy* 30 (1): 40–52.

———. 2021. *The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance*. Carnegie Endowment for International Peace. New York, NY: Oxford University Press.

———. 2023. "Digital Repression Index 2003-2022." Mendeley. https://doi.org/10.17632/RRNZ8P6RVW.3.

Feldstein, Steven, and Brian Chun Hey Kot. 2023a. "Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses." Washington, DC: Carnegie Endowment for International Peace. https://carnegieendowment.org/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses-pub-89229.

———. 2023b. "Global Inventory of Commercial Spyware & Digital Forensics." Mendeley. https://doi.org/10.17632/CSVHPKT8TM.10.

Festinger, Leon. 1957. *A Theory of Cognitive Dissonance*. Standford: Stanford University Press.

Fishman, Robert M. 1990. "Rethinking State and Regime: Southern Europe's Transition to Democracy." *World Politics* 42 (03): 422–40. https://doi.org/10.2307/2010418.

Forsa Institute. 2021. "Befragung von Nicht Geimpften Personen Zu Den Gründen Für Die Fehlende Inanspruchnahme Der Corona-Schutzimpfung." "[Survey of Non-Vaccinated Persons About the Reasons for the Lacking Claim of the Corona-Protection Vaccination]." f21.0437/40770 Sh. Berlin: Forsa Institute. https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/C/Coronavirus/Befragung_Nichtgeimpfte_-_Forsa-Umfrage_Okt_21.pdf.

Frantz, Erica. 2018. *Authoritarianism: What Everyone Needs to Know*. Language and Literacy Series. New York: Oxford University Press.

Frantz, Erica, Andrea Kendall-Taylor, and Joseph Wright. 2020. "Digital Repression in Autocracies." Users Working Paper 27. 2020. Gothenburg, Sweden: Verieties of Democracy Institute. https://www.v-dem.net/media/filer_public/18/d8/18d8fc9b-3ff3-44d6-a328-799dc0132043/digital-repression17mar.pdf.

Freedom House. 2019. "Democracy in Retreat - Freedom in the World 2019." Annual Report. Freedom House. https://freedomhouse.org/sites/default/files/Feb2019_FH_FITW_2019_Report_ForWeb-compressed.pdf.

Frenkel, Sheera. 2020. "Facebook Removes 790 QAnon Groups to Fight Conspiracy Theory." The New York Times. August 19, 2020. https://www.nytimes.com/2020/08/19/technology/facebook-qanon-groups-takedown.html.

Friedrich, Carl Joachim, and Zbigniew Brzezinski. 1956. *Totalitarian Dictatorship and Autocracy*. Cambridge: Havard University Press.

Friedrich Naumann Stiftung. 2020. "Globale Studie: Desinformationen Durchdringen Gesellschaften Weltweit." "[Global Study: Disinformation Pervades Societies All Over The World]." Berlin: Friedrich Naumann Stiftung. https://www.freiheit.org/de/globale-studie-desinformationen-durchdringen-gesellschaften-weltweit.

Frost, Jim. 2020. "Coefficient of Variation in Statistics." Statistics By Jim. October 26, 2020. https://statisticsbyjim.com/basics/coefficient-variation/.

Fuchs, Christian. 2014. *Digital Labour and Karl Marx*. New York, NY: Routledge, Taylor & Francis Group.

Funk, Allie, Adrian Shahbaz, and Kian Vesteinsson. 2023. "Freedom on the Net 2023 - The Repressive Power of Artificial Intelligence." Freedom of the Net Report. Washington, D.C.: Freedom House. https://freedomhouse.org/report/freedom-net/2023/repressive-power-artificial-intelligence.

Furman, Jason, and Robert Seamans. 2019. "AI and the Economy." *Innovation Policy and the Economy* 19 (January): 161–91. https://doi.org/10.1086/699936.

Gallup, Gallup. 2024. "Confidence in Institutions." Gallup. 2024. https://news.gallup.com/poll/1597/Confidence-Institutions.aspx.

Gandhi, Jennifer, and Adam Przeworski. 2006. "Cooperation, Cooptation, and Rebellion under Dictatorships." *Economics and Politics* 18 (1): 1–26. https://doi.org/10.1111/j.1468-0343.2006.00160.x.

Geddes, Barbara, Joseph Wright, and Erica Frantz. 2018. *How Dictatorships Work: Power, Personalization, and Collapse*. 1st ed. Cambridge University Press. https://doi.org/10.1017/9781316336182.

Gellman, Barton. 2020. "Secrets, Surveillance and Snowden." Washington Post. May 11, 2020. https://www.washingtonpost.com/magazine/2020/05/11/2013-edward-snowden-leaked-top-secret-national-security-agency-documents-showing-how-us-was-spying-its-citizens-heres-what-happened-next/.

Gellman, Barton, Aaron Blake, and Greg Miller. 2013. "Edward Snowden Comes Forward as Source of NSA Leaks." The Washington Post. June 9, 2013.

https://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html.

Gerschewski, Johannes. 2013. "The Three Pillars of Stability: Legitimation, Repression, and Co-Optation in Autocratic Regimes." *Democratization* 20 (1): 13–38. https://doi.org/10.1080/13510347.2013.738860.

Gil de Zúñiga, Homero, Aaron Veenstra, Emily Vraga, and Dhavan Shah. 2010. "Digital Democracy: Reimagining Pathways to Political Participation." . . *Journal of Information Technology & Politics* 7 (1): 36–51.

Glasius, Marlies. 2018a. "Illiberal and Authoritarian Practices in the Digital Sphere - Prologue," 19.

———. 2018b. "Extraterritorial Authoritarian Practices: A Framework." *Globalizations* 15 (2): 179–97. https://doi.org/10.1080/14747731.2017.1403781.

———. 2018c. "What Authoritarianism Is … and Is Not: A Practice Perspective." *International Affairs* 94 (3): 515–33. https://doi.org/10.1093/ia/iiy060.

Gowen, Annie. 2018. "As Mob Lynchings Fueled by WhatsApp Messages Sweep India, Authorities Struggle to Combat Fake News." The Washington Post. July 2, 2018. https://www.washingtonpost.com/world/asia_pacific/as-mob-lynchings-fueled-by-whatsapp-sweep-india-authorities-struggle-to-combat-fake-news/2018/07/02/683a1578-7bba-11e8-ac4e-421ef7165923_story.html.

Gramlich, John. 2020. "A Look Back at Americans' Reactions to the Jan. 6 Riot at the U.S. Capitol." Pew Research Center. January 4, 2020. https://www.pewresearch.org/short-reads/2022/01/04/a-look-back-at-americans-reactions-to-the-jan-6-riot-at-the-u-s-capitol/.

Greenberg, Andy. 2023. "How A Shady Chinese Firm's Encryption Chips Got Inside NATO and NASA." Wired. January 15, 2023. https://www.wired.com/story/hualan-encryption-chips-entity-list-china/.

Griffin, Robert, and Mayesha Quasem. 2021. "Crisis of Confidence - How Election 2020 Was Different." Democracy Fund - Voter Study Group. https://www.voterstudygroup.org/publication/crisis-of-confidence.

Guardian Staff. 2024. "Ukraine Claims Russian Forces Using Musk's Starlink in Occupied Areas." The Guardian. February 12, 2024. https://www.theguardian.com/world/2024/feb/12/ukraine-accuses-russia-forces-using-elon-musk-starlink.

Guerrieri, Paolo, and Sara Bentivegna. 2011. *The Economic Impact of Digital Technologies: Measuring Inclusion and Diffusion in Europe*. Cheltenham: E. Elgar.

Gunitsky, Seva. 2015. "Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability." *Perspectives on Politics* 13 (1): 42–54. https://doi.org/10.1017/S1537592714003120.

———. 2020. "The Great Online Convergence: Digital Authoritarianism Comes to Democracies." War on the Rocks. February 19, 2020. https://warontherocks.com/2020/02/the-great-online-convergence-digital-authoritarianism-comes-to-democracies/.

Gupta, Mark Sen. 2020. "What Is Digitization, Digitalization, and Digital Transformation?" ARC Advisory Group. March 24, 2020. https://www.arcweb.com/blog/what-digitization-digitalization-digital-transformation.

Guriev, Sergei, and Daniel Treisman. 2019. "Informational Autocrats." *Journal of Economic Perspectives* 33 (4): 100–127. https://doi.org/10.1257/jep.33.4.100.

Gurijala, Bhanukiran. 2021. "What Is Pegasus? How Surveillance Spyware Invades Phones." Scientific American. August 9, 2021. https://www.scientificamerican.com/article/what-is-pegasus-how-surveillance-spyware-invades-phones/.

Hagey, Keach, and Jeff Horwitz. 2021. "Facebook Tried to Make Its Platform a Healthier Place. It Got Angrier Instead." The Wall Street Journal. September 15, 2021. https://www.wsj.com/articles/facebook-algorithm-change-zuckerberg-11631654215.

Hamilton, Lawrence. 2022. "Conspiracy vs. Science: A Survey of U.S. Public Beliefs." University of New Hampshire - Carsey School of Public Policy. April 25, 2022. https://carsey.unh.edu/publication/conspiracy-vs-science-a-survey-of-us-public-beliefs.

Herbert, Frank. 1965. *Dune*. London: Hodder & Stoughton.

Heydemann, Steven. 2007. "Upgrading Authoritarianism in the Arab World." Analysis Paper 13. Washington, DC: The Sabian Center for Middle East Policy at the Brookings Institution. https://www.brookings.edu/wp-content/uploads/2016/06/10arabworld.pdf.

———. 2020. "Rethinking Social Contracts in the MENA Region: Economic Governance, Contingent Citizenship, and State-Society Relations after the Arab Uprisings." *World Development* 135 (November): 105019. https://doi.org/10.1016/j.worlddev.2020.105019.

Hiebert, Kyle. 2023. "The Growing Global Spyware Industry Must Be Reined In." Centre for International Governance Innovation. May 27, 2023. https://www.cigionline.org/articles/the-growing-global-spyware-industry-must-be-reined-in/.

Hindman, Matthew Scott. 2009. *The Myth of Digital Democracy*. Princeton: Princeton University Press.

Hinz, Enno. 2022. "How Myanmar's Junta Uses Chinese Surveillance Technology." Dw.Com. July 28, 2022. https://www.dw.com/en/how-myanmars-junta-is-using-chinese-facial-recognition-technology/a-62624413.

Hobbs, William R, and Margaret E Roberts. 2018. "How Sudden Censorship Can Increase Access to Information." *American Political Science Review* 112 (3): 621–36.

Holnburger, Josef, Maheba G. Tort, and Pia Lamberty. 2022. "Q VADIS? The Spread of QAnon in the German-Speaking World." CeMAS – Center für Monitoring, Analyze und Strategie gGmbH & Alfred Landecker Foundation. https://cemas.io/en/publications/q-vadis-the-spread-of-qanon-in-the-german-speaking-world/CeMAS_Q_Vadis_The_Spread_of_QAnon_in_the_German-Speaking_World.pdf.

Homeland Security. 2016. "Digital Forensics Tools." TechNote. Washington, DC: U.S. Department of Homeland Security - Science and Technology. https://www.dhs.gov/sites/default/files/publications/Digital-Forensics-Tools-TN_0716-508.pdf.

Horwitz, Jeff. 2021. "Facebook Says Its Rules Apply to All. Company Documents Reveal a Secret Elite That's Exempt." The Wall Street Journal. September 13, 2021. https://www.wsj.com/articles/facebook-files-xcheck-zuckerberg-elite-rules-11631541353.

Howard, Philip N., and Muzammil M. Hussain. 2011. "The Role of Digital Media." *Journal of Democracy* 22 (3): 35–48. https://doi.org/10.1353/jod.2011.0041.

Huntington, Samuel P. 1975. "The United States." In *The Crisis of Democracy: On the Governability of Democracies*, edited by Michael Crozier, Samuel P Huntington, and Joji Watanuki, 59–118. New York: New York University Press.

Ilbiz, Ethem, and Christian Kaunert. 2023. "Securitization, Fear Politics, and the Formation of an Opposition Alliance in Competitive Authoritarian Regimes." *Democratization* 30 (8): 1604–24. https://doi.org/10.1080/13510347.2023.2252346.

Interpol. 2024. "Identifying Terrorist Suspects." Interpol. 2024. https://www.interpol.int/en/Crimes/Terrorism/Identifying-terrorist-suspects.

Jacobsen, Katherine. 2020. "Conspiracy Theories Grow in the U.S., Creating Threats to Journalist Safety." Committee to Protect Journalists. October 26, 2020. https://cpj.org/2020/10/conspiracy-theories-grow-in-the-u-s-creating-threats-to-journalist-safety/.

Jenss, Alke, and Benjamin Schuetze. 2021. "Rethinking Authoritarian Power: The Logistics Space and Authoritarian Practices in and between Secondary Port Cities of the Global South." *International Studies Quarterly* 65 (1): 82–94. https://doi.org/10.1093/isq/sqaa083.

Jessop, Bob. 2019. "Authoritarian Neoliberalism: Periodization and Critique." *South Atlantic Quarterly* 118 (2): 343–61. https://doi.org/10.1215/00382876-7381182.

Jones, Marc Owen. 2013. "Social Media, Surveillance and Social Control in the Bahrain Uprising." *Westminster Papers in Communication and Culture* 9 (2): 68–92. https://doi.org/10.16997/wpcc.167.

———. 2019. "Propaganda, Fake News, and Fake Trends: The Weaponization of Twitter Bots in the Gulf Crisis." *International Journal of Communication* 13.

———. 2022. *Digital Authoritarianism in the Middle East: Deception, Disinformation and Social Media*. London: Hurst.

Karppi, Alexandra, and Mary Hopkins. 2024. "The Human Cost of Democratic Decline." Freedom House. April 11, 2024. https://freedomhouse.org/article/human-cost-democratic-decline.

Kassem, Sarrah. 2023. *Work and Alienation in the Platform Economy: Amazon and the Power of Organization*. Bristol, UK: Bristol University Press.

Kaster, Sean D., and Prescott C. Ensign. 2023. "Privatized Espionage: NSO Group Technologies and Its Pegasus Spyware." *Thunderbird International Business Review* 65 (3): 355–64. https://doi.org/10.1002/tie.22321.

Kaufmann, Daniel, and Aart Kraay. 2024. "Worldwide Governance Indicators." www.govindicators.org.

Kayali, Laura. 2023. "From Napoléon to Macron: How France Learned to Love Big Brother." Politico. July 24, 2023. https://www.politico.eu/article/france-surveillance-cameras-privacy-security-big-brother-paris-olympics/.

Kelly, Sanja, Mai Truong, Madeline Earp, Laura Reed, Adrian Shahbaz, and Ashley Greco-Stoner. 2013. "Freedom on the Net: A Global Assessment of Internet and Digital Media." Freedom in the Net. Freedom House. https://freedomhouse.org/report/freedom-net/2013/despite-pushback-internet-freedom-deteriorates.

Kendall-Taylor, Andrea, Erica Frantz, and Joseph Wright. 2020. "The Digital Dictators: How Technology Strengthens Autocracy." *Foreign Affairs* 99 (2), 103–15. https://www.foreignaffairs.com/articles/china/2020-02-06/digital-dictators

Kenney, Martin, and John Zysman. 2016. "The Rise of the Platform Economy." *Issues in Science and Technology* 32 (3). https://issues.org/the-rise-of-the-platform-economy/.

Kenyon, Miles. 2019. "Dubious Denials & Scripted Spin: Spyware Company NSO Group Goes on 60 Minutes." The Citizen Lab. April 1, 2019. https://citizenlab.ca/2019/04/dubious-denials-scripted-spin-spyware-company-nso-group-goes-on-60-minutes/.

Keremoğlu, Eda, and Nils B. Weidmann. 2020. "How Dictators Control the Internet: A Review Essay." *Comparative Political Studies*, March, 001041402091227. https://doi.org/10.1177/0010414020912278.

Khudayer, Aiesha Y, Rasha M. Abdulsalam, Suha M. Alshaibani, and Jamaludin Bin Ibrahim. 2014. "Impact of NSA-PRISM to National Information Security Strategy & Policy." *International Journal of Information and Communication Technology Research* 4 (1): 25–31.

King, Gary, Jennifer Pan, and Margaret E Roberts. 2013. "How Censorship in China Allows Government Criticism but Silences Collective Expression." *American Political Science Review* 107 (2): 326–43.

———. 2017. "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument." *American Political Science Review* 111 (3): 484–501.

Kingsley, Patrick, and Ronen Bergman. 2022. "Israel to Investigate Domestic Use of Pegasus Spyware as Scrutiny Hits Home." The New York Times. February 7, 2022. https://www.nytimes.com/2022/02/07/world/middleeast/israel-pegasus-spyware.html.

Kirchgaessner, Stephanie. 2021a. "Saudis behind NSO Spyware Attack on Jamal Khashoggi's Family, Leak Suggests." The Guardian. July 18, 2021. https://www.theguardian.com/world/2021/jul/18/nso-spyware-used-to-target-family-of-jamal-khashoggi-leaked-data-shows-saudis-pegasus.

———. 2021b. "Israeli Firm's Spyware Linked to Attacks on Websites in UK and Middle East." The Guardian. November 16, 2021. https://www.theguardian.com/technology/2021/nov/16/israeli-firm-candiru-spyware-linked-to-attacks-on-websites-uk-middle-east.

———. 2022. "Israel Blocked Ukraine from Buying Pegasus Spyware, Fearing Russia's Anger." The Guardian. March 23, 2022. https://www.theguardian.com/world/2022/mar/23/israel-ukraine-pegasus-spyware-russia.

Kirschbaum, Erik. 2020. "Coronavirus Conspiracy Theories about Mind Control Chips, Bill Gates and Face Masks Fuel Lockdown Protests in Germany." South China Morning Post. May 13, 2020. https://www.scmp.com/news/world/europe/article/3084165/coronavirus-conspiracy-theories-about-mind-control-chips-bill.

Kommers, Daniel P. 1980. "The Jurisprudence of Free Speech in the United States and the Federal Republic of Germany." *Southern California Law Review* 53 (2): 657–95.

Kość, Wojciech. 2022. "Poland's Government Scrambles to Minimize Hacking Backlash." Politico. January 3, 2022. https://www.politico.eu/article/poland-government-scrambles-minimize-hacking-backlash/.

Kostka, Genia, and Lukas Antoine. 2020. "Fostering Model Citizenship: Behavioral Responses to China's Emerging Social Credit Systems." *Policy & Internet* 12 (3): 256–89. https://doi.org/10.1002/poi3.213.

Lai, Yan-ho. 2023. "Securitisation or Autocratisation? Hong Kong's Rule of Law under the Shadow of China's Authoritarian Governance." *Journal of Asian and African Studies* 58 (1): 8–25. https://doi.org/10.1177/00219096221124978.

Laricchia, Federica. 2024. "Smartphone Sales Worldwide 2007-2023." Statista. February 8, 2024. https://www.statista.com/statistics/263437/global-smartphone-sales-to-end-users-since-2007/.

Lavrilleux, Ariane, Harald Schumann, Pascal Hansens, and Alexander Fanta. 2023. "France and Six European States Unite to Authorise the Spying on Journalists." Disclose. December 12, 2023.

https://disclose.ngo/en/article/france-and-six-european-states-unite-to-authorise-the-spying-on-journalists.

Lawrence, Eric, John Sides, and Henry Farrell. 2010. "Self-Segregation or Deliberation? Blog Readership, Participation, and Polarization in American Politics." *Perspectives on Politics* 8 (1): 141–57. https://doi.org/10.1017/S1537592709992714.

Lazzeretti, Luciana, Stefania Oliva, Niccolò Innocenti, and Francesco Capone. 2022. "Rethinking Culture and Creativity in the Digital Transformation." *European Planning Studies*, March, 1–9. https://doi.org/10.1080/09654313.2022.2052018.

Legner, Christine, Torsten Eymann, Thomas Hess, Christian Matt, Tilo Böhmann, Paul Drews, Alexander Mädche, Nils Urbach, and Frederik Ahlemann. 2017. "Digitalization: Opportunity and Challenge for the Business and Information Systems Engineering Community." *Business & Information Systems Engineering* 59 (4): 301–8. https://doi.org/10.1007/s12599-017-0484-2.

Lepido, Daniele. 2019. "Vodafone Found Hidden Backdoors in Huawei Equipment." Bloomberg. April 30, 2019. https://www.bloomberg.com/news/articles/2019-04-30/vodafone-found-hidden-backdoors-in-huawei-equipment.

Leuker, Christina, Lukas Maximilian Eggeling, Nadine Fleischhut, John Gubernath, Ksenija Gumenik, Shahar Hechtlinger, Anastasia Kozyreva, Larissa Samaan, and Ralph Hertwig. 2022. "Misinformation in Germany During the Covid-19 Pandemic: A Cross-Sectional Survey on Citizens' Perceptions and Individual Differences in the Belief in False Information." *European Journal of Health Communication* 3 (2): 13–39. https://doi.org/10.47368/ejhc.2022.202.

Levenson, Michael. 2022. "What We Learned About Pegasus, the Smartphone Cracker." The New York Times. January 28, 2022. https://www.nytimes.com/2022/01/28/world/middleeast/israel-pegasus-spyware.html.

Levinson-Waldman, Rachel, Harsha Panduranga, and Faiza Patel. 2022. "Social Media Surveillance by the U.S. Government." Brennan Center for Justice. January 7, 2022. https://www.brennancenter.org/our-work/research-reports/social-media-surveillance-us-government.

Levitsky, Steven, and Lucan Way. 2002. "The Rise of Competitive Authoritarianism." *Journal of Democracy* 13 (2): 51–65. https://doi.org/10.1353/jod.2002.0026.

———. 2010. *Competitive Authoritarianism: Hybrid Regimes after the Cold War*. Problems of International Politics. New York: Cambridge University Press.

Levitsky, Steven, and Daniel Ziblatt. 2018. *How Democracies Die*. First edition. New York: Crown.

Levy, Jack S. 2008. "Case Studies: Types, Designs, and Logics of Inference." *Conflict Management and Peace Science* 25 (1): 1–18.

Lewis, James Andrew. 2014. "Reference Note on Russian Communications Surveillance." https://www.csis.org/analysis/reference-note-russian-communications-surveillance.

Li, King C., Peter Marcovici, Andrew Phelps, Christopher Potter, Allison Tillack, Jennifer Tomich, and Srini Tridandapani. 2013. "Digitization of Medicine." *Academic Radiology* 20 (12): 1479–94. https://doi.org/10.1016/j.acra.2013.09.008.

Lijphart, Arend. 1999. *Patterns of Democracy*. New Haven: Yale University Press.

Linz, Juan J. 1964. "An Authoritarian Regime: Spain." In *Cleavages, Ideologies and Party Systems: Contributions to Comparative Political Sociology*, edited by Erik Allardt and Yrjo Litunen, 291–323. Helsinki: The Academic Bookstore.

———. 1975. *Totalitarian and Authoritarian Regimes*. Boulder, CO: Lynne Rienner Publishers.

———. 1978. *The Breakdown of Democratic Regimes: Crisis, Breakdown and Reequilibration. An Introduction*. Johns Hopkins University Press.

Lipset, Seymour Martin. 1959. *Political Man: The Social Bases of Politics*. Garden City: Doubleday.

Maas, Rüdiger. 2020. *Was Hat Bill Gates Mit Corona Zu Tun? Ein Buch Über Die Entstehung von Verschwörungstheorien Und Den Umgang Mit Ihnen. [What Does Bill Gates Have to Do with Corona? A Book About the Emergence of Conspiracy Theories and Dealing with Them]*. Norderstedt: Books on Demand.

Maati, Ahmed, Mirjam Edel, Koray Saglam, Oliver Schlumberger, and Chonlawit Sirikupt. 2023. "Information, Doubt, and Democracy: How Digitization Spurs Democratic Decay." *Democratization*, August, 1–21. https://doi.org/10.1080/13510347.2023.2234831.

Maati, Ahmed, and Žilvinas Švedkauskas. 2020. "Framing the Pandemic and the Rise of the Digital Surveilance State." *Mezinárodní Vztahy* 55 (4): 48–71. https://doi.org/10.32422/mv-cjir.1736.

———. 2021. "Long-Term Prescription? Digital Surveillance Is Here to Stay." *Mezinárodní Vztahy* 56 (4): 105–18. https://doi.org/10.32422/mv-cjir.1821.

Mac, Ryan, and Sheera Frenkel. 2021. "Facebook Papers Show Employees Raised Concerns About Misinformation." The New York Times. October 22, 2021. https://www.nytimes.com/2021/10/22/technology/facebook-election-misinformation.html.

Maerz, Seraphine F. 2016. "The Electronic Face of Authoritarianism: E-Government as a Tool for Gaining Legitimacy in Competitive and Non-Competitive Regimes." *Government Information Quarterly* 33 (4): 727–35. https://doi.org/10.1016/j.giq.2016.08.008.

Marczak, Bill, and Sarah McKune. 2015. "What We Know about the South Korea NIS's Use of Hacking Team's RCS." Citizen Lab Research Report No. 58. Citizen Lab University of Toronto. https://citizenlab.ca/2015/08/what-we-know-about-the-south-korea-niss-use-of-hacking-teams-rcs/.

Marczak, Bill, and John Scott-Railton. 2016. "THE MILLION DOLLAR DISSIDENT - NSO Group's iPhone Zero-Days Used against a UAE Human Rights Defender." Citizen Lab Research Report 78. Canada: University of Toronto. https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/.

Martin, Kirsten. 2022. "Recommending an Insurrection: Facebook and Recommendation Algorithms." In *Ethics of Data and Analytics*, by Martin, First edition. Boca Raton: CRC Press/Tyalor & Francis Group.

Marzocchi, Ottavio, and Martina Mazzini. 2022. "Pegasus and Surveillance Spyware." Pegasus and surveillance spyware Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies PE 732.268 - May 2022 EN In-Depth Analysis for the PEGASUS committee PE 732.268. Brussels: European Parliament Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies. https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/732268/IPOL_IDA(2022)732268_EN.pdf.

Massi, Marta, ed. 2021. *Digital Transformation in the Cultural and Creative Industries: Production, Consumption and Entrepreneurship in the Digital and Sharing Economy*. Routledge Research in the Creative & Cultural Industries. Abingdon, Oxon ; New York, NY: Routledge.

Mayer, Maximilian, and Yen-Chi Lu. 2022. "Digital Autonomy? Measuring the Global Digital Dependence Structure." Bonn.: Center for Advanced Security, Strategic and Integration Studies.

https://www.kas.de/documents/252038/16166715/Digital+Autonomy+-+Measuring+the+Global+Digital+Dependence+Structure.pdf/fb97d384-53fd-b747-908f-2c86e8d0674b?version=1.2&t=1651491803819.

McCabe, David. 2019. "G.O.P.-Led Senate Panel Affirms Russia Attacked Election, and Urges Action." The New York Times. October 8, 2019. https://www.nytimes.com/2019/10/08/business/senate-report-russia-election.html.

McCoy, Jennifer, Tahmina Rahman, and Murat Somer. 2018. "Polarization and the Global Crisis of Democracy: Common Patterns, Dynamics, and Pernicious Consequences for Democratic Polities." *American Behavioral Scientist* 62 (1): 16–42. https://doi.org/10.1177/0002764218759576.

McIntyre, Niamh, Rosie Bradbury, and Billy Perrigo. 2022. "Behind TikTok's Boom: A Legion of Traumatised, $10-a-Day Content Moderatos." The Bureau of Investigative Journalism. October 20, 2022. https://www.thebureauinvestigates.com/stories/2022-10-20/behind-tiktoks-boom-a-legion-of-traumatised-10-a-day-content-moderators.

McKay, Spencer, and Chris Tenove. 2021. "Disinformation as a Threat to Deliberative Democracy." *Political Research Quarterly* 74 (3): 703–17. https://doi.org/10.1177/1065912920938143.

Mechkova, Valeriya, Daniel Pemstein, Brigitte Seim, and Steven Wilson. 2019. "Measuring Internet Politics: Introducing the Digital Society Project (DSP)." 1. Gothenburg, Sweden: Digital Society Project. http://digitalsocietyproject.org/wp-content/uploads/2022/08/DSP_working_paper_1_v4.pdf.

Merkel, Wolfgang. 2004. "Embedded and Defective Democracies." *Democratization* 11 (5): 33–58. https://doi.org/10.1080/13510340412331304598.

Merrill, Jeremy B., and Olivia Goldhill. 2020. "Cambridge Analytica Used These 5 Political Ads to Target Voters." Quartz. January 10, 2020. https://qz.com/1782348/cambridge-analytica-used-these-5-political-ads-to-target-voters/.

Messler, Norbert. 1986. *The Art Deco Skyscraper in New York*. 2nd rev. ed. New York: P. Lang.

Meyer, Jan Nicola, and Jana-Maria Böswald. 2022. "Mapping the Tools, Tactics and Narratives of Tomorrow's Disinformation Environment." Berlin: Democracy Reporting International. https://democracyreporting.s3.eu-central-1.amazonaws.com/images/62c8333ec3aea.pdf.

Michaelsen, Marcus. 2020. "The Digital Transnational Repression Toolkit, and Its Silencing Effects." Freedom House. 2020. https://freedomhouse.org/report/special-report/2020/digital-transnational-repression-toolkit-and-its-silencing-effects.

Michaelsen, Marcus, and Marlies Glasius. 2018. "Authoritarian Practices in the Digital Age—Introduction." *International Journal of Communication* 12: 3788–94. https://doi.org/n.a.

Middle East Monitor. 2019. "Spyware Developed in Israel Used by Saudis to Hack London-Based Dissident." Middle East Monitor. May 29, 2019. https://www.middleeastmonitor.com/20190529-spyware-developed-in-israel-used-by-saudis-to-hack-london-based-dissident/.

Møller, Jørgen, and Svend-Erik Skaaning. 2010. "Beyond the Radial Delusion: Conceptualizing and Measuring Democracy and Non-Democracy." *International Political Science Review* 31 (3): 261–83. https://doi.org/10.1177/0192512110369522.

Mouffe, Chantal. 1999. "Deliberative Democracy or Agonistic Pluralism?" *Social Research* 66 (3): 745–58.

Mozilla. 2019. "Mozilla Takes Action to Protect Users in Kazakhstan." The Mozilla Blog. August 21, 2019. https://blog.mozilla.org/blog/2019/08/21/mozilla-takes-action-to-protect-users-in-kazakhstan.

Mozur, Paul, Jonah M. Kessel, and Melissa Chan. 2019. "Made in China, Exported to the World: The Surveillance State." The New York Times. April 24, 2019. https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html.

Mufti, Mariam. 2018. "What Do We Know about Hybrid Regimes after Two Decades of Scholarship?" *Politics and Governance* 6 (2): 112. https://doi.org/10.17645/pag.v6i2.1400.

Mussington, David. 2021. "Securing the Critical National Infrastructure." In *The Oxford Handbook of Cyber Security*, edited by Paul Cornish, First edition, 429–46. Oxford: Oxford University Press.

Nagel, Michael. 2005. "Constructing Apathy: How Environmentalism and Environmental Education May Be Fostering 'Learned Hopelessness' in Children." *Australian Journal of Environmental Education* 21 (January): 71–80. https://doi.org/10.1017/S0814062600000963.

Nanos, Janelle. 2018. "How Companies Use Geolocation Data to Target You." Boston Globe. July 2018. https://apps.bostonglobe.com/business/graphics/2018/07/foot-traffic.

Nazzaro, Miranda. 2023. "Putin Calls Musk an 'Outstanding Person' after Starlink Revelations." The Hill. September 12, 2023. https://thehill.com/policy/international/4200236-putin-calls-musk-an-outstanding-person-after-starlink-revelations/.

Neu, Viola. 2023. "'It's All Been Proven.'" Monitor - Wahl und Sozialforschung. Berlin: Konrad Adenauer Stiftung. https://www.kas.de/en/election-and-social-research-monitor/detail/-/content/it-s-all-been-proven.

Neubauer, Deane E. 1967. "Some Conditions of Democracy." *The American Political Science Review* 61 (4): 1002–9. https://doi.org/10.2307/1953402.

Nisbet, Erik C, and Olga Kamenchuk. 2021. "Russian News Media, Digital Media, Informational Learned Helplessness, and Belief in COVID-19 Misinformation." *International Journal of Public Opinion Research* 33 (3): 571–90. https://doi.org/10.1093/ijpor/edab011.

Nordic Monitor. 2022. "Inaction of Erdoğan's Political Rival on Hacking Scandal Unmasks Cowed Opposition in Turkey." Nordic Monitor. April 11, 2022. https://nordicmonitor.com/2022/04/inaction-of-erdogans-political-rival-about-hacking-scandal-unmasks-cowed-opposition-in-turkey/.

O'Carroll, Lisa. 2023. "Draft EU Plans to Allow Spying on Journalists Are Dangerous, Warn Critics." The Guardian. June 22, 2023. https://www.theguardian.com/world/2023/jun/22/draft-eu-plans-to-allow-spying-on-journalists-are-dangerous-warn-critics.

O'Reilly, Colin, and Ryan H. Murphy. 2022a. "An Index Measuring State Capacity, 1789–2018." *Economica* 89 (355): 713–45. https://doi.org/10.1111/ecca.12411.

———. 2022b. "State Capacity Index." Colin W. O'Reilly. 2022. http://www.colinworeilly.com/state-capacity-index.html.

Orwell, George. 1949. *1984*. London: Penguin Books in association with Martin Secker & Warburg Ltd.

Oxford Internet Institute. 2021. "Social Media Manipulation by Political Actors Now an Industrial Scale Problem Prevalent in over 80 Countries – Annual Oxford Report." 2021. https://www.oii.ox.ac.uk/news-events/news/social-media-manipulation-by-political-actors-now-an-industrial-scale-problem-prevalent-in-over-80-countries-annual-oxford-report.

Palmer, Ewan. 2022. "Fact Check: Did Donald Trump Truth Social App Top Google Play Store Chart?" Newsweek. October 19, 2022. https://www.newsweek.com/trump-truth-social-app-google-play-store-1753210.

Palmer, Katharine. 2024. "Branching Out: Factors Motivating Nondemocratic Use of Commodity Spyware." *International Journal of Intelligence and Counter Intelligence* 37 (1): 286–306. https://doi.org/10.1080/08850607.2023.2202345.

Pan, Jennifer, and Alexandra A. Siegel. 2020. "How Saudi Crackdowns Fail to Silence Online Dissent." *American Political Science Review* 114 (1): 109–25. https://doi.org/10.1017/S0003055419000650.

Pancevski, Bojan. 2020. "U.S. Officials Say Huawei Can Covertly Access Telecom Networks." The Wall Street Journal. February 12, 2020. https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256.

Papaioannou, Kostas, Myrto Pantazi, and Jan-Willem van Prooijen. 2023. "Is Democracy under Threat? Why Belief in Conspiracy Theories Predicts Autocratic Attitudes." *European Journal of Social Psychology* 53 (5): 846–56. https://doi.org/10.1002/ejsp.2939.

Parent, Deepa, and Katie McQue. 2023. "'I Log into a Torture Chamber Each Day': The Strain of Moderating Social Media." The Guardian. September 11, 2023. https://www.theguardian.com/global-development/2023/sep/11/i-log-into-a-torture-chamber-each-day-strain-of-moderating-social-media-india.

Peceny, Mark, and Caroline C. Beer. 2003. "Peaceful Parties and Puzzling Personalists." *American Political Science Review* 97 (02): 339–42. https://doi.org/10.1017/S0003055403000716.

Pereira, Daniel. 2020. "Facebook Business Model." Blog/News. The Business Model Analyst. August 28, 2020. https://businessmodelanalyst.com/facebook-business-model/.

Perlroth, Nicole. 2016. "How Spy Tech Firms Let Governments See Everything on a Smartphone." The New York Times. September 2, 2016. https://www.nytimes.com/2016/09/03/technology/nso-group-how-spy-tech-firms-let-governments-see-everything-on-a-smartphone.html.

Perlroth, Nicole, Michael Wines, and Matthew Rosenberg. 2017. "Russian Election Hacking Efforts, Wider Than Previously Known, Draw Little Scrutiny." The New York Times. September 1, 2017. https://www.nytimes.com/2017/09/01/us/politics/russia-election-hacking.html.

Philbeck, Thomas, and Nicholas Davis. 2018. "The Fourth Industrial Revolution: Shaping a New Era." *Journal of International Affairs* 72 (1): 17–22.

Pierce, David, and Anna Kramer. 2021. "Here Are All the Facebook Papers Stories." Protocol. October 25, 2021. https://www.protocol.com/facebook-papers.

Pilling, David, and Madhumita Murgia. 2023. "'You Can't Unsee It': The Content Moderators Taking on Facebook." Financial Times. May 18, 2023. https://www.ft.com/content/afeb56f2-9ba5-4103-890d-91291aea4caa.

Polyakova, Alina, and Chris Meserole. 2019. "Exporting Digital Authoritarianism: The Russian and Chinese Models." *Policy Brief, Democracy and Disorder Series (Washington, DC: Brookings, 2019)*, 1–22.

Polyanskaya, Anna, Andrey Krivov, and Ivan Lomko. 2003. "Big Brother's Virtual Eye – a Research Approach." *Журнал Вестник [Vestnik Online]* 3 (320): n.a. via Wayback Machine: https://web.archive.org/web/20191219182655/http://www.vestnik.com/issues/2003/0430/win/polyanskaya_krivov_lomko.htm

Pond, Philip. 2020. *Complexity, Digital Media and Post Truth Politics: A Theory of Interactive Systems*. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-44537-9.

Prebisch, Raúl. 1950. "The Economic Development of Latin America and Its Principal Problems." E/CN.12/89/REV.1. New York: United Nations - Department of Economic Affairs. https://repositorio.cepal.org/items/9a00fa5b-ad04-4520-ae4c-e3adba791790.

Priest, Dana, Craig Timberg, and Souad Mekhennet. 2021. "Private Israeli Spyware Used to Hack Cellphones of Journalists, Activists Worldwide." Washington Post. July 18, 2021. https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/.

Purnell, Newley, and Jeff Horwitz. 2021. "Facebook Services Are Used to Spread Religious Hatred in India, Internal Documents Show." The Wall Street Journal. October 23, 2021. https://www.wsj.com/articles/facebook-services-are-used-to-spread-religious-hatred-in-india-internal-documents-show-11635016354.

Qiang, Xiao. 2019. "The Road to Digital Unfreedom: President XI's Surveillance State." *Journal of Democracy* 30 (1): 53–67. https://doi.org/10.1353/jod.2019.0004.

Reporters Without Borders. 2018. "ONLINE HARASSMENT OF JOURNALISTS - Attack of the Trolls." Paris: Reporters Without Borders. https://rsf.org/sites/default/files/rsf_report_on_online_harassment.pdf.

———. 2020. "RSF Unveils 20/2020 List of Press Freedom's Digital Predators." Reporters Without Borders. March 10, 2020. https://rsf.org/en/rsf-unveils-202020-list-press-freedom-s-digital-predators.

———. 2023a. "Analysis 2022: Europe - Central Asia - Polarisation to the West, War & Propaganda to the East The European Union Caught between Two Extremes." Reporters Without Borders. 2023. https://rsf.org/en/classement/2022/europe-central-asia.

———. 2023b. "Charges Brought against Former FinFisher Group CEOs." Reporters Withour Borders . May 31, 2023. https://rsf.org/en/charges-brought-against-former-finfisher-group-ceos.

———. 2023c. "Member States Must Do More to Implement European Commission's Recommendation on Journalists' Safety." Reporters Without Borders. September 18, 2023. https://rsf.org/en/member-states-must-do-more-implement-european-commissions-recommendation-journalists-safety.

Repucci, Sarah, and Amy Slipowitz. 2022. "The Global Expansion of Authoritarian Rule." Washington, DC: Freedom House. https://freedomhouse.org/report/freedom-world/2022/global-expansion-authoritarian-rule.

Roberts, Margaret E. 2020. "Resilience to Online Censorship." *Annual Review of Political Science* 23 (1): 401–19. https://doi.org/10.1146/annurev-polisci-050718-032837.

Robertson, Roland, and Kathleen E. White. 2007. "What Is Globalization?" In *The Blackwell Companion to Globalization*, edited by George Ritzer, 54–66. Malden, MA; Oxford: Blackwell Pub.

Rød, Espen Geelmuyden, and Nils B Weidmann. 2015. "Empowering Activists or Autocrats? The Internet in Authoritarian Regimes." *Journal of Peace Research* 52 (3): 338–51. https://doi.org/10.1177/0022343314555782.

Rosenberg, Matthew. 2018. "Cambridge Analytica, Trump-Tied Political Firm, Offered to Entrap Politicians." The New York Times. March 19, 2018. https://www.nytimes.com/2018/03/19/us/cambridge-analytica-alexander-nix.html.

Ross Arguedass, Amy, Craig T. Robertson, Richard Fletcher, and Rasmus K. Nielsen. 2022. *Echo Chambers, Filter Bubbles, and Polarisation: A Literature Review*. Oxford: Reuters Institute for the Study of Journalism.

Rueckert, Phineas. 2021. "Pegasus: The New Global Weapon for Silencing Journalists." Forbidden Stories. July 18, 2021. https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/.

Russu, Catalina. 2022. "The Impact of Low Cyber Security on the Development of Poor Nations." Development Aid. September 12, 2022. https://www.developmentaid.org/news-stream/post/149553/low-cyber-security-and-development-of-poor-nations.

Safai, Yalda. 2020. "Managing the Psychological Effects of the 2020 Election." ABC News. November 3, 2020. https://abcnews.go.com/Health/managing-psychological-effects-2020-election/story?id=73933000.

Saglam, Koray. 2022. "The Digital Blender: Conceptualizing the Political Economic Nexus of Digital Technologies and Authoritarian Practices." *Globalizations*, October, 1–18. https://doi.org/10.1080/14747731.2022.2131235.

———. forthcoming. "Shopping with Orwell: Procurement Patterns of Commercialized Surveillance Software." *Unpublished Manuscript*.

Salinas, Sara. 2018. "Facebook Says the Number of Users Affected by Cambridge Analytica Data Leak Is 87 Million." CNBC. April 4, 2018. https://www.cnbc.com/2018/04/04/facebook-updates-the-number-of-users-impacted-by-cambridge-analytica-leak-to-87-million-.html.

Saloojee, Yussuf, and Elif Dagli. 2000. "Tobacco Industry Tactics for Resisting Public Policy on Health." *Bulletin of the World Health Organization* 78 (7): 902–10.

Santos, Theotonio Dos. 1970. "The Structure of Dependence." *The American Economic Review* 60 (2): 231–36.

Sartori, Giovanni. 1976. *Parties and Party Systems: A Framework for Analysis*. Cambridge: Cambridge University Press.

Schäfer, Mike S. 2016. "Digital Public Sphere." In *The International Encyclopedia of Political Communication*, edited by Gianpietro Mazzoleni, Kevin G. Barnhurst, Ken'ichi Ikeda, Rousiley C. M. Maia, and Hartmut Wessler, 1st ed., 1–7. Wiley. https://doi.org/10.1002/9781118541555.wbiepc087.

Schaffer, Aaron. 2020. "Israeli Spyware Company Accused of Hacking Activists Hires Lobby Firm - Al-Monitor: The Pulse of the Middle East." Al-Monitor: The Pulse of the Middle East. January 10, 2020. https://www.al-monitor.com/originals/2020/01/nso-group-surveillance-khashoggi-lobbying-mercury.html.

Schechner, Sam, Jeff Horwitz, and Emily Glazer. 2021. "How Facebook Hobbled Mark Zuckerberg's Bid to Get America Vaccinated." The Wall Street Journal. September 17, 2021. https://www.wsj.com/articles/facebook-mark-zuckerberg-vaccinated-11631880296.

Scheck, Justin, Newley Purnell, and Jeff Horwitz. 2021. "Facebook Employees Flag Drug Cartels and Human Traffickers. The Company's Response Is Weak, Documents Show." The Wall Street Journal. September 16, 2021. https://www.wsj.com/articles/facebook-drug-cartels-human-traffickers-response-is-weak-documents-11631812953.

Schedler, Andreas. 2013. *The Politics of Uncertainty: Sustaining and Subverting Electoral Authoritarianism*. 1st ed. Oxford Studies in Democratization. Oxford: New York, NY: Oxford University Press.

Scheurman, Trent. 2022. "Comparing Social Media Content Regulation in the US and the EU: How the US Can Move Forward With Section 230 to Bolster Social Media Users' Freedom of Expression." *San Diego International Law Journal* 23 (2): 413.

Schlumberger, Oliver, Mirjam Edel, Ahmed Maati, and Koray Saglam. 2023. "How Authoritarianism Transforms: A Framework for the Study of Digital Dictatorship." *Government and Opposition*, July, 1–23. https://doi.org/10.1017/gov.2023.20.

Schlumberger, Oliver, and Tasha Schedler. 2020. "Authoritarianisms and Authoritarianization." In *The SAGE Handbook of Political Science*, edited by Dirk Berg-Schlosser, Bertrand Badie, and Leonardo Morlino, 1st ed., 2:712–29. 1 Oliver's Yard, 55 City Road London EC1Y 1SP: SAGE Publications Ltd. https://doi.org/10.4135/9781529714333.n45.

Schmelzer, Mike, and Alexandra Karppi. 2024. "Nations in Transit 2024." Freedom House Report. Washington, DC: Freedom House. https://freedomhouse.org/report/nations-transit/2022/from-democratic-decline-to-authoritarian-aggression.

Schwab, Klaus. 2016a. *The Fourth Industrial Revolution*. First U.S. edition. New York: Crown Business.

———. 2016b. "The Fourth Industrial Revolution: What It Means and How to Respond." World Economic Forum. January 14, 2016. https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/.

Scott, Mark. 2024. "The EU's Online Content Rulebook Isn't Ready for Primetime." Politico. February 14, 2024. https://www.politico.eu/article/european-union-digital-services-act-dsa-thierry-breton/.

Scott-Railton, John, Elies Campo, Bill Marczak, Bahr Abdul Razzak, Siena Anstis, Gözde Böcü, Salvatore Solimano, and Ron Deibert. 2022. "CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru." Citizen Lab, University of Toronto. https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/.

Shahbaz, Adrian. 2018. "Freedom on the Net 2018 - The Rise of Digital Authoritarianism." Freedom House Report. Freedom on the Net. Washington, DC: Freedom House. https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf.

Shahbaz, Adrian, and Allie Funk. 2019. "The Crisis of Social Media." Freedom House Report. Freedom on the Net. Washington, DC: Freedom House. https://freedomhouse.org/sites/default/files/2019-11/11042019_Report_FH_FOTN_2019_final_Public_Download.pdf.

Sherman, Justin. 2019. "Digital Authoritarianism and the Threat to Global Democracy - Bulletin of the Atomic Scientists." Bulletin of the Atomic Scientists. July 25, 2019. https://thebulletin.org/2019/07/digital-authoritarianism-and-the-threat-to-global-democracy/.

Siebenhaar, Katharina U., Anja K. Köther, and Georg W. Alpers. 2020. "Dealing With the COVID-19 Infodemic: Distress by Information, Information Avoidance, and Compliance With Preventive Measures." *Frontiers in Psychology* 11 (November): 567905. https://doi.org/10.3389/fpsyg.2020.567905.

Silverio-Fernández, Manuel, Suresh Renukappa, and Subashini Suresh. 2018. "What Is a Smart Device? - A Conceptualisation within the Paradigm of the Internet of Things." *Visualization in Engineering* 6 (1): 3. https://doi.org/10.1186/s40327-018-0063-8.

Singer, Hans Wolfgang. 1950. "The Distribution of Gains between Investing and Borrowing Countries." *The American Economic Review* 40 (2): 473–85.

Sinpeng, Aim. 2021. *Opposing Democracy in the Digital Age: The Yellow Shirts in Thailand*. Ann Arbor, MI: University of Michigan Press. https://doi.org/10.3998/mpub.11666233.

Slater, Dan. 2010. *Ordering Power: Contentious Politics and Authoritarian Leviathans in Southeast Asia*. Cambridge University Press.

Śledziewska, Katarzyna, and Renata Włoch. 2021. *The Economics of Digital Transformation: The Disruption of Markets, Production, Consumption, and Work*. 1st ed. Abingdon, Oxon ; New York, NY : Routledge. https://doi.org/10.4324/9781003144359.

Smidi, Adam, and Saif Shahin. 2017. "Social Media and Social Mobilisation in the Middle East: A Survey of Research on the Arab Spring." *India Quarterly: A Journal of International Affairs* 73 (2): 196–209. https://doi.org/10.1177/0974928417700798.

Smith, Ben. 2021. "Inside the Big Facebook Leak." The New York Times. October 25, 2021. https://www.nytimes.com/2021/10/24/business/media/facebook-leak-frances-haugen.html.

Smith, Cameron. 2018. "Race and the Logic of Radicalisation under Neoliberalism." *Journal of Sociology* 54 (1): 92–107. https://doi.org/10.1177/1440783318759093.

Smith, Helena. 2023. "Greek Government Faces Confidence Vote over Spying Row." The Guardian. January 25, 2023. https://www.theguardian.com/world/2023/jan/25/opposition-file-no-confidence-motion-greek-watergate-scandal-prime-minister-kyriakos-mitsotakis-wiretaps.

Staab, Philipp. 2019. *Digitaler Kapitalismus*. Berlin: Suhrkamp.

Starr, Paul. 2019. "How Neoliberal Policy Shaped the Internet—and What to Do About It Now." The American Prospect. October 2, 2019. https://prospect.org/api/content/e4fb9f4a-e460-11e9-9156-12f1225286c6/.

Statista. 2022. "Instagram Users Worldwide 2025." Statista. 2022. https://www.statista.com/statistics/183585/instagram-number-of-global-users/.

Stavrositu, Carmen. 2014. "Selective Exposure." In *Encyclopedia of Social Media and Politics*, edited by Kerric Harvey, 1117–19. Thousand Oaks: SAGE.

Steele, Christopher D., Ammal Abbasi, S. M. Ashiqul Islam, Amy L. Bowes, Azhar Khandekar, Kerstin Haase, Shadi Hames-Fathi, et al. 2022. "Signatures of Copy Number Alterations in Human Cancer." *Nature* 606 (7916): 984–91. https://doi.org/10.1038/s41586-022-04738-6.

Stevenson, Alexandra. 2018. "Facebook Admits It Was Used to Incite Violence in Myanmar." The New York Times. November 6, 2018. https://www.nytimes.com/2018/11/06/technology/myanmar-facebook.html.

Stroud, Natalie Jomini. 2008. "Media Use and Political Predispositions: Revisiting the Concept of Selective Exposure." *Political Behavior* 30 (3): 341–66. https://doi.org/10.1007/s11109-007-9050-9.

Suhr, Frauke. 2020. "Das halten die Deutschen von Verschwörungsmythen" "[This Is What the Germans Think of Conspiracy Myths]." Statista. September 14, 2020. https://de.statista.com/infografik/22882/anteil-der-befragten-dazu-was-sie-von-verschwoerungsmythen-halten.

Suiter, Jane. 2016. "Post-Truth Politics." *Political Insight* 7 (3): 25–27. https://doi.org/10.1177/2041905816680417.

Švedkauskas, Žilvinas, Chonlawit Sirikupt, and Michel Salzer. 2020. "Russia's Disinformation Campaigns Are Targeting African Americans." Washington Post. July 24, 2020. https://www.washingtonpost.com/politics/2020/07/24/russias-disinformation-campaigns-are-targeting-african-americans/.

Swire, Briony, Ullrich K. H. Ecker, and Stephan Lewandowsky. 2017. "The Role of Familiarity in Correcting Inaccurate Information." *Journal of Experimental Psychology: Learning, Memory, and Cognition* 43 (12): 1948–61. https://doi.org/10.1037/xlm0000422.

SWNS Staff. 2021. "Nearly Half of Americans Convinced Dinosaurs Still Exist in a Remote Corner of the World." Yahoo News. June 1, 2021. https://uk.news.yahoo.com/nearly-half-americans-convinced-dinosaurs-151600448.html.

Tansel, Cemal Burak, ed. 2017. *States of Discipline: Authoritarian Neoliberalism and the Contested Reproduction of Capitalist Order*. Transforming Capitalism. London; New York: Rowman & Littlefield International.

———. 2018. “Authoritarian Neoliberalism and Democratic Backsliding in Turkey: Beyond the Narratives of Progress.” *South European Society and Politics* 23 (2): 197–217. https://doi.org/10.1080/13608746.2018.1479945.

Teloglou, Tasos, Eliza Triantafillou, Crofton Black, Omer Benjakob, Avi Scharf, Tomas Statius, Gabriel Geiger, et al. 2022. “Flight of the Predator.” Lighthouse Reports. November 30, 2022. https://www.lighthousereports.com/investigation/flight-of-the-predator/.

Tennis, Maggie. 2020. “Russia Ramps up Global Elections Interference: Lessons for the United States.” NGO/Blog/News. Center for Strategic and International Studies. July 20, 2020. https://www.csis.org/blogs/technology-policy-blog/russia-ramps-global-elections-interference-lessons-united-states.

Teorell, Jan, and Axel Hadenius. 2006. “Democracy without Democratic Values: A Rejoinder to Welzel and Inglehart.” *Studies in Comparative International Development* 41 (3): 95–111. https://doi.org/10.1007/BF02686238.

Tesquet, Par Olivier. 2017. “Amesys: Egyptian trials and tribulations of a French digital arms dealer.” Télérama. July 5, 2017. https://www.telerama.fr/monde/amesys-egyptian-trials-and-tribulations-of-a-french-digital-arms-dealer,160452.php.

Think Impact. 2021. “50+ Whatsapp Statistics 2022 - Usage and Revenue [Updadet].” Think Impact. August 9, 2021. https://www.thinkimpact.com/whatsapp-statistics/.

Thomas, Elise, and Albert Zhang. 2020. “ID2020, Bill Gates and the Mark of the Beast: How Covid-19 Catalyses Existing Online Conspiracy Movements.” Australian Strategic Policy Institute. https://www.jstor.org/stable/resrep25082.

Tidy, Joe. 2019. “I Was a Victim of the WhatsApp Hack.” News. BBC News. 2019. https://www.bbc.com/news/technology-50249859.

Timberg, Craig, Elizabeth Dwoskin, and Reed Albergotti. 2021. “Inside Facebook, Jan. 6 Violence Fueled Anger, Regret over Missed Warning Signs.” The Washington Post. October 22, 2021. https://www.washingtonpost.com/technology/2021/10/22/jan-6-capitol-riot-facebook/.

Tolan, Casey. 2021. “The Operative.” CNN. 2021. https://edition.cnn.com/interactive/2021/06/us/capitol-riot-paths-to-insurrection/amy-kremer.html.

Travère, Audrey. 2021. "The Rise and Fall of NSO Group." Translated by Phineas Rueckert. Forbidden Stories. July 19, 2021. https://forbiddenstories.org/the-rise-and-fall-of-nso-group/.

Tsourapas, Gerasimos. 2020. "Global Autocracies: Strategies of Transnational Repression, Legitimation, and Co-Optation in World Politics." *International Studies Review*, August, viaa061. https://doi.org/10.1093/isr/viaa061.

Tucker, Joshua, Andrew Guess, Pablo Barbera, Cristian Vaccari, Alexandra Siegel, Sergey Sanovich, Denis Stukal, and Brendan Nyhan. 2018. "Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature." *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3144139.

Turillazzi, Aina, Mariarosaria Taddeo, Luciano Floridi, and Federico Casolari. 2023. "The Digital Services Act: An Analysis of Its Ethical, Legal, and Social Implications." *Law, Innovation and Technology* 15 (1): 83–106. https://doi.org/10.1080/17579961.2023.2184136.

UCLA: Statistical Consulting Group. 2021a. "How Can I Analyze Count Data in Stata?" UCLA Advanced Research Computing Statistical Methods and Data Analytics. 2021. https://stats.oarc.ucla.edu/stata/faq/how-can-i-analyze-count-data-in-stata/.

———. 2021b. "Negative Binomial Regression | Stata Data Analysis Examples." UCLA Advanced Research Computing Statistical Methods and Data Analytics. 2021. https://stats.oarc.ucla.edu/stata/dae/negative-binomial-regression/.

Urbach, Nils, and Maximilian Röglinger, eds. 2019. *Digitalization Cases: How Organizations Rethink Their Business for the Digital Age*. Management for Professionals. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-95273-4.

U.S. Securities and Exchange Commission. 2021. "United States Securities and Exchange Commission - Facebook Inc." Government Agency. United States Securities and Exchange Commission. 2021. https://www.sec.gov/ix?doc=/Archives/edgar/data/1326801/000132680121000014/fb-20201231.htm.

Vaccari, Cristian, and Andrew Chadwick. 2020. "Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News." *Social Media & Society* 6 (1): 205630512090340. https://doi.org/10.1177/2056305120903408.

V-Dem. 2022. "Varieties of Democracy - Dataset Version 12." Gothenburg, Sweden: University of Gothenburg. https://www.v-dem.net/static/website/img/refs/codebookv12.pdf.

Volk, Sabine. 2021. "Political Performances of Control During COVID-19: Controlling and Contesting Democracy in Germany." *Frontiers in Political Science* 3 (June): 654069. https://doi.org/10.3389/fpos.2021.654069.

Vosoughi, Soroush, Deb Roy, and Sinan Aral. 2018. "The Spread of True and False News Online." *Science* 359 (6380): 1146–51. https://doi.org/10.1126/science.aap9559.

VSquare. 2023. "How EU Countries Spy on Their Citizens." VSquare. August 28, 2023. https://vsquare.org/pegasus-spyware-poland-hungary-slovakia-romania/.

Walker, Shaun. 2021. "Viktor Orbán Accused of Using Pegasus to Spy on Journalists and Critics." The Guardian. July 18, 2021. http://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests.

Wallerstein, Immanuel. 2004. *World-Systems Analysis: An Introduction*. Durham, North Carolina: Duke University Press. https://doi.org/10.1515/9780822399018.

Wardle, Claire, and Hossein Derakhshan. 2017. "Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making." Council of Europe report DGI(2017)09. Strasbourg: Council of Europe. https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c.

Washington Post. 2021. "Takeaways from the Pegasus Project." The Washington Post. July 18, 2021. https://www.washingtonpost.com/investigations/2021/07/18/takeaways-nso-pegasus-project/.

Weber, Max. 1921. *Wirtschaft Und Gesellschaft [Economy and Society]*. Edited by Johannes Winckelmann. 5., rev. Edition 1972. Tübingen: Mohr Siebeck.

Weidmann, Nils B., and Espen Geelmuyden Rød. 2019. *The Internet and Political Protest in Autocracies*. Oxford Studies in Digital Politics. New York, NY: Oxford University Press.

Welzel, Christian, and Ronald F. Inglehart. 2019. "Political Culture, Mass Beliefs, and Value Change." In *Democratization*, edited by Christian Haerpfer and Ronald F. Inglehart, 126–44. Oxford University Press. https://doi.org/10.1093/hepl/9780198732280.003.0009.

Wenzel, Andrea. 2019. "To Verify or to Disengage: Coping with 'Fake News' and Ambiguity." *International Journal of Communication* 13 (n.a.): 1977–95.

West, Darrell M. 2012. *Digital Schools: How Technology Can Transform Education*. Washington, D.C: Brookings Institution Press.

Wong, Julia Carrie. 2020. "Down the Rabbit Hole: How QAnon Conspiracies Thrive on Facebook." The Guardian. June 25, 2020. https://www.theguardian.com/technology/2020/jun/25/qanon-facebook-conspiracy-theories-algorithm.

World Bank. 2024a. "GDP per Capita (Current US$)." World Bank Open Data. 2024. https://data.worldbank.org/indicator/NY.GDP.PCAP.CD.

———. 2024b. "World Bank Open Data." World Bank Open Data. 2024. https://data.worldbank.org.

World Economic Forum. 2022. "The Global Risks Report 2022." 17. Insight Report. Geneva: World Economic Forum. https://www.weforum.org/publications/global-risks-report-2022/in-full/chapter-3-digital-dependencies-and-cyber-vulnerabilities/.

World Health Organization. 2020. "Managing the COVID-19 Infodemic: Promoting Healthy Behaviors and Mitigating the Harm from Misinformation and Disinformation." World Health Organization. September 23, 2020. https://www.who.int/news/item/23-09-2020-managing-the-covid-19-infodemic-promoting-healthy-behaviors-and-mitigating-the-harm-from-misinformation-and-disinformation.

Wright, Joseph. 2010. "Aid Effectiveness and the Politics of Personalism." *Comparative Political Studies* 43 (6): 735–62. https://doi.org/10.1177/0010414009358674.

WSJ Staff. 2021. "Facebook's Documents About Instagram and Teens, Published." The Wall Street Journal. September 30, 2021. https://www.wsj.com/articles/facebook-documents-instagram-teens-11632953840.

Xu, Xu. 2020. "To Repress or to Co-opt? Authoritarian Control in the Age of Digital Surveillance." *American Journal of Political Science* 65 (2): 309–25. https://doi.org/10.1111/ajps.12514.

Xu, Xu, Genia Kostka, and Xun Cao. 2022. "Information Control and Public Support for Social Credit Systems in China," 16 Seiten. https://doi.org/10.17169/REFUBIUM-36075.

Yayboke, Erol, and Sam Brannen. 2020. "Promote and Build." CSIS Briefs. Center for Strategic & International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/201015_Yayboke_Brannen_PromoteAndBuild_Brief.pdf.

Yoo, Youngjin, Ola Henfridsson, and Kalle Lyytinen. 2010. "The New Organizing Logic of Digital Innovation: An Agenda for Information Systems Research." *Information Systems Research* 21 (4): 724–35. https://doi.org/10.1287/isre.1100.0322.

Zadrozny, Brandy. 2021. "'Carol's Journey': What Facebook Knew about How It Radicalized Users." NBC News. October 23, 2021. https://www.nbcnews.com/tech/tech-news/facebook-knew-radicalized-users-rcna3581.

Zappulla, Antonio, and Joel Simon. 2023. "Weaponizing the Law against Journalists Is Killing Our Democracies." World Economic Forum. May 10, 2023. https://www.weforum.org/agenda/2023/05/journalist-media-legal-repression/.

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

8. Appendix

1. Cases added to the GICSDF Dataset – Table A.1.

Country	Name of product / company	Category of technology
Armenia	Predator	Spyware
Botswana	Circles	Spyware
Cyprus	Pegasus	Spyware
Democratic Republic of Congo	Pegasus	Spyware
Egypt	Cerebro	Spyware
Equatorial Guinea	Circles	Spyware
Greece	Pegasus	Spyware
Greece	Predator	Spyware
Guinea-Bisseau	Cicles	Spyware
Kenya	Circles	Spyware
Nigeria	Circles	Spyware
Pakistan	Hacking Team	Spyware
Sierra Leone	Cognyte	Spyware
South Korea	Hacking Team	Spyware
Sudan	preator	Spyware
Tajikistan	Pegasus	Spyware
Turkey	Candiru	Spyware
Vietnam	Cellebrite	Spyware
Zambia	Circles	Spyware
Zimbabwe	Circles	Spyware

2. Coefficient of Variation Calculation

$$(Formula\ 1):\ CV_{v_t} = \frac{Standard\ Deviation\ of\ variable\ v\ at\ time\ t}{Mean\ of\ variable\ v\ at\ time\ t} = \frac{\sigma_{v_t}}{\mu_{v_t}} = \frac{\sqrt{\frac{\sum(v_{i_t} - \mu_{v_t})^2}{N}}}{\frac{1}{n}\sum_{i=1}^{n} v_{i_t}}$$

CV_{v_t} values between 0 and 1 are considered very small to moderate, rendering arithmetic mean calculations as appropriate mean models. Values above 1 are considered high. If sufficient shares of CV_{v_t} (i.e., more than 90%) fall in this interval of [0:1], variation is considered small enough.

3. Coefficients of Variations of Independent Variables – within years across all countries

Table A.2.

	Standard Deviation of Values within each year, across all countries (for variables ranging from negative to positive values, variation respectively)												
Year	GDP per capita (current US$)	GDP, PPP (const int. 2017 $)	Military exp. (% of GDP)	Internet Users (% population)	Patent applications (residents)	Digital Repression Capacity	State Capacity Index	Neopatrimonial Rule Index	Electoral Democracy Index	Presidentialism Index	Government online content regulation approach	Government capacity to regulate online content	Internet legal regulation content
2010	24539.08	1.15E+13	1.1762	27.16126	49329.5058	0.912952598	1.630649546	0.304323	0.261838	0.311012	1.178312396	1.226884098	1.563183095
2011	26901.46	1.20E+13	1.161149	27.4329	55804.0684	0.908776548	1.650012378	0.302234	0.258572	0.308563	1.160960171	1.226066142	1.530499107
2012	26145.48	1.25E+13	1.304901	27.97749	66489.3032	0.906973166	1.641814572	0.302601	0.257244	0.30805	1.151303171	1.23148001	1.527236788
2013	27937.92	1.29E+13	1.295686	28.47054	77411.5624	0.908224691	1.669957157	0.303012	0.256928	0.308219	1.157351669	1.230375732	1.549858119
2014	28490.53	1.34E+13	1.284462	28.29855	85548.1054	0.903654176	1.678426182	0.303086	0.256649	0.308657	1.154328364	1.230117503	1.554638554
2015	25695.53	1.39E+13	1.416215	28.07803	99011.1375	0.894350769	1.687386849	0.30382	0.257501	0.309766	1.143182422	1.212266817	1.56308099
2016	25992.47	1.44E+13	1.38165	27.71468	116904.609	0.903675107	1.693820367	0.305474	0.257213	0.309032	1.132042216	1.217787961	1.557482246
CV	0.047383	0.0741261	0.068257	0.015556	0.28256527	0.006004104	0.013390044	0.00341	0.006465	0.003105	0.01161418	0.005484018	0.008857907
Note					X								

Patent applications by residents seems to have a comparably high CV of variations from year to year across all countries.

Table A.3.

Standard Deviation of Values within each year, across all countries (for variables ranging from negative to positive values, variation respectively)													
Year	Rule of Law (V-Dem)	Rule of Law (WGI)	Civil Liberties Index	Government effectiveness Index	Civil Society Organizations Repression	Clientelism Index	Government Cyber Security Capacity	Government Internet Filtering Capacity	Government Internet Shut-Down Capacity	Person of the Leader	Government censorship effort media	Journalist Harassment	State control over territory
2010	0.310406	0.998061	0.244161047	1.005427	1.481747	0.261283	1.303533726	1.229839426	1.286599	1.500278	1.542447127	1.371015171	9.253397571
2011	0.30977	0.996957	0.243210367	1.000094	1.464134	0.258776	1.305709931	1.222845679	1.278492	1.480206	1.522845005	1.333429598	9.544034162
2012	0.310025	0.996405	0.240379774	1.001731	1.465372	0.258091	1.301197645	1.208769912	1.272906	1.496435	1.503319611	1.336642416	9.660298264
2013	0.309868	0.994445	0.244474802	1.002178	1.452027	0.257132	1.299683945	1.212286077	1.266716	1.492717	1.517819384	1.30348338	10.42186389
2014	0.309382	1.013468	0.247301176	1.014043	1.465079	0.255168	1.299147975	1.216765457	1.266413	1.484305	1.543914084	1.308699744	10.81153
2015	0.310268	1.012471	0.252299645	1.01196	1.470124	0.255436	1.2881388	1.217399027	1.281219	1.507991	1.56394222	1.312371367	11.14937
2016	0.311466	1.023538	0.256432388	1.008193	1.496628	0.25831	1.293622001	1.228862019	1.295592	1.528185	1.535819344	1.335622906	10.94507
CV	0.001979	0.010431	0.021084647	0.004936	0.009073	0.00753	0.004289426	0.006079587	0.007716	0.009924	0.012049616	0.016157313	0.068715106
Note													

Table A.4.

	Standard Deviation of Values within each year, across all countries (for variables ranging from negative to positive values, variation respectively)			
Year	Fiscal State Capacity	Remuneration of Administration	Meritocracy of Administration	State ownership of economy
2010	1.19211291	0.71347768	1.45606539	1.09985228
2011	1.2108472	0.71090186	1.4725222	1.08310458
2012	1.2221246	0.70010157	1.4722959	1.08142959
2013	1.22579735	0.69522146	1.45567338	1.06849824
2014	1.22801083	0.69497708	1.46089304	1.06815603
2015	1.23359475	0.69515164	1.46851184	1.09614965
2016	1.22848686	0.70719427	1.46964781	1.08466083
CV	0.01082193	0.01052255	0.00466779	0.01042615
Note				

4. Coefficient of variation across all years observations per country, then sorted into intervals by size

Table A.5.

Intervals of CV values	GDP per capita (current US$)	GDP, PPP (const int. 2017 $)	Military exp. (% of GDP)	Internet Users (% population)	Patent applications (residents)	Digital Repression Capacity	State Capacity Index	Neopatrimonial Rule Index	Electoral Democracy Index	Presidentialism Index	Government online content regulation approach	Government capacity to regulate online content	Internet legal regulation content
0:0,1	0.60335196	0.69273743	0.51955307	0.24581006	0.24581006	0.592179	0.486034	0.832402	0.832402	0.709497	0.77095	0.687151	0.815642
0:0,2	0.91061453	0.91061453	0.67039106	0.51955307	0.51955307	0.743017	0.653631	0.949721	0.932961	0.882682	0.893855	0.826816	0.899441
0:0,3	0.96089385	0.91061453	0.72625698	0.67597765	0.67597765	0.821229	0.776536	0.988827	0.960894	0.949721	0.944134	0.871508	0.932961
0:0,4	0.96089385	0.91061453	0.73184358	0.77653631	0.77653631	0.893855	0.843575	0.994413	0.98324	0.98324	0.96648	0.905028	0.955307
0:0,5	0.96089385	0.91061453	0.74301676	0.84357542	0.84357542	0.921788	0.916201	0.994413	0.994413	0.98324	0.977654	0.96648	0.98324
0:0,6	0.96089385	0.91061453	0.74301676	0.89944134	0.89944134	0.960894	0.932961	0.994413	1	0.988827	0.988827	0.98324	0.98324
0:0,7	0.96089385	0.91061453	0.74301676	0.91620112	0.91620112	0.96648	0.944134	0.994413	1	0.994413	1	0.994413	0.98324
0:0,8	0.96089385	0.91061453	0.74301676	0.93296089	0.93296089	0.977654	0.960894	0.994413	1	0.994413	1	0.994413	0.98324
0:0,9	0.96089385	0.91061453	0.74860335	0.94413408	0.94413408	0.977654	0.972067	0.994413	1	0.994413	1	0.994413	0.98324
0:1,0	0.96089385	0.91061453	0.74860335	0.94413408	0.94413408	0.988827	0.98324	1	1	0.994413	1	1	0.98324

Table A.5.

Intervals of CV values	Rule of Law (V-Dem)	Rule of Law (WGI)	Civil Liberties Index	Government effectiveness Index	Civil Society Organizations Repression	Clientelism Index	Government Cyber Security Capacity	Government Internet Filtering Capacity	Government Internet Shut-Down Capacity	Person of the Leader	Government censorship effort media	Journalist Harassment	State control over territory
0:0,1	0.782123	0.407821	0.888268	0.391061	0.413408	0.804469	0.675978	0.597765	0.75419	0.653631	0.418994	0.418994	0.93854749
0:0,2	0.899441	0.670391	0.932961	0.620112	0.631285	0.927374	0.832402	0.75419	0.860335	0.765363	0.648045	0.614525	0.95530726
0:0,3	0.949721	0.759777	0.96648	0.703911	0.77095	0.960894	0.893855	0.854749	0.921788	0.804469	0.759777	0.731844	0.96648045
0:0,4	0.977654	0.826816	0.988827	0.787709	0.854749	0.988827	0.916201	0.927374	0.944134	0.877095	0.832402	0.810056	0.96648045
0:0,5	1	0.893855	1	0.832402	0.932961	1	0.949721	0.960894	0.949721	0.899441	0.882682	0.837989	0.97206704
0:0,6	1	0.910615	1	0.888268	0.949721	1	0.949721	0.972067	0.960894	0.944134	0.932961	0.893855	0.97206704
0:0,7	1	0.944134	1	0.938547	0.972067	1	0.96648	0.988827	0.96648	0.955307	0.972067	0.921788	0.97206704
0:0,8	1	0.96648	1	0.960894	0.98324	1	0.972067	0.994413	0.977654	0.96648	0.972067	0.955307	0.97206704
0:0,9	1	0.972067	1	0.972067	0.98324	1	0.98324	0.994413	0.98324	0.96648	0.98324	0.96648	0.97206704
0:1,0	1	0.977654	1	0.977654	0.994413	1	0.98324	1	0.98324	0.972067	0.988827	0.977654	0.97206704

Table A.6.

Intervals of CV values	Fiscal State Capacity	Remuneration of Administration	Meritocracy of Administration	State ownership of economy
0:0,1	0.81564246	0.93296089	0.63687151	0.56424581
0:0,2	0.89944134	0.94972067	0.87709497	0.80446927
0:0,3	0.92178771	0.96089385	0.94413408	0.88826816
0:0,4	0.94972067	0.97206704	0.95530726	0.91620112
0:0,5	0.96648045	0.98324022	0.97206704	0.93296089
0:0,6	0.98882682	0.98324022	0.98882682	0.94413408
0:0,7	0.98882682	0.98882682	1	0.94413408
0:0,8	0.99441341	0.98882682	1	0.97765363
0:0,9	0.99441341	0.98882682	1	0.98324022
0:1,0	0.99441341	0.98882682	1	0.98882682

5. Coefficient of variation across all averages observations per country, then sorted into intervals by size

Table A.7.

Intervals of CV values	GDP per capita (current US$)	GDP, PPP (const int. 2017 $)	Military exp. (% of GDP)	Internet Users (% population)	Patent applications (residents)	Digital Repression Capacity	State Capacity Index	Neopatrimonial Rule Index	Electoral Democracy Index	Presidentialism Index	Government online content regulation approach	Government capacity to regulate online content	Internet legal regulation content
0:0,1	0.92178771	0.91620112	0.7150838	0.62569832	0.486034	0.743017	0.731844	0.96648	0.938547	0.921788	0.910615	0.837989	0.905028
0:0,2	0.96089385	0.91620112	0.73184358	0.86592179	0.664804	0.899441	0.860335	0.994413	0.988827	0.977654	0.932961	0.893855	0.960894
0:0,3	0.96089385	0.91620112	0.73743017	0.93854749	0.698324	0.949721	0.938547	0.994413	0.994413	0.994413	0.98324	0.938547	0.96648
0:0,4	0.96089385	0.91620112	0.73743017	0.95530726	0.726257	0.96648	0.960894	1	1	0.994413	0.98324	0.960894	0.96648
0:0,5	0.96089385	0.91620112	0.73743017	0.95530726	0.73743	0.96648	0.972067	1	1	0.994413	0.988827	0.972067	0.972067
0:0,6	0.96089385	0.91620112	0.74301676	0.95530726	0.743017	0.972067	0.972067	1	1	1	0.994413	0.977654	0.98324
0:0,7	0.96089385	0.91620112	0.74301676	0.95530726	0.75419	0.98324	0.972067	1	1	1	1	0.98324	0.988827
0:0,8	0.96089385	0.91620112	0.74301676	0.95530726	0.75419	0.988827	0.972067	1	1	1	1	0.994413	0.988827
0:0,9	0.96089385	0.91620112	0.74860335	0.95530726	0.75419	0.994413	0.994413	1	1	1	1	1	0.994413
0:1,0	0.96089385	0.91620112	0.74860335	0.95530726	0.75419	0.994413	1	1	1	1	1	1	0.994413

Table A.8.

Intervals of CV values	Rule of Law (V-Dem)	Rule of Law (WGI)	Civil Liberties Index	Government effectiveness Index	Civil Society Organizations Repression	Clientelism Index	Government Cyber Security Capacity	Government Internet Filtering Capacity	Government Internet Shut-Down Capacity	Person of the Leader	Government censorship effort media	Journalist Harassment	State control over territory
0:0,1	0.932961	0.709497	0.960894	0.642458	0.687151	0.949721	0.854749	0.826816	0.899441	0.782123	0.692737	0.653631	0.96089385
0:0,2	0.977654	0.849162	0.98324	0.782123	0.871508	0.994413	0.910615	0.916201	0.938547	0.865922	0.865922	0.804469	0.97206704
0:0,3	1	0.888268	0.994413	0.843575	0.921788	1	0.938547	0.972067	0.938547	0.905028	0.916201	0.860335	0.97206704
0:0,4	1	0.932961	1	0.899441	0.927374	1	0.960894	0.98324	0.949721	0.949721	0.938547	0.882682	0.97206704
0:0,5	1	0.949721	1	0.921788	0.932961	1	0.972067	0.98324	0.96648	0.960894	0.988827	0.905028	0.97206704
0:0,6	1	0.96648	1	0.938547	0.949721	1	0.977654	0.988827	0.972067	0.972067	0.994413	0.938547	0.97206704
0:0,7	1	0.98324	1	0.96648	0.96648	1	0.98324	0.994413	0.98324	0.972067	0.994413	0.96648	0.97206704
0:0,8	1	0.98324	1	0.972067	0.972067	1	0.988827	0.994413	0.98324	0.98324	0.994413	0.977654	0.97206704
0:0,9	1	0.98324	1	0.972067	0.98324	1	0.988827	0.994413	0.988827	0.988827	0.994413	0.98324	0.97206704
0:1,0	1	0.98324	1	0.98324	0.98324	1	0.988827	1	0.988827	1	0.994413	0.98324	0.97206704

Table A.9.

Intervals of CV values	Fiscal State Capacity	Remuneration of Administration	Meritocracy of Administration	State ownership of economy
0:0,1	0.9273743	0.96648045	0.90502793	0.90502793
0:0,2	0.96089385	0.97765363	0.97765363	0.97765363
0:0,3	0.97765363	0.98324022	0.98882682	0.98882682
0:0,4	0.98882682	0.98324022	0.98882682	0.98882682
0:0,5	0.98882682	0.99441341	0.98882682	0.98882682
0:0,6	0.98882682	0.99441341	0.98882682	0.98882682
0:0,7	1	0.99441341	0.99441341	0.99441341
0:0,8	1	0.99441341	0.99441341	0.99441341
0:0,9	1	0.99441341	0.99441341	0.99441341
0:1,0	1	0.99441341	1	1

6. Concepts and Operationalizations: Overview over all Variables

Table A.10.

Meta-Concept	#	Variable	Variable Source Name	Interpretation	Source	inverted
Country	01	*country*	country_name	Name of the purchasing country	V-Dem	-
	02	*country_text_id*	country_text_id	Three letter ID of the purchasing country	V-Dem	-
Mercenary Surveillance Software Acquisition (MASSA)	03	*digitool*	-	Number of acquisitions (sum of spy, foren, and other)	Feldstein & Kot	-
	04	*spy*	Category of technology	Number of spywares acquired	Feldstein & Kot	-
	05	*foren*	Category of technology	Number of digital forensics acquired	Feldstein & Kot	-
	06	*dummy_didi*	-	Dummy of surveillance software acquisition ("1" purchase; "0" no purchase")	-	-
	07	*dummy_spy*	-	Dummy of spy ("1" purchase; "0" no purchase")	-	-
	08	*dummy_for*	-	Dummy of foren ("1" purchase; "0" no purchase")	-	-
	09	*other*	Category of technology	Number of other acquired neglectable as n=1	Feldstein & Kot	-
	10	*dummy_other*	-	Dummy of other ("1" purchase; "0" no purchase") neglectable as n=1	-	-
State Capacity	11	*admincrit*	v2stcritrecadm	Relevance of meritocratic criteria for career in state administration career Interval ~[-5,0 : 5,0], from low to high	V-Dem	-
	12	*adminren*	v2strenadm	The extent of which state officials are salaried employees Interval ~[-5,0 : 5,0], from low to high	V-Dem	-
	13	*fiscap*	v2stfisccap	The state's capacity to fund itself through tax collection Interval ~[-5,0 : 5,0], from low to high	V-Dem	-
	14	*stateco*	v2clstown	The state's ownership of the economy Interval ~[-5,0 : 5,0], from low to high	V-Dem	yes
	15	*terrcont*	v2svstterr	The state's control over its territory Interval [0:100], from low to high	V-Dem	-
	16	*goveff*	e_wbgi_gee	Government effectiveness, quality of civil services Interval ~[-2,5 : 2,5], from low to high	WB WGI/V-Dem	-
	17	*statecap*	statecap_base_fiscal	Measuring state capacity as index Interval ~[-5,0 : 5,0], from low to high	O'Reilly & Murphy	-
Financial Recourses	18	*gdpcon*	GDP, PPP (constant 2017 international $)	GDP purchasing power parity in international 2016 $	WB	-
	19	*gdppc*	GDP per capita (current US$)	GDP per capita in current US$	WB	-
	20	*milex*	Military expenditure (% of GDP)	Share of military spending Interval [0:100], from low to high	WB	-
	21	*democr*	v2x_polyarchy	Measuring electoral democracy as index	V-Dem	-

				Interval ~[-5,0 : 5,0], from low to high		
	22	*civlib*	v2x_civlib	Measuring civil liberties as index Interval ~[-5,0 : 5,0], from low to high	V-Dem	yes
	23	*csreprss*	v2csreprss	Repression against civil society organizations Interval ~[-5,0 : 5,0], from low to high	V-Dem	yes
	24	*medcens*	v2mecenefm	Efforts by government to censor media Interval ~[-5,0 : 5,0], from low to high	V-Dem	yes
	25	*journhrs*	v2meharjrn	Harassment of journalists Interval ~[-5,0 : 5,0], from low to high	V-Dem	yes
Regime Traits	26	*rulev*	v2x_rule	Measuring the rule of law as index Interval [0: 1], from low to high	V-Dem	-
	27	*rulewgi*	e_wbgi_rle	Measuring the rule of law as index Interval ~[-2,5 : 2,5], from low to high	WB WGI/V-Dem	--
	28	*client*	v2xnp_client	Measuring the degree of clientelism as index Interval [0: 1], from low to high	V-Dem	--
	29	*pres*	v2xnp_pres	Measuring the degree of presidentialism as index Interval [0: 1], from low to high	V-Dem	-
	30	*person*	v2exl_legitlead	Measuring the importance of the person of the leader Interval ~[-5,0 : 5,0], from low to high	V-Dem	-
	31	*neopat*	v2x_neopat	Measuring the degree of neopatrimonialism as index Interval [0: 1], from low to high	V-Dem	-
	32	*digrepcap*	Digital Repression Capacity Index	Measuring the capacity for digital repression as index Interval ~[-5,0 : 5,0], from low to high	Feldstein	-
Technological capacities	33	*patres*	Patent applications, residents	Number of patent applications submitted by residents	WB	-
	34	*eduqual*	v2peedueq	Approximating the access to high quality education Interval ~[-5,0 : 5,0], from low to high	V-Dem	-
Infrastructural control	35	*legalcap*	v2smregcon	Approximating the legal capabilities of the state to regulate online content Interval ~[-5,0 : 5,0], from low to high	V-Dem	yes
	36	*regapp*	v2smregapp	Approximating the regulatory approach from low control (outsourced to private sector) to high (statist) Interval ~[-5,0 : 5,0], from low to high	V-Dem	yes
Infrastructure	37	*inet*	Individuals using the Internet (% of population)	Interval [0:100], from low to high	WB	-

7. Conceptual & Methodological issues of selected Indices and variables

Upon closer investigation of the variables for neopatrimonialism, clientelism, presidentialism (V-Dem, v2x_neopat, v2xnp_client, v2xnp_pres, respectively), state capacity (O'Reilly & Murphy 2022, statecap_base_fisc, which is also a V-Dem based indicator), as well as the Worldwide Governance Indicators on government effectiveness and rule of law (WGI, taken from V-Dem, e_wbgi_gee, e_wbgi_rle), several conceptual issues become apparent. All Indicators include components such as rule of law, components of democracy measures also included in the electoral democracy index by V-Dem (v2x_polyarchy), and seem to measure either administrative capacity, democracy and rule of law (as for presidentialism, clientelism, neopatrimonialism), democratic elements and rule of law (as for state capacity), or seem to carry heavy democracy biases (as for government effectiveness, and rule of law as measured by the Worldwide Governance Indicators) (see respectively in detail Coppedge, Gerring, Knutsen, Lindberg, Teorell, Altman, et al. 2023; O'Reilly and Murphy 2022a; Kaufmann and Kraay 2024).These issues, and their potentially distorting effects in the analysis also become apparent when consulting the pairwise correlation (see following section). As for the number of patent applications by residents, this variable has been dropped, as its missing values would remove more than 40 country observations from the analysis. With 179 country-cases, this would mean losing to much information, for only marginal added information, as patent applications by residents are not remotely as good as a proxy to measure digital technological capacities than the digital repression capacity index by Felstein; also, there is a strong positive correlation between national income and patent applications. Therefore, these variables are dropped. Preliminary analyzes have nonetheless been conducted, as can be seen in the .log files upon request.

8. Descriptive Analysis

8.1. Table A.11. Descriptive Summary Statistics Dependent Variables

Variable	Obs	Mean	Std. Dev.	Min	Max
digitool	179	1.179	1.992	0	14
dummy_digi (n of "1" = 80)	179	.447	.499	0	1
spy	179	.827	1.235	0	6
dummy_spy (n of "1" = 75)	179	.419	.495	0	1
foren	179	.346	1.439	0	14
dummy_for (n of "1" = 28)	179	.156	.364	0	1
"other" (n=1, Israel with IOT Hacking)	179	.006	.075	0	1

8.2. Table A.12.Outliers in Dependent Variables

country_name	digitool	spy	foren
United Arab Emirates	6	5	1
Burma/Myanmar	14	0	14
Saudi Arabia	7	6	1
United States of America	13	2	11

8.3. Table A.13. Descriptive Summary Statistics of Independent Variables

Variable	Obs	Mean	Std. Dev.	Min	Max
civlib 1015	179	.701	.244	.016	.976
client 1015	179	.472	.256	.021	.921
csreprss 1015	179	-1.005	1.444	-3.324	3.759
democr 1015	179	.527	.256	.018	.922
digrepcap 1015	179	0	.904	-2.342	2.569
gdpcon 1015	163	3.963e+12	1.275e+13	38112441	1.056e+14
gdpcon 1015 bio	163	3963.149	12750.892	.038	105614
gdppc 1015	171	17185.973	26566.023	418.862	176302.34
gdppc 1015 10k	171	1.719	2.657	.042	17.63
goveff 1015	175	-.088	1.003	-2.225	2.171
journhrs 1015	179	-.706	1.312	-3.891	2.96
inet 1015	169	39.703	27.731	0	96.221
legalcap 1015	179	-.378	1.544	-2.421	3.572
medcens 1015	179	-.72	1.506	-3.499	2.879
milex 1015	134	1.837	1.234	.154	8.477
neopat 1015	179	.471	.302	.006	.977
patres 1015	131	11641.598	64618.155	1	619755.17
person 1015	179	-.101	1.474	-3.011	3.587
pres 1015	179	.395	.307	.009	.992
regapp 1015	179	-.356	1.155	-3.556	2.874
rulev 1015	179	.543	.309	.029	.999
rulewgi 1015	175	-.073	1	-2.411	1.994
statecap 1015	175	.571	1.637	-4.023	3.824
stateco 1015	179	-.641	1.076	-2.901	3.474
terrcont 1015	174	91.836	9.901	42.611	100
eduqual 1015	179	.673	1.465	-2.36	3.529
fiscap 1015	179	.953	1.215	-1.988	3.178
admincrit 1015	179	.435	1.081	-2.143	3.474
adminren 1015	179	.994	.702	-1.38	2.177

8.4. Table A.14.Correlation of Independent Variables Summary

High correlations (pwcorr; r >0.69)											
Variable	Correlates										
(1) civlib_1015	csrepress	democr	journhrs	legalcap	medcens	neopat	pres	rulev	stateco		
(2) client_1015	goveff	neopat	rulev	rulewgi	statecap						
(3) csreprss_1015	civlib	democr	journhrs	legalcap	medcens	pres	rulev	stateco	democr		
(4) democr_1015	civlib	csreprrs	journhrs	legalcap	medcens	neopat	person	pres	rulev	statecap	
(5) digrepcap_1015	-										
(6) gdpcon_1015	-										
(7) gdppc_1015	inet										
(8) goveff_1015	client	neopat	rulev	rulewgi	statecap	eduqual	fiscap	admincrit			
(9) journhrs_1015	civlib	csreprrs	democr	medcens	neopat	pres	rulev				
(10) inet_1015	gdppc										
(11) legalcap_1015	civlib	csreprrs	democr	medcens	neopat	stateco					
(12) medcens_1015	civlib	csreprrs	democr	journhrss	legalcap	neopat	person	pres	rulev	stateco	
(13) milex_1015	-										
(14) neopat_1015	civliba	client	democr	goveff	journhrss	legalcap	medcens	pres	rulev	rulewgi	statecap
(15) patres_1015											
(16) person_1015	democr	medcens									
(17) pres_1015	civliba	csreprrs	democr	journhrss	medcens	neopat	rulev	rulewgi	statecap	admincrit	
(18) regapp_1015	-										
(19) rulev_1015	civliba	client	csreprrs	democr	journhrss	medcens	neopat	pres	rulewgi	statecap	admincri
(20) rulewgi_1015	client	goveff	neopat	pres	rulev	statecap	fiscap	admincrit			
(21) statecap_1015	client	democr	goveff	neopat	pres	rulvev	rulewgi	fiscap	admincrit		
(22) stateco_1015	civliba	csreprrs	legalcap	medcens							
(23) terrcont_1015											
(24) eduqual_1015	goveff										
(25) fiscap_1015	goveff	rulewgi	statecap								
(26) admincrit_1015	goveff	pres	rulev	rulewgi	statecap						
(27) adminren_1015	-										

8.5. Pairwise Correlation Table of Independent Variables

Table A.15.

Variables	(1) civlib_1015	(2) client_1015	(3) csreprss_1015	(4) democr_1015	(5) digrepcap_1015	(6) gdpcon_1015	(7) gdppc_1015	(8) goveff_1015	(9) journhrs_1015	(10) inet_1015	(11) legalcap_1015	(12) medcens_1015	(13) milex_1015	(14) neopat_1015	(15) patres_1015	(16) person_1015	(17) pres_1015	(18) regapp_1015	(19) rulev_1015	(20) rulewgi_1015	(21) statecap_1015	(22) stateco_1015	(23) terrcont_1015	(24) eduqual_1015	(25) fiscap_1015	(26) admincrit_1015	(27) adminren_1015
(1) civlib_1015	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
(2) client_1015	0.494	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
(3) csreprss_1015	0.899	0.513	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
(4) democr_1015	0.921	0.644	0.908	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
(5) digrepcap_1015	0.296	0.149	0.295	0.234	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
(6) gdpcon_1015	0.069	0.052	0.092	0.119	0.041	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
(7) gdppc_1015	0.047	0.071	0.028	0.048	0.108	0.077	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
(8) goveff_1015	0.588	0.768	0.589	0.671	0.211	0.067	0.273	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
(9) journhrs_1015	0.871	0.633	0.852	0.913	0.151	0.161	0.061	0.673	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
(10) inet_1015	0.048	0.059	0.026	0.086	0.006	0.079	0.801	0.185	0.039	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
(11) legalcap_1015	0.894	0.488	0.848	0.885	0.381	0.006	0.054	0.486	0.823	0.015	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
(12) medcens_1015	0.889	0.565	0.918	0.923	0.230	0.068	0.081	0.653	0.877	0.066	0.847	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
(13) milex_1015	0.020	0.051	0.033	0.013	0.025	0.113	0.047	0.035	0.038	0.158	0.009	0.027	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
(14) neopat_1015	0.803	0.733	0.839	0.888	0.064	0.078	0.086	0.788	0.836	0.046	0.759	0.869	0.017	1	0	0	0	0	0	0	0	0	0	0	0	0	0
(15) patres_1015	0.134	0.176	0.076	0.158	0.153	0.053	0.036	0.227	0.116	0.132	0.134	0.096	0.025	0.157	1	0	0	0	0	0	0	0	0	0	0	0	0
(16) person_1015	0.625	0.487	0.689	0.713	0.227	0.064	0.107	0.486	0.648	0.197	0.668	0.708	0.037	0.698	0.157	1	0	0	0	0	0	0	0	0	0	0	0
(17) pres_1015	0.831	0.563	0.863	0.879	0.185	0.058	0.038	0.658	0.809	0.009	0.818	0.868	0.063	0.963	0.120	0.718	1	0	0	0	0	0	0	0	0	0	0
(18) regapp_1015	0.723	0.282	0.648	0.693	0.354	0.083	0.094	0.436	0.648	0.134	0.745	0.676	0.062	0.113	0.541	0.548	0.613	1	0	0	0	0	0	0	0	0	0
(19) rulev_1015	0.787	0.734	0.801	0.843	0.004	0.093	0.123	0.832	0.799	0.044	0.706	0.821	0.013	0.972	0.173	0.617	0.900	0.554	1	0	0	0	0	0	0	0	0
(20) rulewgi_1015	0.664	0.655	0.689	0.719	0.105	0.055	0.258	0.900	0.705	0.196	0.605	0.720	0.004	0.765	0.176	0.569	0.685	0.557	0.805	1	0	0	0	0	0	0	0
(21) statecap_1015	0.711	0.742	0.725	0.815	0.118	0.058	0.142	0.805	0.775	0.052	0.668	0.775	0.025	0.885	0.168	0.564	0.804	0.484	0.905	0.758	1	0	0	0	0	0	0
(22) stateco_1015	0.765	0.201	0.748	0.713	0.378	0.067	0.035	0.341	0.634	0.097	0.781	0.735	0.134	0.585	0.236	0.618	0.667	0.736	0.528	0.548	0.479	1	0	0	0	0	0
(23) terrcont_1015	0.374	0.475	0.257	0.297	0.041	0.028	0.136	0.488	0.278	0.064	0.259	0.031	0.036	0.369	0.076	0.118	0.113	0.307	0.145	0.086	0.429	0.399	1	0	0	0	0
(24) eduqual_1015	0.394	0.698	0.348	0.438	0.267	0.063	0.136	0.761	0.479	0.029	0.398	0.088	0.559	0.258	0.409	0.192	0.648	0.598	0.688	0.078	0.558	0.488	0.111	1	0	0	0
(25) fiscap_1015	0.693	0.628	0.723	0.783	0.004	0.063	0.048	0.677	0.668	0.044	0.706	0.743	0.034	0.743	0.216	0.659	0.733	0.515	0.725	0.705	0.768	0.609	0.389	0.488	1	0	0
(26) admincrit_1015	0.670	0.654	0.662	0.738	0.128	0.077	0.073	0.736	0.715	0.061	0.676	0.768	0.040	0.817	0.229	0.538	0.765	0.561	0.815	0.669	0.795	0.449	0.359	0.539	0.679	1	0
(27) adminren_1015	0.398	0.228	0.308	0.398	0.011	0.228	0.069	0.342	0.316	0.029	0.297	0.350	0.027	0.316	0.094	0.229	0.318	0.269	0.339	0.278	0.378	0.229	0.378	0.329	0.419	0.319	1

9. Testing Distributions of Dependent Variables

9.1. Table A.16. Tests for Normality: Skewness and Kurtosis Test

Variable	Obs	Pr(Skewness)	Pr(Kurtosis)	adj_chi2(2)	Prob>chi2
digitool	179	0.000	0.000	.	0.000
spy	179	0.000	0.000	43.520	0.000
foren	179	0.000	0.000	.	0.000
digrepcap_16	179	0.893	0.251	1.350	0.508

Variable	Obs	Pr(Skewness)	Pr(Kurtosis)	adj_chi2(2)	Prob>chi2

9.2. Table A.17. Testing for Poisson Distribution with a test regression model of digitool

Poisson regression

digitool	Coef.	St.Err.	t-value	p-value	[95% Conf	Interval]	Sig
democr_1015	-.559	.726	-0.77	.442	-1.982	.864	
gdpcon_1015	0	0	0.71	.481	0	0	
digrepcap_1015	.733	.111	6.61	0	.516	.951	***
statecap_1015	-.022	.073	-0.30	.767	-.164	.121	
inet_1015	-.003	.003	-1.23	.219	-.009	.002	
legalcap_1015	-.12	.109	-1.10	.271	-.333	.093	
Constant	.368	.33	1.11	.266	-.28	1.015	

Mean dependent var	1.214	SD dependent var	2.063
Pseudo r-squared	0.121	Number of obs	159
Chi-square	72.869	Prob > chi2	0.000
Akaike crit. (AIC)	541.764	Bayesian crit. (BIC)	560.178

**** p<.01, ** p<.05, * p<.1*

Deviance goodness-of-fit = 337.5897
Prob > chi2(153) = 0.0000
Pearson goodness-of-fit = 427.0443
Prob > chi2(153) = 0.0000

Deviance goodness-of-fit = 337.5897
Prob > chi2(153) = 0.0000
Pearson goodness-of-fit = 427.0443
Prob > chi2(153) = 0.0000

Poisson model for digitool not a good fit.

9.3. Table A.18. Testing for Poisson Distribution with a test regression model of spy

Poisson regression

spy	Coef.	St.Err.	t-value	p-value	[95% Conf	Interval]	Sig
democr_1015	-.504	.862	-0.59	.559	-2.192	1.185	
gdpcon_1015	0	0	1.35	.178	0	0	
digrepcap_1015	.594	.131	4.52	0	.336	.851	***
statecap_1015	.009	.088	0.10	.919	-.163	.181	
inet_1015	-.005	.003	-1.53	.126	-.012	.001	
legalcap_1015	-.077	.13	-0.59	.555	-.331	.178	
Constant	.071	.392	0.18	.857	-.697	.839	

Mean dependent var	0.836	SD dependent var	1.247
Pseudo r-squared	0.089	Number of obs	159
Chi-square	38.759	Prob > chi2	0.000
Akaike crit. (AIC)	410.593	Bayesian crit. (BIC)	429.006

*** p<.01, ** p<.05, * p<.1

Deviance goodness-of-fit = 231.4702
Prob > chi2(153) = 0.0000
Pearson goodness-of-fit = 239.837
Prob > chi2(153) = 0.0000

Deviance goodness-of-fit = 231.4702
Prob > chi2(153) = 0.0000
Pearson goodness-of-fit = 239.837
Prob > chi2(153) = 0.0000

Poisson model for spy not a good fit.

9.4. Table A.19. Testing for Poisson Distribution with a test regression model of foren

Poisson regression

foren	Coef.	St.Err.	t-value	p-value	[95% Conf	Interval]	Sig
democr_1015	-.786	1.357	-0.58	.562	-3.447	1.874	
gdpcon_1015	0	0	-0.70	.486	0	0	
digrepcap_1015	1.028	.209	4.92	0	.619	1.438	***
statecap_1015	-.086	.131	-0.66	.511	-.342	.17	
inet_1015	0	.005	0.06	.953	-.009	.01	
legalcap_1015	-.222	.201	-1.10	.27	-.616	.172	
Constant	-.956	.617	-1.55	.121	-2.164	.253	

Mean dependent var	0.371	SD dependent var	1.516
Pseudo r-squared	0.118	Number of obs	159
Chi-square	39.949	Prob > chi2	0.000
Akaike crit. (AIC)	311.123	Bayesian crit. (BIC)	329.537

*** p<.01, ** p<.05, * p<.1

Deviance goodness-of-fit = 237.4562
Prob > chi2(153) = 0.0000
Pearson goodness-of-fit = 678.426
Prob > chi2(153) = 0.0000

Deviance goodness-of-fit = 237.4562
Prob > chi2(153) = 0.0000
Pearson goodness-of-fit = 678.426
Prob > chi2(153) = 0.0000

Poisson model for foren not a good fit.

9.5. Table A.20. Testing a Negative Binomial Regression Model for digitool, spy, and

digitool	Coef.	St.Err.	t-value	p-value	[95% Conf	Interval]	Sig
democr_1015	-.044	1.319	-0.03	.973	-2.629	2.541	
gdpcon_1015	0	0	0.26	.793	0	0	
digrepcap_1015	.973	.208	4.68	0	.566	1.38	***
statecap_1015	-.123	.141	-0.87	.383	-.401	.154	
inet_1015	-.003	.005	-0.66	.511	-.013	.007	
legalcap_1015	-.137	.189	-0.73	.468	-.507	.233	
Constant	.091	.609	0.15	.882	-1.103	1.284	
lnalpha	.275	.237	.b	.b	-.191	.74	

Mean dependent var	1.214	SD dependent var	2.063
Pseudo r-squared	0.064	Number of obs	159
Chi-square	30.408	Prob > chi2	0.000
Akaike crit. (AIC)	458.264	Bayesian crit. (BIC)	479.746

*** p<.01, ** p<.05, * p<.1

spy	Coef.	St.Err.	t-value	p-value	[95% Conf	Interval]	Sig
democr_1015	-.401	1.196	-0.34	.737	-2.745	1.942	
gdpcon_1015	0	0	0.71	.479	0	0	
digrepcap_1015	.71	.187	3.80	0	.344	1.077	***
statecap_1015	-.027	.124	-0.22	.827	-.27	.216	
inet_1015	-.006	.005	-1.21	.227	-.014	.003	
legalcap_1015	-.104	.175	-0.60	.551	-.446	.238	
Constant	.022	.554	0.04	.969	-1.064	1.107	
lnalpha	-.217	.349	.b	.b	-.901	.468	

Mean dependent var	0.836	SD dependent var	1.247
Pseudo r-squared	0.058	Number of obs	159
Chi-square	23.419	Prob > chi2	0.000
Akaike crit. (AIC)	392.452	Bayesian crit. (BIC)	413.935

*** p<.01, ** p<.05, * p<.1

foren	Coef.	St.Err.	t-value	p-value	[95% Conf	Interval]	Sig
democr_1015	.943	3.027	0.31	.755	-4.991	6.877	
gdpcon_1015	0	0	-0.14	.887	0	0	
digrepcap_1015	1.628	.491	3.31	.001	.665	2.59	***
statecap_1015	-.366	.342	-1.07	.284	-1.036	.304	
inet_1015	.004	.011	0.34	.732	-.019	.026	
legalcap_1015	-.225	.414	-0.54	.587	-1.036	.586	
Constant	-2.093	1.358	-1.54	.123	-4.755	.569	
lnalpha	1.616	.315	.b	.b	.999	2.234	

Mean dependent var	0.371	SD dependent var	1.516
Pseudo r-squared	0.079	Number of obs	159
Chi-square	16.968	Prob > chi2	0.005
Akaike crit. (AIC)	211.965	Bayesian crit. (BIC)	233.447

*** p<.01, ** p<.05, * p<.1

Negative Binomial Model appropriate, as indicated by alpha =0 which supports the rejection of a Poisson regression model for a negative binomial one.

9.6. Table A.21. Tests for Normality of predicted Residuals for OLS Regression Model with digirepcap_16: Skewness and Kurtosis Test

Variable	Obs	Pr(Skewness)	Pr(Kurtosis)	adj_chi2(2)	Prob>chi2
residuals	132	0.608	0.950	0.270	0.875

Null hypotheses, that the distribution is not normally distributed, can be refuted. Residuals appear to follow normal distribution.

10. Model Specifications

10.1. Table A.22. Tests for Multicollinearity of OLS Regression Model with Independent Variables averaged from 2010-5

Variance inflation factor

	VIF	1/VIF
journhrs 1015	2.826	.354
fiscap 1015	2.27	.441
person 1015	2.009	.498
regapp 1015	1.849	.541
eduqual 1015	1.801	.555
terrcont 1015	1.756	.569
adminren 1015	1.47	.68
gdpcon 1015 bio	1.107	.904
gdppc 1015 10k	1.03	.971
milex 1015	1.021	.979
Mean VIF	1.714	.

Interpretation

VIF = 1 no correlation between the variables

VIF [1:5] moderate correlation

VIF > 5 severe correlation and risk of multicollinearity

Ergo, no indication of multicollinearity in this model.

Note: gdpcon_1015_bio and gdppc_1015_10k are linearly transformed variables of gdpcon_1015 and gdppc_1015 divided by one billion, and ten thousand, to represent values in billions and ten thousand of dollar respectively.

10.2. Table A.23 Multicollinearity Check for Regression Models S1-6, D1-6, and R1-6

(obs=132)

Collinearity Diagnostics

Variable	VIF	SQRT VIF	Tolerance	R-Squared
journhrs_1015	3.07	1.75	0.3262	0.6738
person_1015	2.14	1.46	0.4676	0.5324
digrepcap_1015	1.62	1.27	0.6181	0.3819
gdpcon_1015_bio	1.13	1.06	0.8856	0.1144
gdppc_1015_10k	1.05	1.02	0.9556	0.0444
milex_1015	1.07	1.03	0.9384	0.0616
regapp_1015	2.49	1.58	0.4013	0.5987
stateco_1015	3.04	1.74	0.3286	0.6714
terrcont_1015	1.79	1.34	0.5585	0.4415
eduqual_1015	2.13	1.46	0.4704	0.5296
adminren_1015	1.47	1.21	0.6789	0.3211
fiscap_1015	2.91	1.71	0.3432	0.6568
Mean VIF	1.99			

	Eigenval	Cond.Index
1	6.0530	1.0000
2	2.1175	1.6907
3	1.3396	2.1257
4	0.9185	2.5671
5	0.6292	3.1016
6	0.4907	3.5120
7	0.4369	3.7223
8	0.3026	4.4722
9	0.2287	5.1445
10	0.1921	5.6133
11	0.1652	6.0535
12	0.1226	7.0252
13	0.0033	42.9989
Condition Number	42.9989	

Eigenvalues & Cond Index computed from scaled raw sscp (w/ intercept); Det(correlation matrix) 0.0113

11. Robustness and Time-Sensitivity Checks of Regression Models

Table A.24. Dependent Variable digitool

Year	2010-5		2012-4		2014-5		2013-6		2010		2015
Variables	digitool	Variables	digitool	Variables	digitool	Variables	digitool	Variables	digitool	Variables	digitool
journhrs_1015	0.372**	journhrs_1215	0.387**	journhrs_1415	0.366**	journhrs_1316	0.353*	journhrs_10	0.323*	journhrs_15	0.391**
	(0.176)		(0.175)		(0.180)		(0.183)		(0.176)		(0.180)
person_1015	-0.160	person_1215	-0.151	person_1415	-0.147	person_1316	-0.137	person_10	-0.155	person_15	-0.138
	(0.129)		(0.128)		(0.132)		(0.133)		(0.122)		(0.134)
digrepcap_1015	1.111***	digrepcap_1215	1.101***	digrepcap_1415	1.072***	digrepcap_1316	1.110***	digrepcap_10	1.092***	digrepcap_15	1.070***
	(0.211)		(0.209)		(0.211)		(0.209)		(0.216)		(0.212)
gdpcon_1015	-0.000	gdpcon_1215	-0.000	gdpcon_1415	-0.000	gdpcon_1316	-0.000	gdpcon_10	-0.000	gdpcon_15	-0.000
	(0.000)		(0.000)		(0.000)		(0.000)		(0.000)		(0.000)
gdppc_1015	-0.000	gdppc_1215	-0.000	gdppc_1415	-0.000	gdppc_1316	-0.000	gdppc_10	-0.000	gdppc_15	-0.000
	(0.000)		(0.000)		(0.000)		(0.000)		(0.000)		(0.000)
milex_1015	0.071	milex_1215	0.042	milex_1415	0.020	milex_1316	0.033	milex_10	0.116	milex_15	0.009
	(0.110)		(0.107)		(0.106)		(0.107)		(0.110)		(0.102)
regapp_1015	-0.136	regapp_1215	-0.154	regapp_1415	-0.143	regapp_1316	-0.148	regapp_10	-0.066	regapp_15	-0.161
	(0.152)		(0.153)		(0.156)		(0.157)		(0.153)		(0.159)
terrcont_1015	0.006	terrcont_1215	0.005	terrcont_1415	0.008	terrcont_1316	0.006	terrcont_10	0.002	terrcont_15	0.006
	(0.020)		(0.020)		(0.019)		(0.019)		(0.022)		(0.018)
eduqual_1015	-0.379***	eduqual_1215	-0.356***	eduqual_1415	-0.346***	eduqual_1316	-0.365***	eduqual_10	-0.428***	eduqual_15	-0.331**
	(0.134)		(0.133)		(0.132)		(0.134)		(0.141)		(0.132)
adminren_1015	-0.081	adminren_1215	-0.097	adminren_1415	-0.117	adminren_1316	-0.079	adminren_10	0.021	adminren_15	-0.163
	(0.236)		(0.235)		(0.239)		(0.238)		(0.242)		(0.243)
fiscap_1015	0.429**	fiscap_1215	0.419**	fiscap_1415	0.403**	fiscap_1316	0.408**	fiscap_10	0.348*	fiscap_15	0.419**
	(0.193)		(0.188)		(0.185)		(0.187)		(0.200)		(0.187)
Constant	-0.685	Constant	-0.572	Constant	-0.813	Constant	-0.649	Constant	-0.281	Constant	-0.576
	(1.765)		(1.716)		(1.627)		(1.644)		(1.930)		(1.581)
Observations	132	Observations	130	Observations	129	Observations	130	Observations	125	Observations	127
Pseudo R^2	0.129	Pseudo R^2	0.129	Pseudo R^2	0.122	Pseudo R^2	0.126	Pseudo R^2	0.125	Pseudo R^2	0.123

Standard errors in parentheses; *** p<0.01, ** p<0.05, * p<0.1

Table A.25. Dependent Variable spy

Year	2010-5		2012-4		2014-5		2013-6		2010		2015
Variable	spy	Variable	spy	Variable	spy	Variable	spy	Variable	spy	Variable	spy
journhrs_1015	0.329*	journhrs_1215	0.347**	journhrs_1415	0.343*	journhrs_1316	0.346*	journhrs_10	0.259	journhrs_15	0.390**
	(0.178)		-0.176		(0.175)		(0.177)		(0.180)		(0.172)
person_1015	-0.182	person_1215	-0.181	person_1415	-0.172	person_1316	-0.182	person_10	-0.162	person_15	-0.177
	(0.139)		-0.136		(0.135)		(0.135)		(0.139)		(0.132)
digrepcap_1015	0.988***	digrepcap_1215	0.974***	digrepcap_1415	0.937***	digrepcap_1316	0.975***	digrepcap_10	0.994***	digrepcap_15	0.931***
	(0.206)		-0.203		(0.200)		(0.199)		(0.213)		(0.198)
gdpcon_1015	0.000	gdpcon_1215	0	gdpcon_1415	0.000	gdpcon_1316	0.000	gdpcon_10	0.000	gdpcon_15	0.000
	(0.000)		0		(0.000)		(0.000)		(0.000)		(0.000)
gdppc_1015	-0.000	gdppc_1215	0	gdppc_1415	-0.000	gdppc_1316	-0.000	gdppc_10	-0.000	gdppc_15	-0.000
	(0.000)		0		(0.000)		(0.000)		(0.000)		(0.000)
milex_1015	0.078	milex_1215	0.051	milex_1415	0.026	milex_1316	0.039	milex_10	0.122	milex_15	0.017
	(0.107)		-0.104		(0.102)		(0.103)		(0.110)		(0.097)
regapp_1015	-0.179	regapp_1215	-0.177	regapp_1415	-0.180	regapp_1316	-0.187	regapp_10	-0.143	regapp_15	-0.197
	(0.153)		-0.152		(0.154)		(0.155)		(0.160)		(0.154)
terrcont_1015	0.015	terrcont_1215	0.014	terrcont_1415	0.016	terrcont_1316	0.015	terrcont_10	0.011	terrcont_15	0.015
	(0.020)		-0.019		(0.018)		(0.018)		(0.023)		(0.017)
eduqual_1015	-0.283**	eduqual_1215	-0.256**	eduqual_1415	-0.237*	eduqual_1316	-0.252**	eduqual_10	-0.339**	eduqual_15	-0.225*
	(0.130)		-0.128		(0.125)		(0.127)		(0.140)		(0.124)
adminren_1015	-0.024	adminren_1215	-0.023	adminren_1415	-0.027	adminren_1316	-0.020	adminren_10	0.021	adminren_15	-0.073
	(0.231)		-0.23		(0.229)		(0.228)		(0.242)		(0.229)
fiscap_1015	0.267	fiscap_1215	0.251	fiscap_1415	0.236	fiscap_1316	0.239	fiscap_10	0.231	fiscap_15	0.251
	(0.190)		-0.183		(0.177)		(0.179)		(0.200)		(0.177)
Constant	-1.709	Constant	-1.579	Constant	-1.758	Constant	-1.715	Constant	-1.355	Constant	-1.681
	(1.770)		-1.687		(1.581)		(1.604)		(2.010)		(1.534)
Observations	132	Observations	130	Observations	129	Observations	130	Observations	125	Observations	127
Pseudo R^2	0.114	Pseudo R^2	0.114	Pseudo R^2	0.111	Pseudo R^2	0.116	Pseudo R^2	0.107	Pseudo R^2	0.117

Standard errors in parentheses; *** p<0.01, ** p<0.05, * p<0.1

Table A.26. Dependent Variable foren

Year	2010-5		2012-4		2014-5		2013-6		2010		2015
Variables	foren	Variables	foren	Variables	foren	Variables	foren	Variables	foren	Variables	foren
journhrs_1015	0.533	journhrs_1215	0.555	journhrs_1415	0.459	journhrs_1316	0.400	journhrs_10	0.561	journhrs_15	0.394
	(0.377)		(0.385)		(0.395)		(0.408)		(0.373)		(0.402)
person_1015	0.148	person_1215	0.164	person_1415	0.156	person_1316	0.231	person_10	0.204	person_15	0.216
	(0.244)		(0.243)		(0.253)		(0.266)		(0.260)		(0.270)
digrepcap_1015	1.423***	digrepcap_1215	1.465***	digrepcap_1415	1.460***	digrepcap_1316	1.561***	digrepcap_10	1.338***	digrepcap_15	1.505***
	(0.490)		(0.499)		(0.516)		(0.536)		(0.509)		(0.535)
gdpcon_1015	-0.000	gdpcon_1215	-0.000	gdpcon_1415	-0.000	gdpcon_1316	-0.000	gdpcon_10	-0.000	gdpcon_15	-0.000
	(0.000)		(0.000)		(0.000)		(0.000)		(0.000)		(0.000)
gdppc_1015	-0.000	gdppc_1215	-0.000	gdppc_1415	-0.000	gdppc_1316	-0.000	gdppc_10	-0.000	gdppc_15	-0.000
	(0.000)		(0.000)		(0.000)		(0.000)		(0.000)		(0.000)
milex_1015	0.096	milex_1215	0.060	milex_1415	0.048	milex_1316	0.060	milex_10	0.160	milex_15	0.034
	(0.243)		(0.240)		(0.235)		(0.241)		(0.259)		(0.226)
regapp_1015	-0.158	regapp_1215	-0.256	regapp_1415	-0.214	regapp_1316	-0.247	regapp_10	-0.031	regapp_15	-0.257
	(0.320)		(0.336)		(0.347)		(0.355)		(0.323)		(0.362)
terrcont_1015	-0.015	terrcont_1215	-0.015	terrcont_1415	-0.012	terrcont_1316	-0.018	terrcont_10	-0.012	terrcont_15	-0.020
	(0.039)		(0.038)		(0.037)		(0.038)		(0.045)		(0.037)
eduqual_1015	-0.775**	eduqual_1215	-0.790**	eduqual_1415	-0.814**	eduqual_1316	-0.867**	eduqual_10	-0.886**	eduqual_15	-0.798**
	(0.306)		(0.315)		(0.324)		(0.338)		(0.345)		(0.331)
adminren_1015	-0.216	adminren_1215	-0.230	adminren_1415	-0.217	adminren_1316	-0.066	adminren_10	0.100	adminren_15	-0.179
	(0.510)		(0.514)		(0.528)		(0.545)		(0.555)		(0.552)
fiscap_1015	0.964**	fiscap_1215	0.974**	fiscap_1415	0.924**	fiscap_1316	0.928**	fiscap_10	0.679	fiscap_15	0.925**
	(0.444)		(0.439)		(0.433)		(0.445)		(0.456)		(0.443)
Constant	-0.702	Constant	-0.677	Constant	-0.940	Constant	-0.654	Constant	-1.000	Constant	-0.284
	(3.369)		(3.326)		(3.226)		(3.275)		(3.854)		(3.146)
Observations	132	Observations	130	Observations	129	Observations	130	Observations	125	Observations	127
Pseudo R^2	0.181	Pseudo R^2	0.184	Pseudo R^2	0.172	Pseudo R^2	0.179	Pseudo R^2	0.188	Pseudo R^2	0.167

Standard errors in parentheses; *** p<0.01, ** p<0.05, * p<0.1

Table A.27. Dependent Variable dummy_digi

Year	2010-5		2012-4		2014-5		2013-6		2010		2015
Variables	dummy_digi	Variables	dummy_digi	Variables	dummy_digi	Variables	dummy_digi	Variables	dummy_digi	Variables	dummy_digi
journhrs_1015	0.486*	journhrs_1215	0.505*	journhrs_1415	0.490*	journhrs_1316	0.505*	journhrs_10	0.415	journhrs_15	0.524*
	(0.283)		(0.282)		(0.280)		(0.285)		(0.271)		(0.275)
person_1015	-0.381*	person_1215	-0.350	person_1415	-0.340	person_1316	-0.336	person_10	-0.490**	person_15	-0.312
	(0.223)		(0.221)		(0.220)		(0.220)		(0.222)		(0.213)
digrepcap_1015	1.722***	digrepcap_1215	1.694***	digrepcap_1415	1.634***	digrepcap_1316	1.666***	digrepcap_10	1.688***	digrepcap_15	1.606***
	(0.369)		(0.364)		(0.358)		(0.358)		(0.378)		(0.353)
gdpcon_1015	-0.000	gdpcon_1215	-0.000	gdpcon_1415	-0.000	gdpcon_1316	-0.000	gdpcon_10	-0.000	gdpcon_15	-0.000
	(0.000)		(0.000)		(0.000)		(0.000)		(0.000)		(0.000)
gdppc_1015	-0.000**	gdppc_1215	-0.000*	gdppc_1415	-0.000*	gdppc_1316	-0.000*	gdppc_10	-0.000**	gdppc_15	-0.000*
	(0.000)		(0.000)		(0.000)		(0.000)		(0.000)		(0.000)
milex_1015	0.148	milex_1215	0.131	milex_1415	0.101	milex_1316	0.112	milex_10	0.145	milex_15	0.082
	(0.171)		(0.161)		(0.158)		(0.160)		(0.185)		(0.151)
regapp_1015	-0.384	regapp_1215	-0.364	regapp_1415	-0.328	regapp_1316	-0.353	regapp_10	-0.348	regapp_15	-0.354
	(0.270)		(0.267)		(0.266)		(0.269)		(0.277)		(0.267)
terrcont_1015	0.068**	terrcont_1215	0.060*	terrcont_1415	0.058**	terrcont_1316	0.056*	terrcont_10	0.069*	terrcont_15	0.054*
	(0.033)		(0.031)		(0.029)		(0.029)		(0.040)		(0.028)
eduqual_1015	-0.827***	eduqual_1215	-0.771***	eduqual_1415	-0.717***	eduqual_1316	-0.729***	eduqual_10	-0.868***	eduqual_15	-0.665***
	(0.244)		(0.241)		(0.230)		(0.235)		(0.250)		(0.229)
adminren_1015	-0.118	adminren_1215	-0.101	adminren_1415	-0.112	adminren_1316	-0.069	adminren_10	-0.093	adminren_15	-0.181
	(0.391)		(0.394)		(0.395)		(0.394)		(0.397)		(0.403)
fiscap_1015	0.428	fiscap_1215	0.427	fiscap_1415	0.409	fiscap_1316	0.408	fiscap_10	0.224	fiscap_15	0.423
	(0.295)		(0.287)		(0.282)		(0.285)		(0.296)		(0.282)
Constant	-6.006**	Constant	-5.359**	Constant	-5.169**	Constant	-5.029**	Constant	-5.764*	Constant	-4.769**
	(2.879)		(2.674)		(2.495)		(2.535)		(3.470)		(2.422)
Observations	132	Observations	130	Observations	129	Observations	130	Observations	125	Observations	127
Pseudo R^2	0.281	Pseudo R^2	0.275	Pseudo R^2	0.269	Pseudo R^2	0.271	Pseudo R^2	0.265	Pseudo R^2	0.272

Standard errors in parentheses; *** p<0.01, ** p<0.05, * p<0.1

Table A.28. Dependent Variable dummy_spy

Year	2010-5		2012-4		2014-5		2013-6		2010		2015
Variables	dummy_spy	Variables	dummy_spy	Variables	dummy_spy	Variables	dummy_spy	Variables	dummy_spy	Variables	dummy_spy
journhrs_1015	0.385	journhrs_1215	0.423	journhrs_1415	0.440	journhrs_1316	0.445	journhrs_10	0.290	journhrs_15	0.486*
	(0.277)		(0.276)		(0.276)		(0.280)		(0.266)		(0.271)
person_1015	-0.400*	person_1215	-0.380*	person_1415	-0.378*	person_1316	-0.368*	person_10	-0.472**	person_15	-0.347*
	(0.219)		(0.216)		(0.215)		(0.215)		(0.217)		(0.209)
digrepcap_1015	1.586***	digrepcap_1215	1.550***	digrepcap_1415	1.504***	digrepcap_1316	1.526***	digrepcap_10	1.583***	digrepcap_15	1.481***
	(0.354)		(0.347)		(0.343)		(0.342)		(0.370)		(0.339)
gdpcon_1015	0.000	gdpcon_1215	0.000	gdpcon_1415	-0.000	gdpcon_1316	-0.000	gdpcon_10	0.000	gdpcon_15	-0.000
	(0.000)		(0.000)		(0.000)		(0.000)		(0.000)		(0.000)
gdppc_1015	-0.000**	gdppc_1215	-0.000*	gdppc_1415	-0.000*	gdppc_1316	-0.000	gdppc_10	-0.000**	gdppc_15	-0.000
	(0.000)		(0.000)		(0.000)		(0.000)		(0.000)		(0.000)
milex_1015	0.098	milex_1215	0.091	milex_1415	0.064	milex_1316	0.071	milex_10	0.072	milex_15	0.048
	(0.170)		(0.160)		(0.157)		(0.159)		(0.185)		(0.150)
regapp_1015	-0.344	regapp_1215	-0.320	regapp_1415	-0.303	regapp_1316	-0.322	regapp_10	-0.334	regapp_15	-0.333
	(0.264)		(0.261)		(0.261)		(0.264)		(0.275)		(0.263)
terrcont_1015	0.071**	terrcont_1215	0.063**	terrcont_1415	0.061**	terrcont_1316	0.059**	terrcont_10	0.078**	terrcont_15	0.057**
	(0.033)		(0.031)		(0.029)		(0.029)		(0.040)		(0.028)
eduqual_1015	-0.776***	eduqual_1215	-0.712***	eduqual_1415	-0.657***	eduqual_1316	-0.668***	eduqual_10	-0.861***	eduqual_15	-0.615***
	(0.234)		(0.230)		(0.221)		(0.225)		(0.248)		(0.221)
adminren_1015	-0.168	adminren_1215	-0.148	adminren_1415	-0.156	adminren_1316	-0.136	adminren_10	-0.181	adminren_15	-0.221
	(0.384)		(0.385)		(0.387)		(0.385)		(0.393)		(0.394)
fiscap_1015	0.288	fiscap_1215	0.288	fiscap_1415	0.272	fiscap_1316	0.278	fiscap_10	0.137	fiscap_15	0.294
	(0.287)		(0.279)		(0.274)		(0.277)		(0.291)		(0.274)
Constant	-6.291**	Constant	-5.587**	Constant	-5.404**	Constant	-5.267**	Constant	-6.658*	Constant	-5.023**
	(2.850)		(2.671)		(2.495)		(2.526)		(3.482)		(2.423)
Observations	132	Observations	130	Observations	129	Observations	130	Observations	125	Observations	127
Pseudo R^2	0.246	Pseudo R^2	0.239	Pseudo R^2	0.236	Pseudo R^2	0.237	Pseudo R^2	0.235	Pseudo R^2	0.240

Standard errors in parentheses; *** p<0.01, ** p<0.05, * p<0.1

Table A.29. Dependent Variable dummy_for

Year	2010-5		2012-4		2014-5		2013-6		2010		2015
Variables	dummy_for	Variables	dummy_for	Variables	dummy_for	Variables	dummy_for	Variables	dummy_for	Variables	dummy_for
journhrs_1015	0.662	journhrs_1215	0.718*	journhrs_1415	0.677	journhrs_1316	0.706*	journhrs_10	0.627*	journhrs_15	0.686*
	(0.409)		(0.417)		(0.414)		(0.422)		(0.372)		(0.404)
person_1015	0.337	person_1215	0.368	person_1415	0.391	person_1316	0.367	person_10	0.258	person_15	0.381
	(0.264)		(0.264)		(0.265)		(0.268)		(0.266)		(0.266)
digrepcap_1015	1.515***	digrepcap_1215	1.617***	digrepcap_1415	1.561***	digrepcap_1316	1.651***	digrepcap_10	1.355***	digrepcap_15	1.524***
	(0.491)		(0.511)		(0.512)		(0.517)		(0.466)		(0.508)
gdpcon_1015	0.000	gdpcon_1215	0.000	gdpcon_1415	-0.000	gdpcon_1316	-0.000	gdpcon_10	-0.000	gdpcon_15	-0.000
	(0.000)		(0.000)		(0.000)		(0.000)		(0.000)		(0.000)
gdppc_1015	0.000	gdppc_1215	0.000	gdppc_1415	0.000	gdppc_1316	0.000	gdppc_10	0.000	gdppc_15	0.000
	(0.000)		(0.000)		(0.000)		(0.000)		(0.000)		(0.000)
milex_1015	-0.010	milex_1215	-0.057	milex_1415	-0.066	milex_1316	-0.028	milex_10	0.131	milex_15	-0.059
	(0.245)		(0.239)		(0.222)		(0.231)		(0.253)		(0.207)
regapp_1015	-0.588	regapp_1215	-0.674*	regapp_1415	-0.692*	regapp_1316	-0.716*	regapp_10	-0.517	regapp_15	-0.672*
	(0.360)		(0.370)		(0.379)		(0.383)		(0.350)		(0.376)
terrcont_1015	0.044	terrcont_1215	0.038	terrcont_1415	0.034	terrcont_1316	0.037	terrcont_10	0.052	terrcont_15	0.030
	(0.042)		(0.040)		(0.040)		(0.041)		(0.051)		(0.038)
eduqual_1015	-1.104***	eduqual_1215	-1.101***	eduqual_1415	-1.056***	eduqual_1316	-1.083***	eduqual_10	-1.109***	eduqual_15	-1.012***
	(0.323)		(0.333)		(0.332)		(0.337)		(0.335)		(0.327)
adminren_1015	-0.074	adminren_1215	0.003	adminren_1415	0.068	adminren_1316	0.084	adminren_10	-0.037	adminren_15	0.121
	(0.516)		(0.514)		(0.509)		(0.513)		(0.533)		(0.511)
fiscap_1015	1.057**	fiscap_1215	1.043**	fiscap_1415	0.998**	fiscap_1316	0.997**	fiscap_10	0.734*	fiscap_15	1.009**
	(0.460)		(0.456)		(0.436)		(0.445)		(0.435)		(0.437)
Constant	-6.582*	Constant	-6.083*	Constant	-5.860*	Constant	-6.205*	Constant	-7.210	Constant	-5.502
	(3.755)		(3.613)		(3.562)		(3.701)		(4.570)		(3.436)
Observations	132	Observations	130	Observations	129	Observations	130	Observations	125	Observations	127
Pseudo R^2	0.303	Pseudo R^2	0.320	Pseudo R^2	0.324	Pseudo R^2	0.331	Pseudo R^2	0.268	Pseudo R^2	0.325

Standard errors in parentheses; *** p<0.01, ** p<0.05, * p<0.1