AUTHORITARIAN SURVIVAL IN THE DIGITAL AGE – INTERNET ACCESS AND CONTROL IN AFRICAN AUTOCRACIES

D I S S E R T A T I O N

of the University of St.Gallen,
School of Management,
Economics, Law, Social Sciences,
International Affairs and Computer Science,
to obtain the title of
Doctor of Philosophy in International
Affairs and Political Economy

submitted by

Lisa Marie Garbe

from Germany

Approved on the application of

Prof. Dr. Tina Freyburg

and

Prof. Dr. Carl Henrik Knutsen

Dissertation no. 5105

Difo-Druck GmbH Untersiemau

AUTHORITARIAN SURVIVAL IN THE DIGITAL AGE – INTERNET ACCESS AND CONTROL IN AFRICAN AUTOCRACIES

D I S S E R T A T I O N

of the University of St.Gallen,
School of Management,
Economics, Law, Social Sciences,
International Affairs and Computer Science,
to obtain the title of
Doctor of Philosophy in International
Affairs and Political Economy

submitted by

Lisa Marie Garbe

from Germany

Approved on the application of

Prof. Dr. Tina Freyburg

and

Prof. Dr. Carl Henrik Knutsen

Dr. Joss Wright

Dissertation no. 5105

Difo-Druck GmbH Untersiemau

The University of St.Gallen, School of Management, Economics, Law, Social Sciences, International Affairs and Computer Science, hereby consents to the printing of the present dissertation, without hereby expressing any opinion on the views herein expressed.

St.Gallen, May 20, 2021

The President:

Prof. Dr. Bernhard Ehrenzeller

ACKNOWLEDGEMENTS

I am deeply grateful to Tina Freyburg who provided me with tremendous support and inspiration throughout the entire journey of this thesis. Tina pushed me to take on challenging tasks and think beyond disciplinary boundaries. Her (sometimes overwhelmingly) detailed feedback has significantly improved my arguments and writing. But not only for her intellectual input, I also owe Tina gratitude for her hospitality during multiple stays in Zurich and great company during hour-long cycles through Toronto and perilous boda boda rides in Kampala: It was a great pleasure and I look forward to continue working on joint projects. Thank you, Tina.

Furthermore, I would like to thank Carl Henrik Knutsen who has been an attentive and critical supervisor and whose comments were always on point. His work inspired my thinking and helped me tackle multiple of the questions raised in this thesis. I also thank Joss Wright who was kind enough to host me at the Oxford Internet Institute and provided important technical perspectives on my work.

I am very grateful to Véronique Wavre who has not only shared an office with me in St.Gallen but also my daily ups and downs during the phase of data collection. Thank you, Vero, also for taking care of the chocolate supply to our office and saving my mood during rough St.Gallen winter days. I also thank the rest of the team at the Chair for Comparative Politics: Michael Asiedu, Martina Fuerrutter, Hugo Marcos Marné, Karina Mross, and Ciaran O'Flynn. You have been great company not only in the office, but also during these last four years. Thank you for making me do some sports and discovering the surroundings. I am also grateful to Frank Schimmelfennig's team at ETH Zurich for great discussions and feedback during four years of winter retreat.

In addition to the team at the Chair for Comparative Politics, I thank my fellow (former) PhD students at the Department for Political Science, notably Gina Di Maio, Manali Kumar, Simon Pistor, Sebastian Plappert, Lina Seitzl, and Daniel Unterweger. You made me enjoy going to the office every day and ensured that, during hour-long lunch or coffee breaks, I did not miss to discuss the actually important things in life: epic movies, epic food, or epic Trump fails. I am grateful to you for making my time in St. Gallen truly enjoyable. I really miss excellent dinner events and hikes in Appenzell.

A number of people accompanied me during these past four years and deserve a special mention in this acknowledgement. Steven Livingston, whom I met right at the beginning of my PhD, has not only been a great source of intellectual input, but also supported several of my funding applications. Besides, I thank Nic Cheeseman, Ron Deibert, Anita Gohdes, and Daniela Stockmann, whom I met at different stages of my PhD, for inspiring my work. I further thank Peter William Walsh, who critically read and commented

on my writing, but also made sure I spent enough time in English pubs. I am grateful to Daniëlle Flonk, Pauline Lemaire, Lisa-Marie Selvik, and Jan Rydzak for their interest in my research and great conversations that are reflected in this thesis. Finally, I owe gratitude to multiple student assistants who provided crucial support in collecting the data analysed in this thesis: Thank you, Dominic Brotschi, Johannes Matt, Carlos Morado, Helen Pittam, Henry Schmees, and Suen Wang.

This thesis would not have been possible without the support of several people during my field stays in Uganda. In particular, I thank Daniel Mwesigwa, Bill Daniel Opio, and Stacie Cuby Wria who not only provided critical perspectives on my research, but also made me feel home in Kampala. I further thank Research World Ltd, CEON-U, and the National Democratic Institute, who kindly collected and provided data for my research. Most importantly, I owe gratitude to all interviewees I met in Kampala, Gulu, and Kitgum, who shared their time, knowledge, and experiences with me.

I also want to thank my family and friends who always showed interest in what I am doing, listened to my complaints, and did not become tired of visiting me. Finally, I thank Theo Maria Santiago Lorenzo Toppe for supporting my decision to start a PhD, for spending endless hours on the train, and for coming to Oxford with me. You have not only made sure that the fridge was never empty in these last months of writing, but also critically engaged with my work. Your passionate speeches about early childhood research have (weirdly enough) enhanced my own interest in academic work. Without you, I may not have started this PhD in the first place. Thank you, Theo, for your inspiration.

Berlin, 01.08.2021

Lisa Garbe

TABLE OF CONTENTS

Summary V

Zusammenfassung VI

General Introduction 1

1.1 Research gap and questions 4

1.2 Theoretical perspectives 6

1.3 Methodology 11

1.4 Outlook 15

Pulling through elections by pulling the plug: Internet disruptions and electoral violence 16

2.1 Introduction 17

2.2 Electoral violence in authoritarian regimes 18

2.3 Theory 20

2.4 The Case of Uganda's 2016 presidential elections 24

2.5 Research design 25

2.6 Results 28

2.7 Understanding the impact of the internet disruption 29

2.8 Discussion and conclusion 31

Telecommunications Ownership and Control (TOSCO). A new dataset to explore the political power of internet business in Africa, 2000-2019 34

3.1 Introduction 35

3.2 Conceptualising ownership as variable in political science research 37

3.3 The TOSCO dataset 43

3.4 Telecommunications ownership and the political effects of the internet 51

3.5 Discussion and outlook 53

Political Determinants of Foreign Investment in Internet Infrastructure in African Autocracies 55

4.1 Introduction 56

4.2 Internet infrastructure and control 58

4.3 Theory 59

4.4 Empirical approach 64

4.5 Results 68

4.6 Discussion 71

4.7 Conclusion 73

Blocking the Bottleneck: Internet Shutdowns and Ownership at Election Times in Sub-Saharan Africa 74
5.1 Introduction ... 75
5.2 Internet shutdowns in election times ... 77
5.3 State control and ownership of the internet's physical infrastructure ... 80
5.4 Research design and operationalisation of variables ... 81
5.5 Results ... 85
5.6 Discussion and outlook ... 88
5.7 Conclusion ... 90
General Conclusion ... 92
6.1 Main contributions ... 92
6.2 Avenues for future research ... 94
6.3 Concluding remarks ... 97
References ... 98
Appendices ... 114

LIST OF TABLES

Table 1. Overview of theories 7

Table 2. Descriptive statistics 26

Table 3. Properties of owner identities 40

Table 4. Shareholders with at least four subsidiaries 50

Table 5. Estimated effect of state-owned ISPs on democratic change in Africa 53

Table 6. Descriptive statistics 65

Table 7. Results from linear mixed models 70

Table 8. Calibrated data 82

Table 9. csQCA output—parsimonious solution for internet shutdowns (negative outcome) 85

Table 10. csQCA output—parsimonious solution for internet shutdowns (positive outcome) 86

LIST OF FIGURES

Figure 1. Internet and social media blocking worldwide in 2019 5

Figure 2. Electoral autocracies 1990–2019 12

Figure 3. Economic and political indicators in African autocracies, 2018 13

Figure 4. Election violence during African elections 2015-2018 17

Figure 5. Theoretical argument 20

Figure 6. Electoral violence in Uganda, 2016 28

Figure 7. Marginal effects of opposition support on violence conditioned by internet access 29

Figure 8. Structure of telecommunications ownership in 2019 Angola 45

Figure 9. Distribution of the identity of the majority owner, 2000-2019 48

Figure 10. Patterns of state involvement in the telecommunications sector, 2000-2019 49

Figure 11. Share of majority-foreign owned ISPs in Africa, 2000-2019 57

Figure 12. Aggregated shares of foreign majority-owned ISPs per country 67

Figure 13. Foreign investment in ISPs 2000-2019 69

SUMMARY

Why do some autocrats tightly control internet access while others do not? Since the early days of the internet, political scientists have studied the dilemma facing authoritarian regimes in the digital age: On one hand, adopting internet technologies has become inevitable for economic growth; on the other, authoritarian governments risk losing their monopoly over information and communication when granting internet access to the broader population. To mitigate potential challenges arising from access to new information and communication technologies, some authoritarian governments strictly control internet access by censoring, blocking, or manipulating digital information flows. This thesis investigates authoritarian governments' motive and capacity to exert control over internet access.

Methodologically, this thesis combines large-*N* statistical analyses with case studies and in-depth interviews to shed light on the ways in which authoritarian governments respond to increasing digitalisation. My research highlights the shortcomings of comparative studies treating the internet as a technical 'black box' and contributes to a more nuanced understanding of the conditions under which internet access and use can challenge authoritarian rule.

The thesis consists of four studies that are presented in related but independent research papers. Evidence from the first study, analysing Uganda's presidential elections in 2016, suggests that opposition supporters benefit from internet access to report about electoral malpractice and mobilise support; at the same time, opposition supporters with higher internet access face greater risk of electoral violence. In another set of studies, I focus on the role of internet service provider (ISP) ownership in shaping a government's capacity to exert control over internet access. The second study theorises the way in which ownership reflects state-business relations and demonstrates that state ownership is negatively associated with democratisation. The third study zooms into the determinants of ISP ownership and finds that authoritarian governments that rely on repression of their population attract more foreign investors from other autocracies. Finally, the fourth study investigates the effects of ISP state ownership. The results suggest that state ownership of ISPs facilitates the blocking of internet access during politically contested times, yet also point to further mechanisms of government control over ISPs.

ZUSAMMENFASSUNG

Warum entscheiden sich manche Autokratien dafür, Internetzugang weitreichend zu kontrollieren – und andere nicht? Seit den Anfängen des Internets untersuchen Sozialwissenschaftler:innen das Dilemma, mit dem sich Autokratien durch eine fortschreitende Digitalisierung konfrontiert sehen: Einerseits sind Internettechnologien unabdingbar für wirtschaftlichen Erfolg geworden. Andererseits riskieren autokratische Regierungen mit zunehmender Digitalisierung, die Kontrolle über Information und Kommunikation zu verlieren. Um die Risiken digitaler Technologien abzumildern, üben einige Autokratien strikte Kontrolle über Interzugang aus, indem sie digitale Inhalte zensieren, manipulieren oder blockieren. Meine Forschung untersucht die Motivation und Kapazität von autokratischen Regierungen, Interzugang zu kontrollieren.

Methodisch kombiniert die Arbeit quantitative Verfahren mit qualitativen Interviews und Fallstudien, um den Umgang autokratischer Regierungen mit zunehmender Digitalisierung besser zu verstehen. Die Arbeit zeigt die Schwachstellen bisheriger Studien auf, die das Internet als 'Black Box' behandeln, und trägt so zu einem differenzierteren Verständnis der Bedingungen bei, unter denen Internetzugang autokratische Herrschaft gefährden kann.

Die Arbeit besteht aus vier unabhängigen Studien: Die erste Studie, die sich mit den Präsidentschaftswahlen in Uganda im Jahr 2016 beschäftigt, legt nahe, dass Oppositionelle während Wahlen von Internetzugang profitieren, da dieser ihnen ermöglicht, Wahlmanipulation anzuprangern und dagegen zu mobilisieren. Gleichzeitig zeigen die Ergebnisse, dass Oppositionelle in Gebieten mit stärkerer Internetanbindung auch einem erhöhten Risiko staatlicher Repression ausgesetzt sind. Die übrigen Studien beschäftigen sich damit, wie Internetanbieter die Kapazität von Regierungen beeinflussen, Internetzugang zu kontrollieren. Die zweite Studie gibt einen theoretischen Überblick darüber, inwiefern Eigentumsverhältnisse die Beziehungen zwischen Staat und Unternehmen reflektieren, und zeigt, dass Staatseigentümerschaft negativ mit Demokratisierung zusammenhängt. Die dritte Studie analysiert, welche Faktoren den Anteil ausländischer Anteilseigner an lokaler Internetinfrastruktur in Autokratien erklären. Die Resultate legen nahe, dass Autokratien, die ihre Bevölkerung unterdrücken, offener für Investitionen aus anderen Autokratien sind. In der letzten Studie untersuche ich mögliche Effekte von Staatseigentümerschaft von Internetanbietern. Die Ergebnisse deuten an, dass Staatseigentümerschaft ein begünstigender Faktor für Internet-Blockaden während Wahlen ist, verweisen aber auch auf andere Mechanismen staatlicher Kontrolle über Internetanbieter.

GENERAL INTRODUCTION

The digital revolution has confronted authoritarian rulers around the globe with one inherent problem: if they adopt internet technologies and embrace associated economic profits, they risk losing their monopoly on controlling access to information and communication. Most authoritarian countries have made efforts to adopt internet technologies, some of which have even outperformed Western countries in terms of connectivity (Stier, 2017). In fact, it appears that those regimes that are most reluctant to an analogue independent public sphere, are even more likely to foster the adoption of internet technologies than less rigid regimes (Rød & Weidmann, 2015). In order to address the so-called "dictator's dilemma" (Kedzie, 1997) arising from the adoption of internet technologies, authoritarian governments have developed different ways of controlling access to information and communication online, including censorship, filtering, and blocking (Deibert et al., 2010; Deibert et al., 2008; Deibert, 2013). However, not all authoritarian regimes have been equally engaged in efforts to control the internet. Most studies comparing the determinants and effects of control of information and communication technologies (ICT) across authoritarian regimes have focused on censorship or surveillance techniques (e.g. Hellmeier, 2016; Stoycheff, Burgess, & Martucci, 2020), but tend to neglect control over basic internet infrastructure. This is especially noteworthy since most forms of manipulation of ICT require control over access to basic internet infrastructure (DeNardis & Musiani, 2016). This thesis aims to better understand the dynamics of control over internet access in authoritarian contexts, notably at election times. The overarching research question of this thesis is: *Under what conditions can authoritarian governments exert control over access to the internet?*

Throughout this thesis, I address this question from different angles, broadly distinguishing between factors that inform a government's motive and capacity to control internet access and use. First, I investigate how new characteristics of ICT may strengthen opposition actors in authoritarian regimes, particularly at election times, and hence be perceived as a threat to regime survival. Second, I examine regime-specific characteristics that explain authoritarian governments' openness to investment in the telecom sector and constrain their capacity to control access to, and the flow of, digital information. Third, I look at how state ownership of telecom operators enhances a government's capacity to disrupt internet access at

election times. Overall, the thesis consists of four studies that are presented in independent but related research papers:

The first study "Pulling through elections by pulling the plug: Internet disruptions and electoral violence", examines the role of ICT for opposition actors in authoritarian contexts with a particular focus on elections. By zooming into the case of Uganda's presidential elections in 2016, which were accompanied by a temporary halt of access to social media, I examine ICT use by opposition supporters, and state violence, across opposition strongholds with differential internet access. Drawing on qualitative interviews, this study sheds light on the ways in which a shutdown can prevent opposition actors from challenging electoral malpractice.

The second study, "Telecommunications Ownership and Control (TOSCO). A new dataset to explore the political power of internet business in Africa, 2000-2019" (joint work with Tina Freyburg and Veronique Wavre), provides a detailed discussion of the conceptualisation and operationalisation of ownership as a variable and the significance of ownership as a means to exercise power over access to the internet. It thereby problematises the role of telecom owners in resisting or fostering democratising features of internet use. Using replication data from a study by Rød and Weidmann (2015), we demonstrate that not internet penetration as such, but rather control over those companies providing internet access, may foster authoritarian survival.

The third study, "Political determinants of foreign investment in internet infrastructure in African autocracies", examines the variation of foreign ownership in domestic internet service providers (ISPs) across authoritarian African regimes. I argue that authoritarian regimes should be hesitant to accept foreign investment in domestic internet infrastructure, because they seek to establish and maintain control over access to ICT. Using data from both foreign and domestic ownership of ISPs, I illustrate that in authoritarian regimes, openness to foreign investment in the telecom sector depends on a regime's traditional reliance on repression and co-optation of the opposition. Specifically, the results indicate that authoritarian regimes relying on repression are more likely to accept investment from like-minded regimes.

The fourth study, "Blocking the bottleneck: Internet shutdowns and ownership at election times in sub-Saharan Africa" (joint work with Tina Freyburg), links documented internet shutdowns in sub-Saharan African countries to configurations of ISP state majority ownership, regime type, and election violence. The results reveal a positive relationship between a temporary halt of internet provision and ISP majority ownership by authoritarian states when facing election-related violence, yet also illustrate the importance of alternative means to exert control over ISPs.

The thesis is novel and original in terms of theory, evidence, and methodology. Theoretically, it re-evaluates and adds to theories on authoritarian survival by closely examining the motive and capacity of authoritarian regimes to control internet access and use. The way in which access to the internet has changed how people communicate and share information presents novel challenges for the survival of governments, notably in electoral autocracies. By focusing on the role of ICT during elections, I provide new insights into the way internet-based ICT can help to monitor and address analogue forms of electoral manipulation and may therefore trigger digitally repressive responses by their governments. By conceptualising ISP ownership as a means to control internet access, I expand on existing theories of (digital) repression that underline the importance of internet infrastructure. Specifically, I elaborate on complex state-business relations that shape a government's capacity to control internet access.

Empirically, this thesis contributes to the study of a region that tends to be neglected in research on internet censorship and manipulation. Despite the increasing number of reports on incidences of internet manipulation in Africa (Anthonio, 2019), most empirical studies on information controls focus on China, Russia, or the Arab World. By using original data, this thesis provides an important empirical contribution to further understanding these phenomena in authoritarian-developing contexts. First, the dataset on ISP ownership offers a unique data collection to account for the role of internet infrastructure and its ownership in understanding the complex interplay between state and corporate actors in manipulating internet access. Second, by combining survey data and information about electoral violence from polling stations across Ugandan districts, I suggest an innovative approach to understanding the impact of internet disruptions.

Methodologically, this thesis uses a mixed-methods approach, including time-series cross-sectional statistical analyses, in-depth interviews, and case studies to shed light on the conditions under which authoritarian rulers exert control over internet access. By aggregating fine-grained company-level information, it provides a realistic assessment of the extent to which internet infrastructure is controlled by varying owners across countries and over time. Furthermore, by examining levels of internet penetration across opposition-leaning counties in Uganda, it assesses intra-country variance of ICT use and electoral violence to produce a more nuanced understanding of internet use in authoritarian contexts and the consequences of internet disruptions.

Overall, the presented research is not only scientifically relevant, but has important implications for citizen activists and policy-makers. This thesis evaluates the ways in which ICT use challenges authoritarian elections, and the means by which authoritarian rulers prevent and react to challenges arising from ICT. The comparative analysis of control over internet access and its effects on electoral conduct draws attention to the importance of securing communication and the use of alternative means for election

monitoring. An evaluation of corporate actors and their involvement in manipulation of internet access raises important legal, ethical, and corporate social responsibility concerns.

1.1 Research gap and questions

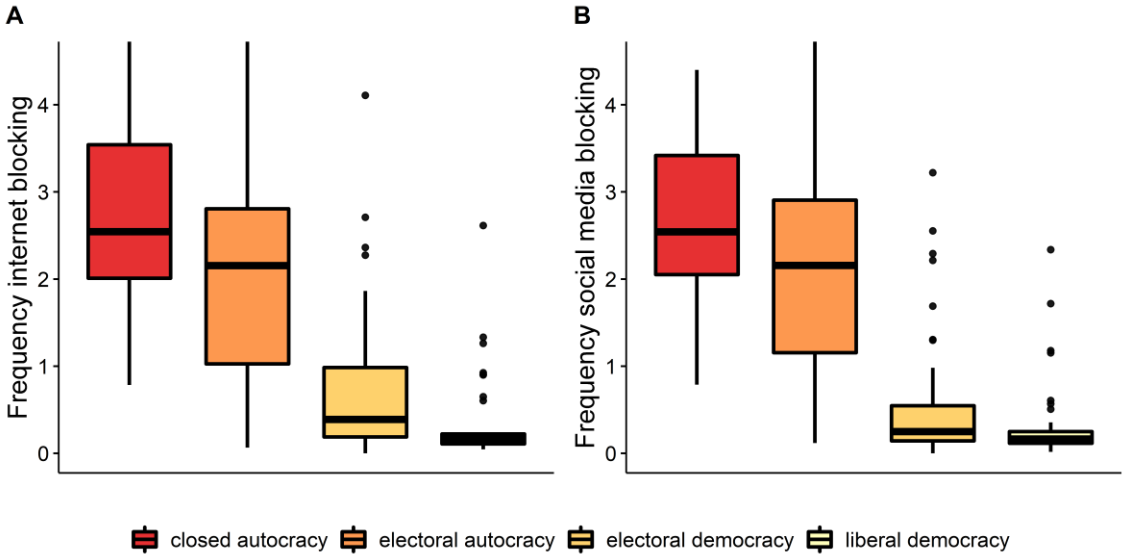
Lessig (2006: 123f) argued that there are four constraints to the free use of the internet: law, social norms, the market, and the internet's architecture. Focusing on authoritarian contexts, Boas (2006: 3) reasons that "by manipulating the architecture of a flexible technology, and by leveraging influence over laws, social norms, and the market […], the leaders of authoritarian regimes can exert control over the use of a supposedly control-frustrating technology". Deibert *et al.* (2010) categorise these different mechanisms of control as *overt and covert tracks*. While the overt track aims to legalise content controls (by defining conditions under which certain types of content may be restricted), the covert track creates technical possibilities for the application of content controls (ibid.). Efforts by data scientists to measure internet activity in order to disclose practices of censorship, surveillance, or network disruptions[1] show that the covert track of internet controls is widely applied by governments across the world.

However, the degree to which governments systematically use technical forms of controlling ICT seems to vary across and within non-democratic countries (Hellmeier, 2016). Figure 1 illustrates the variance of the frequency by which governments fully disrupt internet access or block access to social media across regime types in 2019. Specifically, it plots a country's regime type against the frequency of internet and social media blocking by the government (Coppedge *et al.*, 2020a). While most liberal and electoral democracies display a low frequency of internet blocking ($M = 0.92$, $SD = 0.73$) and social media shutdowns ($M = 0.99$, $SD = 0.68$), the frequency of shutdowns in closed and especially in electoral autocracies appears to vary more substantially ($M = -0.74$, $SD = 1.18$ for shutdowns; $M = -0.64$, $SD = 1.28$ for social media shutdowns).[2] A similar trend can be observed for the frequency of internet filtering (see Appendix A1) and for a subsample of African countries (see Appendix A2). Country-specific trends underline this variation: in Chad, an electoral autocracy in central Africa, the government frequently blocks access to web content, in particular big social media platforms such as Twitter, Facebook, or WhatsApp (Internet Sans Frontières, 2018; Giles & Mwai, 2020). By contrast, other electoral autocracies, such as Zambia and Madagascar, are largely considered free from internet blocking. In consequence, the main aim of this thesis *is to explain the conditions under which authoritarian regimes can exert control over access to the internet, and the ways in which they do so*.

[1] The Open Network Initiative [https://opennet.net/] and the Open Observatory of Network Interference [https://ooni.torproject.org/], for instance, provide detailed information about censorship, surveillance, and traffic manipulation for large parts of the world.

[2] Lower values indicate higher frequencies of blocking.

Figure 1. Internet and social media blocking worldwide in 2019



Note. Colours indicate the four categorical regime types closed autocracies (red), electoral autocracies (light right), electoral democracies (light blue), and liberal democracies (blue) following Lührmann, Lindberg and Tannenberg (2017). Variables for frequency of internet blocking (*v2govshut*) and social media blocking (*v2smgovsm*) come from the Varieties of Democracy project (V-Dem; Coppedge *et al.*, 2020b).

Comparativists pay increasing attention to the effects of internet penetration on democratisation (Rød & Weidmann, 2015), violence (Pierskalla & Hollenbach, 2013), and collective action (Bailard, 2015). Studies using internet penetration as a proxy for "digital threat" have important caveats, however. Internet penetration may not accurately reflect the potential threat of digital technologies to authoritarian survival, since internet access may be limited to urban and regime-critic elites where it can have regime-challenging potential despite low connectivity (Nisbet, Stoycheff, & Pearce, 2012). This is illustrated by many African autocrats manipulating internet access in countries with extremely low internet penetration rates, such as Chad, the Democratic Republic of Congo, and Ethiopia in 2019. Therefore, it seems important to study internet use by individuals in authoritarian countries to understand whether and how internet access may pose a threat to authoritarian survival and hence motivate government control over internet access. The first sub-question of this thesis is: *How can internet use by individuals challenge authoritarian survival?*

Even if governments perceive internet access and use on their territory as a potential threat to their rule, not all of them may respond in the same way. The hierarchical structure of the internet allows for control at different layers, most notably at the infrastructural, the network, and the application layer (Keremoğlu & Weidmann, 2020). Egyptian authorities, for instance, rely on direct blocking of access to specific websites (Dada & Sayadi, 2017), whereas Ethiopia has repeatedly cut internet access entirely for parts of the country (Workneh, 2020). Despite the increasing number of studies that uncover different techniques used by governments to suppress, monitor, or manipulate internet access, few scholars have analysed

systematically how governments are actually capable of doing so. The second sub-question of this thesis is therefore: *How do authoritarian governments control internet access?*

It looks like countries worldwide seek to expand internet access whether they are democratic or not (Stier, 2017). This is plausible, since in the 21st century internet connectivity is inevitably linked to economic progress. However, due to the high fixed-costs that are needed to set up internet infrastructure, such as for copper and fibre (Greenstein, 2020), many governments rely on private and foreign investors. In the Western world, internet infrastructure has therefore been increasingly privatised over the last few decades (Leiponen, 2006; DeNardis, 2014). Hence, private actors have gained enormous control over those parts of the internet's infrastructure that are "essential for Internet usage" (Eriksson & Giacomello, 2009: 208). This may present governments whose political survival rests upon strong control over the public sphere with a dilemma (Kedzie, 1997): "how to benefit from the global economy without relinquishing domestic control"? Maintaining tight control over access to information becomes more difficult once people have access to the global internet. While state control over internet access may be the most straight-forward way to censor and manipulate information flows, many countries in the Global South rely on foreign investment in order to build and maintain internet infrastructure. This leads to the third sub-question guiding this thesis: *What factors constrain government control over internet access?*

1.2 Theoretical perspectives

In seeking answers to these three questions, I combine insights from several theoretical strands to understand the conditions under which authoritarian African rulers can control access to the internet. I rely on insights from theories of authoritarianism, political communication, and international business, to outline how the use of ICT challenges the traditional strategies of authoritarian rulers to hold onto power, and why and when rulers seek to prevent and manipulate such usage (see Table 1).

By taking into account the role of internet technologies and their ownership, as well as the ways in which they change access to information and communication, I add new perspectives to theories of authoritarian survival in the digital age. First, by acknowledging the new opportunities provided by ICT to overcome collective action problems and challenge electoral malpractice, I contribute to theories on political communication and electoral malpractice (see 1.2.1.). Second, by outlining how ISP ownership influences a government's capacity to control internet access, I underline the importance of state-business relations for (digital) repression (see 1.2.2.). Third, by highlighting the ways in which authoritarian governments respond to institutional pressure to expand internet access, I point to the global dimension of authoritarianism and the increasing importance of authoritarian collaboration to maintain control over internet access and use (see 1.2.3.).

Table 1. Overview of theories

Question & Chapter	Theoretical Assumptions	Key Works
Question: *How can internet use by individuals challenge authoritarian survival?* **Sub-Chapter:** 1.2.1. Internet use in authoritarian environments	• citizens typically face collective action problems, notably at election times • ICT help overcome collective action problems by lowering costs and providing flexible communication • ICT offer the possibilities to express opinions anonymously and mitigate preference falsification	• Edwards & McCarthy 2004; Gurr 2015; McCarthy & Zald 1977; Tilly 1978; Turner & Killian 1957; Bhasin & Gandhi 2013; Friedrich & Brzezinski, 1963; Kuran 1989; Simmons 2014 • Bennett & Segerberg 2013; Bimber 2017; Habermas 2005; Mutsvairo 2016; Rauchfleisch & Kovic 2016 • Farrel 2012; Mare 2016; Karekwaivanane 2019; Rasmussen 2017
Question: *How do authoritarian governments effectively control internet access?* **Sub-Chapter:** 1.2.2. Ownership of internet service providers	• owners have instrumental power to and structural power over a company • power to: owners' goals and risk aversion depend on owner identity • power over: the number of shares determines power concentration of owners	• Culpepper 2011; Fuchs 2005; Göhler 1972; Pitkin 1972 • Birkinshaw et al. 2006; La Porta et al. 1999 ; Leech 2013 ; Strange 2018; Shleifer & Vishny 1997; Thomsen & Pedersen 2000 • Bennedzen & Wolfenzon; Holderness & Sheehan 1988; Thomsen & Pedersen 2000
Question: *What factors constrain government control over internet access?* **Sub-Chapter:** 1.2.3. Institutional Constraints in Autocracies	• authoritarian survival rests upon repression, co-optation, and legitimation • authoritarian rulers' reliance on repression and co-optation shape their openness towards FDI in internet infrastructure • authoritarian rulers prefer FDI from foreign-autocratic investors	• Gerschewski 2013; Frantz & Kendall-Taylor 2014; Maerz & Schneider 2017 • Davenport 2007; Bueno de Mesquita et al. 1999, 2003; Gandhi 2008; Gohdes 2020; Magaloni 2008; Wintrobe 1990; Rommel 2018; Conrad 2011; Xu 2020 • Ambrosio 2010; Bader et al. 2010; Cooley 2015; Schmotz & Tansey 2017; von Soest 2015

1.2.1 Internet use in authoritarian environments

Several observers attribute the success of the social movements during the so-called "Arab Spring" to digital media, labelling them as "Facebook revolution[s]" or "Twitter uprisings" (Harlow, 2013; El-Nawawy, Khamis, & Khamis, 2012). While scholars are hesitant to infer a monocausal relationship between digital media and social movements, they point to their catalyst function in facilitating protest (Howard & Hussain, 2011). In a pre-internet era, the public was largely dependent on mass media as an observing and listening audience. In most authoritarian countries, the public sphere is severely restricted as traditional media outlets are often subject to tight government control (Djankov et al., 2003). Following recent theoretical work in political communication, I argue that internet access has changed the opportunities for anti-regime movements in authoritarian regimes through two different logics: First, the (purported) anonymity of the internet helps overcome problems of preference falsification and connect marginalised members of a community. Second, internet access helps citizens and opposition actors to overcome typical collective action problems. Jointly, these factors are likely to challenge authoritarian survival and hence motivate governments to exert control over internet access.

In authoritarian regimes, individuals are often faced with the problem of "preference falsification" (Kuran, 1989): even if they secretly favour the opposition, they may be afraid to share their true opinions due to the threat of being punished and the uncertainty about others' opinions. This makes it extremely difficult to learn about the extent to which grievances are shared, a condition that is regarded as fundamental for the emergence of collective action (Gurr, 2015; Turner & Killian, 1957; Simmons, 2014). New forms of ICT are said to mitigate this problem as the alleged anonymity of the internet encourages people to share their true beliefs and hence learn about the extent of regime opposition (Farrell, 2012; Tufekci & Wilson, 2012). This anonymity can also make it more difficult for governments to repress public opinion. For example, in Zimbabwe, the profile of political blogger Baba Jukwa, who exposed secrets from president Robert Mugabe's inner circle, attracted more than 400.000 followers (Flanagan, 2014). Mugabe put a bounty of 300.000 USD on the person(s) in charge of Baba Jukwa's profile—an effort that was ultimately unsuccessful. This example highlights that the purported anonymity of the internet creates new opportunities for opposition members to share critical information with the broader population (Karekwaivanane, 2019).

Second, citizens are typically confronted with resource constraints to mobilisation (McCarthy & Zald, 1977). This includes the aggregation of resources, such as time and money, that are necessary to mobilise for anti-regime protest. Such resources are often scarce, especially in remote places that lack access to important infrastructure (Edwards & McCarthy, 2004). In addition, individuals often lack organisational structures that are necessary to jointly organise collective action (ibid.). As outlined by recent scholarly work in political communication, new forms of ICT help to overcome both resources constraints as well as the need for organisational structures. Internet access has made communication and access to information much cheaper, and hence allows its users to overcome traditional resources constraints to member recruitment (Rasmussen, 2014; Rauchfleisch & Kovic, 2016; Mutsvairo, 2016). In addition, the need for formal organisational structures may become obsolete with internet access, since individuals can quickly and easily share information without meeting in person (Bennett & Segerberg, 2013; Bimber, 2017).

In sum, access to the internet helps citizens overcome traditional collective action problems due to the low-cost and flexible features of the internet. This may prove particularly useful to citizens in authoritarian regimes who are usually faced with problems of resource constraints and preference falsification. In Study 1, I closely examine the internet use of regime-critic citizens in Uganda as well as the potential consequences of an internet disruption for its effectiveness.

1.2.2 Ownership of internet service providers

In 2011, facing increasing pressure by anti-regime protesters, Egypt's then-president Hosni Mubarak allegedly made just a few phone calls to local ISPs in order to shut down nearly all internet traffic in the North African country (Babu-Kurra 2011). This example highlights that a government essentially relies on those companies that offer last-mile internet, typically ISPs, to exert control over internet access. Specifically, it depends on the willingness of ISPs operating on its territory to comply with its request to manipulate internet access. In this thesis, I analyse the most straightforward way to exert control over ISPs, namely control via ownership.

Owners are defined as the entities that hold shares in a company. Business scholars have detailed how owners can exert direct control over a company's actions through their voting rights, but also informal control through meetings with the management or general assemblies (Shleifer & Vishny, 1997; Leech, 2013). This is underlined by political research on the effects of business ownership on media reporting (Bailard, 2016; Dunaway & Lawrence, 2015) or state repression (Wegenast & Schneider, 2017). Following this line of thought, I argue that a company's ownership reflects the relationship between the company and the state. When applied to the specifics of the telecom sector, company ownership reveals insights into the incentives of ISPs to provide and manipulate internet access in the face of government pressure.

Shareholders' ways of exercising influence over a company's decision-making can be conceptualised in two ways (Göhler, 2009; Pitkin, 1972). First, an owner uses instrumental power to achieve certain goals. These goals depend on the owner's identity, in particular whether the owner is public, private, financial, or whether they are an individual or family (La Porta, Lopez-De-Silanes, & Shleifer, 1999; Thomsen & Pedersen, 2000) and where its legal headquarters is registered (Strange, 2018; Birkinshaw et al., 2006). For instance, a company owned by private shareholders may largely pursue profit-maximisation, whereas a state-owned company may (also) pursue political goals. If a government wants to restrict internet access, it may face more resistance from ISPs predominantly interested in profit maximisation. In addition, shareholders coming from different jurisdictions might face additional pressure to follow international human rights and corporate social responsibility standards (Birkinshaw et al., 2006; Van Dam et al., 2017). In Guinea, for instance, the telecommunications regulator demanded all ISPs to cooperate in order to set up a "center for control and oversight of traffic (voice and data)" (Human Rights Watch, 2016). Three out of four ISPs in Guinea owned by foreign investors (Orange, MTN and Cellcom) responded to the request with a joint letter stating that the request suffered from a "total absence of legal basis" (Micek & Kenyanito, 2016), that it would violate the right to privacy, and decided not to provide the requested data. This example highlights that company decisions can be complex and may depend on owner-specific characteristics that (partially) explain their relationship with the host government.

Second, the extent to which an owner can exercise structural power over a company depends on their number of shares. So-called "block-holders", owning at least 51 percent of a company's stakes "are usually directly involved in firm management [and] do not merely monitor management teams, they lead them" (Holderness & Sheehan, 1988: 314). In companies in which no shareholder holds more than 30 percent of the stakes, control is dispersed and owners have less capacity to influence management decisions (Armstrong, Guay, & Weber, 2010: 210).

In sum, whether or not an authoritarian government has the capacity to manipulate internet access should depend in part on the owners of ISPs operating on its territory. In Study 2, we provide a detailed conceptualisation of ISP ownership as an indicator of state-business relations. In Study 4, we empirically demonstrate that state ownership may facilitate a government's capacity to disrupt internet access during authoritarian elections.

1.2.3 Institutional constraints in autocracies

In Benin in 2017, the parliament rejected a draft bill by president Patrice Talon that aimed to abolish the presidential term limits (Adeola, 2017), thereby illustrating the crucial challenges facing authoritarian rulers when power is shared with opposition forces. Indeed, nowadays most authoritarian rulers rely not only on repression but also on co-optation and legitimation for regime survival (Gerschewski, 2013), which are not mutually exclusive but reciprocal (Frantz & Kendall-Taylor, 2014). In this thesis, I acknowledge that an authoritarian government's reliance on repression as well as co-optation of opposition forces shapes their course of action, including their motivation and capacity to maintain control over access to the internet. Setting up internet infrastructure is costly, which is why many countries rely on foreign investment in the telecom sector. Political economists have pointed to the costs of foreign ownership, including a loss of control over the domestic economy (Lecraw, 1977; Freyburg, Garbe, & Wavre, 2021). I therefore expect authoritarian rulers only to grant access to foreign investors, and hence partially give up control over internet access, under the following two conditions: First, an incumbent's reliance on repression and co-optation of the opposition is expected to reduce or enhance their willingness to accept foreign investment in the telecom sector, and hence their ability to control access to the internet. Second, authoritarian rulers relying on repression are more willing to accept investors from like-minded regimes.

First, repression is often regarded as one of the core features of dictatorship (Gerschewski, 2013, 21). In the digital era, ICT provide repressive governments with an informational advantage to identify and localise anti-regime sentiments. Governments may exploit internet infrastructure to identify regime opponents and increase the precision of repression (Xu, 2020), or cut internet access to hide state violence

(Gohdes, 2015b). In order to leverage internet infrastructure for their purposes, repressive governments rely on control over internet access and may be more hesitant to accept foreign investors in this crucial sector. By contrast, many modern autocracies rely on the co-optation of potential rivals through formal institutions such as legislatures or parties (Gandhi, 2008; Gandhi & Lust-Okar, 2009), that can put pressure on the government to provide public goods such as internet access. Therefore, authoritarian rulers who are constrained by opposition forces within formal political institutions, should face increased pressure to accept foreign investment in the telecom sector and (partially) lose control over internet access.

Second, while some authoritarian governments might hesitate to accept foreign investment in internet infrastructure, they might be less sceptical towards investors from like-minded regimes. They seek to maintain authoritarian rule through economic, social, and political collaboration with other autocrats (Weyland, 2017; Schmotz & Tansey, 2018) that are "particularly supportive of their own rule" (von Soest 2015, 629). Therefore, regimes that are concerned about losing control over internet infrastructure, yet face pressure to accept foreign investment, may be more willing to grant access to investors from other autocracies.

In sum, authoritarian rulers rely on different levels of repression and co-optation, which may motivate and constrain them in granting access to foreign investors. Findings from Study 3 suggest that repressive regimes are not less open to foreign investment in the telecom sector *per se*, but selectively grant access to foreign-autocratic investors.

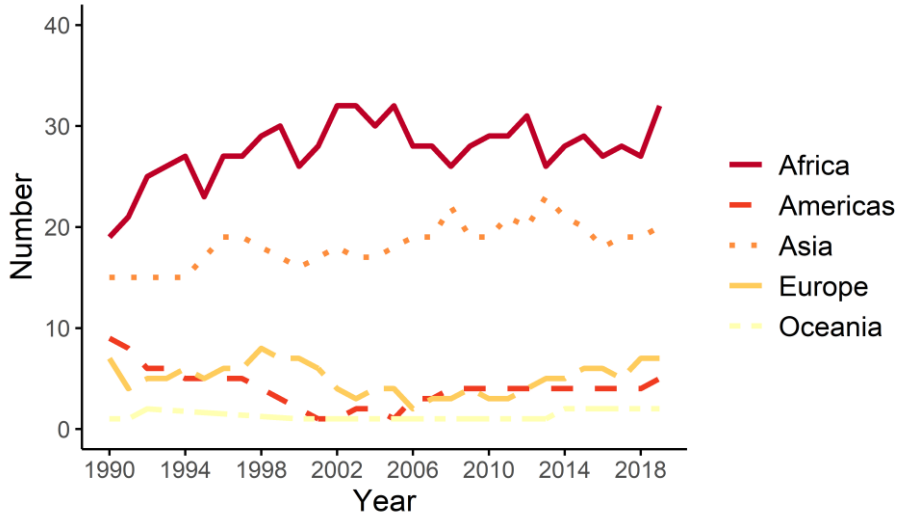
1.3 Methodology

In this thesis, I follow a Weberian understanding of scientific inquiry aiming at the "careful and rigorous application of a set of theories and concepts so as to produce a thoughtful ordering of empirical actuality" (Jackson, 2016: 23). More specifically, I take an explanatory approach (Toshkov, 2016: 35f) to study both the causal mechanisms of how ICT use potentially threatens authoritarian survival, and the causal consequences of ISP ownership for control over internet access. To this end, I combine different quantitative data sources, including observational and survey data, and qualitative data sources, notably expert interviews of politicians and journalists from Uganda. In order to analyse these data, I use large-*N* probabilistic methods such as general linear mixed models (GLMM) and deterministic medium-*N* methods, namely qualitative comparative analysis (QCA). In the following, I provide an overview of the sampling strategy and generalisability. Appendix A3 provides an overview of additional key variables (internet service providers, internet shutdowns, and ownership) and their operationalisation.

1.3.1 Sampling and case selection

In this thesis, I focus predominantly on electoral autocracies, defined as those regimes[3] in which elections for the chief executive are held allowing for minimal party competition, but are not held under free and fair conditions (Schedler, 2006; Levitsky & Way, 2010). This focus excludes regimes where elections are held but no de-facto competition exists, as authoritarian rulers in those countries are less likely to see the use of ICT as a threat to their rule. In electoral autocracies, governments typically create "arenas through which opposition forces may—and frequently do—pose significant challenges" (Levitsky & Way, 2002: 54). In turn, the use of ICT by opposition forces may be considered an additional threat to authoritarian survival. I follow Lührmann, Lindberg and Tannenberg (2017: 1f) in operationalising electoral autocracies as regimes that hold "de-facto multiparty elections for the chief executive, but […] fall short of democratic standards due to significant irregularities, limitations on party competition or other violations of Dahl's institutional requisites for democracies".[4] Figure 2 highlights the prevalence of electoral autocracies in Africa in contrast to other world regions.

Figure 2. Electoral autocracies 1990–2019



Note. Indicates the number of electoral autocracies per continent between 1990 and 2019 (Coppedge *et al.*, 2020b).

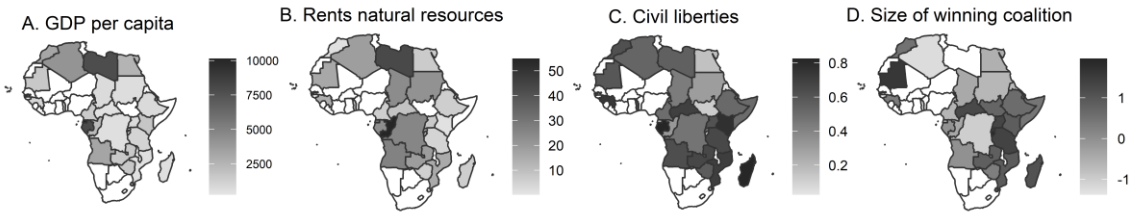
Authoritarian countries in Africa offer great variation in economic and political factors that are likely to drive the motivation and capabilities of governments to control internet access. Figure 3 provides an

[3] Political regimes are the "rules and procedures that determine how national leaders are chosen" (Howard & Roessler, 2006, 366). Thus, regimes can vary in the extent to which rules allow for contestation and participation in selecting a government (ibid.).

[4] To measure regime type, I use a categorical variable (*v2x_regime*) from the Varieties of Democracy (V-Dem) project that relies on coding by country experts (Coppedge *et al.*, 2020b). I chose V-Dem data for two main reasons. First, in comparison to other democracy indices, V-Dem data provide measures of uncertainty to reduce measurement error which has been identified as a problem in other indices (Pemstein, Meserve, & Melton, 2010). Second, in V-Dem, regimes violating political freedoms are more often coded as electoral autocracies than in other indices, underlining its conservative classification (Lührmann, Tannenberg, & Lindberg, 2018).

overview of civil liberties, size of the winning coalition, GDP per capita, and the share of revenues from natural resources in GDP in African autocracies in 2018.

Figure 3. Economic and political indicators in African autocracies, 2018



Note. Indicators for GDP per capita (*API_NY.GDP.PCA*) and revenues from natural resources as percent of GDP (*API_NY.GDP.TOTL.RT*) come from World Bank data (World Bank, 2020b). Civil liberties are captured by an index (*v2x_clpol*) reflecting liberal rights ranging from 0 to 1. The indicator size of the winning coalition (*v2regsupgroupssize*) reflects the share of the population that belongs to the government's winning coalition and ranges from extremely small to large values (Coppedge *et al.*, 2020a). Non-autocracies are left blank.

Politically, African autocracies are marked by varying degrees of illiberalism (Hadenius & Teorell, 2007; Magaloni & Kricheli, 2010; Levitsky & Way, 2010; Resnick & Van de Walle, 2013). This is illustrated by differences in the extent to which civil liberties are violated or repressed and opposition actors are able to effectively contest the ruler. In some authoritarian regimes, like Kenya and Malawi, political institutions such as legislatures have turned into important actors challenging the government, whereas in others, they appear to be mere window dressing (Barkan, 2008). In addition, African governments rely on different forms and degrees of repression to clamp down on civic space (Rudbeck, Mukherjee, & Nelson, 2016).

Economically, a considerable number of African countries are still classified as developing countries (UNDP, 2014). Most of them have recognised investment in ICT as a crucial driver of economic growth and started privatising the telecom market fostered by liberalisation programmes of Western organisations such as the World Bank (e.g. Albiman & Sulong, 2016). Indeed, Africa's mobile technology economy is one of the fastest-growing in the world (Tortora, 2014). The market potential of increasing populations makes the African continent a thriving field for public and private, national and international interests (Rodine-Hardy, 2013). Yet, the extent to which African autocracies have expanded internet access still varies considerably (Nyirenda-Jere & Biru, 2015). This is also reflected in more fundamental economic disparities such as variation in GDP growth and natural resources wealth (Calderon *et al.*, 2019). To date, empirical studies on the determinants and effects of ICT in Africa are scarce due to the difficulty in obtaining reliable data (Emmer & Kunst, 2018).

1.3.2 Generalisability

Several insights with regard to governments' motive and capacity to control internet access should be applicable to authoritarian-developing countries beyond the African context. First, the ways in which ICT can be used to challenge electoral malpractice and authoritarian rule should apply to (developing) autocracies more widely. Internet access, in particular through mobile phones, has become an important tool during elections in developing countries across the world (Baguma & Eilu, 2015), potentially challenging authoritarian survival (Ruijgrok, 2020), and motivating autocrats to exert control over internet access. This knowledge should be particularly relevant given the increase in electoral autocracies and internet use in many developing countries (Maerz *et al.*, 2020; Avgerou, Hayes, & La Rovere, 2016). However, in particular the sub-Saharan African context differs remarkably in terms of internet infrastructure (Myovella, Karacuka, & Haucap, 2020), resulting in very low rates of fixed broadband penetration compared to the rest of the world (see Appendix A4). It remains to be studied how the various ways of connecting to the internet potentially shape how people use ICT to mobilise and challenge authoritarian survival (cf. Burrell, 2010; Oyedemi, 2015).

Second, insights regarding the ways in which state-business relations shape governments' capacity to control internet access should be applicable to other authoritarian regimes. Anecdotal evidence suggests that when governments blocked internet access in countries such as Indonesia or Venezuela, they also benefited from direct state ownership of local ISPs (e.g. Access Now, 2018). This supports the mechanism presented in this thesis on how state-business relations facilitate control over internet access. Moreover, other developing regions in the world, such as Latin America or the Middle East, which also experienced colonial rule, have booming markets with young consumers, and were exposed to major privatisation efforts (Wallsten, 2001; Howard & Mazaheri, 2009), suggesting a similar setting in which ISP-government relations unfold. However, Africa lags far behind OECD, Asian, and Latin American countries in terms of privatisation (Gasmi *et al.*, 2013). Hence, results from this thesis may not be representative of authoritarian governments' capacity to exert control over internet access and use globally.

Third, the ways in which authoritarian institutions shape governments' capacity to maintain control over internet infrastructure by discouraging foreign investment or selectively granting access to foreign-autocratic investors should be applicable to authoritarian regimes more widely. Given the importance of ICT for economic development (Jin & Cho, 2015), authoritarian-developing countries are generally confronted with the problem that maintaining state control over internet access might inhibit economic growth. Several of the foreign-autocratic multinational ISPs providing internet access in Africa, including Ooreedo, Etisalat, or Viettel also invest in internet infrastructure in non-African autocracies, emphasising the potential for authoritarian collaboration in the telecom sector beyond the African context.

1.4 Outlook

This thesis is structured as follows. Chapter 2 presents the case study on Uganda's presidential elections that investigates the ways in which internet access changes the opportunities of local opposition actors and hence threatens authoritarian survival (Study 1). Chapter 3 conceptualises ISP ownership and presents data on ISP ownership in Africa (TOSCO) (Study 2). Chapter 4 uses aggregated ISP ownership data to investigate the conditions under which authoritarian governments grant access to foreign investment in ISPs and, hence, partially give up control over internet access (Study 3). Chapter 5 looks into the consequences of ISP ownership for control over access to ISP by examining the occurrence of internet shutdowns during African elections between 2014 and 2016 (Study 4). Finally, Chapter 6 summarises the main contributions of this thesis and discusses potential avenues for future research.

PULLING THROUGH ELECTIONS BY PULLING THE PLUG: INTERNET DISRUPTIONS AND ELECTORAL VIOLENCE

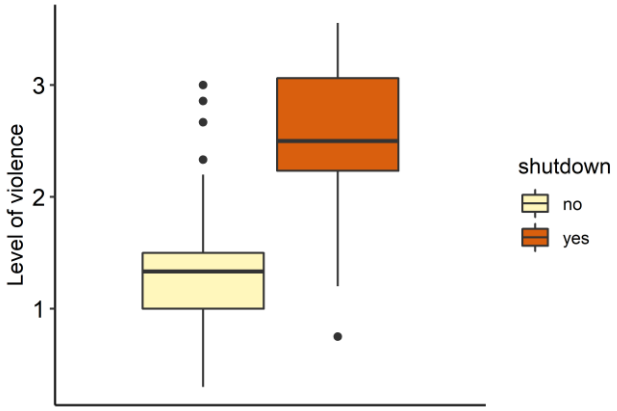
Abstract

This paper examines the role of internet access and its disruption for the conduct of authoritarian elections. I argue that internet access provides both opposition supporters and government authorities with new means to shape electoral conduct. While opposition supporters can use ICT to report on electoral malpractice and mobilise for support, government authorities may use ICT to identify anti-regime sentiment and selectively repress opposition supporters. In consequence, an internet disruption may have a differential impact on opposition and government actors. On the one hand, it may reduce public exposure of state violence. On the other, it might prevent opposition supporters from effectively using ICT to challenge electoral malpractice. Studying Uganda's 2016 presidential elections, evidence from election monitoring and survey data suggests that electoral violence is significantly higher in opposition strongholds with greater internet access prior to the internet disruption. Insights from qualitative interviews with politicians, journalists, and activists, underline that the disruption of internet access indeed hindered opposition supporters to effectively challenge electoral malpractice. Overall, the results point to the important role that ICT can play for opposition actors in authoritarian elections. At the same time, they highlight their susceptibility to manipulation by government authorities.

2.1 Introduction

Does internet use challenge authoritarian elections? The number of African elections during which governments disrupted or manipulated internet access suggests indeed that many African rulers perceive internet use as a threat: Between 2015 and 2018 alone, one-third of all national elections in sub-Saharan Africa (SSA) was accompanied by an internet disruption, with governments either blocking specific websites or curtailing access to entire networks (Freyburg & Garbe, 2018; Rydzak, Karanja, & Opiyo, 2020). At the same time, as shown in Figure 4, levels of electoral violence were significantly higher during those African elections that were accompanied by an internet shutdown[5], even when controlling for relevant factors, including local conflict, internet penetration, and regime type, raising the question whether and how internet use and its disruption affect electoral conduct (see Appendix B1 for results from linear mixed models).

Figure 4. Election violence during African elections 2015-2018



Note: Higher scores indicate higher levels of election violence; horizontal lines show the median. The indicator for election violence committed by state authorities (v2elintim) comes from the Varieties of Democracy project (Coppedge *et al.*, 2020a); data for internet shutdowns from #KeepItOn campaign of the civil society organisation Access Now (Access Now, 2016). *N* = 58.

The role of new information and communication technologies (ICTs) for the conduct of authoritarian-developing elections remains poorly understood (Gagliardone, 2019). Anecdotal evidence, such as from the Ushahidi platform, which crowdsourced data on incidents of violence during multiple African elections, including in Kenya, Burundi, and Sudan, suggests that citizens and opposition actors routinely use ICT to address electoral violence (Okolloh, 2009; Colombo, D'Aoust, & Sterck, 2018; Bunz, 2014). Simultaneously, governments increasingly monitor online discourse to identify anti-regime sentiment (King, Pan, & Roberts, 2013; Qin, Strömberg, & Wu, 2017). Scholars have thoroughly examined the determinants and

[5] I follow Rydzak (2018: 6) in defining an internet disruption as any "intentional, significant disruption of electronic communication within a given area and/or affecting a predetermined group of citizens".

effects of electoral violence offline. But how does internet access, and its disruption, affect electoral violence?

Recent work in political communication (Bennett & Segerberg, 2013; Bimber, 2017; Mare, 2016; Karekwaivanane, 2019) suggests that the use of ICT helps opposition supporters address traditional challenges in mobilising support (McCarthy & Zald, 1977; Kuran, 1989). Particularly in developing countries, mobile phones can undermine electoral malpractice by enabling the opposition to expose violence or fraud and to monitor election results in real-time (Baguma & Eilu, 2015). In turn, and for the same reasons, authoritarian governments are likely to manipulate or suppress online communication during contested elections. As indicated by literature on digital repression, ICT likely help governments localise opposition actors and selectively repress regime opponents during periods of internet disruptions (Xu, 2020; Gohdes, 2020). Given that a growing number of people rely on ICT to access information, communicate, and mobilise at election times (Karekwaivanane, 2019), it is plausible to expect a disruption of ICT access to have profound consequences for the conduct of elections, resulting in increased electoral violence.

In the next section, I review the literature on electoral violence, followed by a theoretical argument on how access to and disruption of internet services affect the occurrence of electoral violence. Subsequently, I introduce and discuss Uganda's 2016 presidential elections as a case study and present statistics drawn from original survey data (N = 2042) and election monitoring data from polling stations (N = 895) across Ugandan constituencies. The results indicate that electoral violence is higher in those constituencies with more opposition support and higher internet access. The findings are contextualised by 25 semi-structured face-to-face interviews with journalists, citizen activists, and politicians from three opposition-leaning Ugandan districts, as well as evidence from major Ugandan news outlets. The qualitative insights help to understand the potential consequences of the internet disruption for opposition supporters' ability to address electoral violence. The last section summarises the findings and discusses the differential impact of an internet disruption on opposition and government actors.

Overall, my findings suggest that internet disruptions can affect the occurrence of electoral violence. While a disruption prevents opposition supporters from effectively using ICT to challenge electoral malpractice, at the same time, it may obscure the use of violent state repression. My study thus highlights the importance of disentangling the ways in which ICT are used by different actors at election times to better understand the effects of internet access and its disruption on core democratic processes.

2.2 Electoral violence in authoritarian regimes

Today, most countries in the world, whether democratic or not, hold regular elections. Authoritarian rulers may have different motivations for holding elections, including the co-optation of elites (Boix & Svolik,

2013), party members (Magaloni, 2008), and broader groups in society (Gandhi & Przeworski, 2006); or to strengthen the regime's legitimacy (Waterbury, 1999), identify bases of support and opposition (Gandhi & Lust-Okar, 2009) and foster long-term regime stabilisation (Knutsen, Nygård, & Wig, 2017). In any case, however, the incumbent ruler needs to ensure that the election result does not threaten their rule. Cheeseman and Klaas (2018: 5) thus argue that "the art of retaining power has become the art of electoral manipulation".

Electoral violence, defined as "events in which incumbent leaders and ruling party agents employ or threaten violence against the political opposition or potential voters before, during or after elections" (Hafner-Burton, Hyde, & Jablonski, 2014: 150), can be seen as the most coercive form of electoral malpractice (van Ham & Lindberg, 2015).[6] Between 2012 and 2016, a quarter of all elections worldwide and more than one-third of SSA elections involved severe violence (Cheeseman & Klaas, 2018, 95f). In Nigeria, for instance, on polling day in 2007, opposition candidates were harassed or arrested by police forces, and around 300 people were killed in election-related violence (Bratton, 2008).

One of the main aims of electoral violence and intimidation is to demobilise potential non-supporters and prevent them from casting their vote (Höglund, 2009; Bratton, 2008). As such, electoral violence is usually targeted at areas with strong opposition and well-informed voters (Rauschenbach & Paula, 2019; von Borzyskowski & Kuhn, 2020; Bhasin & Gandhi, 2013).[7] Electoral violence can therefore have far-reaching consequences not only for the electoral process but also for election results.

In response to electoral violence, citizens may engage in collective action (Tucker, 2007), especially when they know that others are too (Bratton, 2008). However, these backlashes rarely occur in electoral autocracies, where individuals have little incentives to risk political engagement (Tucker, 2007). By enabling new forms of communicating and sharing information, the increasing availability of internet services may help "solve collective action problems that have long bedeviled those traditionally shut out of mainstream politics" (Tucker *et al.*, 2017: 47). For example, prior research shows that social media use shapes peoples' perception of electoral malpractice (Reuter & Szakonyi, 2013), which may influence their decision to engage in counter-mobilisation. However, we still know little about the effects of internet access, and specifically its disruption, on electoral violence. I seek to contribute to the literature on the targeting of electoral violence by addressing the following question: *How does access to internet services and its disruption affect the occurrence of electoral violence?*

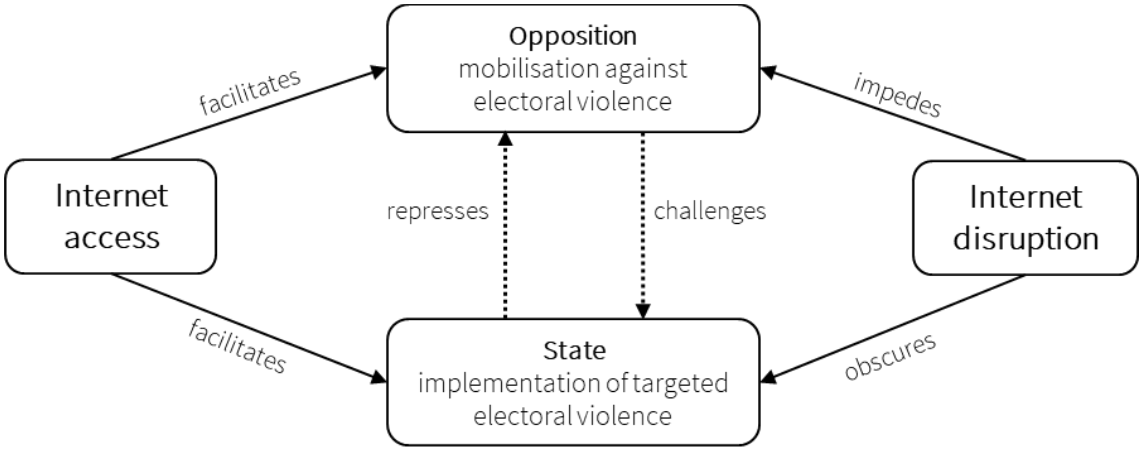
[6] Höglund (2010) argues that electoral violence differs from political violence due to its different motives and hence needs to be studied as a phenomenon in itself.

[7] Therefore, electoral violence decreases with electoral support (Collier & Vicente, 2012; Chaturvedi, 2005).

2.3 Theory

Since the early days of the internet, scholars are interested in the conditions under which internet access may bolster or challenge authoritarian rule studying the effect of internet penetration on authoritarian survival, protest behaviour, or state repression (Rød & Weidmann, 2015; Ruijgrok, 2017, 2020; Xu, 2020; Gohdes, 2015b; Deibert *et al.*, 2008). I borrow from recent insights in political communication to define the ways in which internet access, and its disruption, can affect electoral violence, as summarised in Figure 5. First, I systematically discuss the potential of *internet access* for state actors to commit electoral violence and opposition supporters to challenge it. Second, I argue that a *disruption of internet access* limits opposition supporters' ability to address electoral violence while, at the same time, it allows state actors to obscure their use of electoral violence.

Figure 5. Theoretical argument



2.3.1 Committing and preventing targeted violence: The role of internet access

For opposition supporters, internet access may help to address electoral violence. On the one hand, internet access encourages individuals under authoritarian rule to reveal their true preferences and, by providing information about the opposition's strength, to encourage protest against electoral violence. On the other, once people decide to engage in mobilisation, ICT use substantially facilitates the organisation of their efforts. According to social movement theory, to become active in anti-regime mobilisation, citizens need to have a sense of the extent to which their grievances are shared with others (Gurr, 2015; Turner & Killian, 1957). Applied to the context of elections, voters are more likely to challenge electoral malpractice if they know that others are too (Bratton, 2008). However, opposition elites and their supporters in authoritarian regimes are often confronted with the problem of "preference falsification" (Kuran, 1989): Even if they secretly favour the opposition, citizens may deny their preferences in public due to the threat of punishment and uncertainty about broader public opinion. So-called "islands of separateness"

(Friedrich & Brzezinski, 1963: 279ff)—places in which people express and mobilise for their anti-regime opinions–are therefore scarce. In the context of elections, citizens may lack information about the extent to which others share their disapproval of the regime and, hence, may be reluctant to engage in mobilisation challenging election malpractice. The alleged anonymity on the internet can encourage individuals to share their 'true' preferences (Farrell, 2012), especially in places where the public sphere is heavily restricted (Chen *et al.*, 2016). For instance, in Zimbabwe, the Facebook site run by anonymous blogger Baba Jukwa provided a crucial space for critical voices ahead of the elections in 2013 and had a significant impact on the mobilisation of voters (Karekwaivanane, 2019; Mare, 2016).

Moreover, internet access makes it easier for protesters to communicate and organise without the existence of formal organisations (Bennett & Segerberg, 2013; cf. Bimber, 2017). Citizens typically face a constraint of resources needed to successfully organise mobilisation, such as money, time, and knowledge (McCarthy & Zald, 1977).[8] Internet access reduces the costs of sharing information and makes formal organisational structures obsolete (Bennett & Segerberg, 2013; Castells, 2015). In particular social networking sites provide a platform "for debate and knowledge-sharing while also enabling a message to reach its targeted audience in unprecedented fashion, within seconds" (Mutsvairo, 2016: 6). They can be used nation-wide, such as Twitter for mobilisation during Nigeria's elections (Bartlett *et al.*, 2015), or in specific local contexts, such as WhatsApp groups ahead of county elections in Kenya (Omanga, 2019). Baguma and Eilu (2015) argue that, in developing countries, particularly mobile (smart) phones provide individuals with an efficient tool for monitoring electoral malpractice.[9] Importantly, mobilisation taking place online can also spill over to offline engagement (Chibita, 2016). Pictures and other pieces of information can instantly be shared with broader networks, documenting incidences of violence and enabling opposition actors to send assistance to affected polling stations. During several African elections, citizens used online platforms to report on violence during elections and thereby "enable stakeholders at the local level to prevent or evade conflict" (Mutahi & Kimari, 2017: 20; cf. Bartlett *et al.*, 2015).

For state authorities, internet access may help target electoral violence at specific opposition actors. Authoritarian rulers are affected by the problem of preference falsification, too, facing uncertainty as to which parts of the population may threaten regime survival (Boix & Svolik, 2013). Many authoritarian governments use formal and informal institutions to co-opt members of society and thereby alleviate monitoring problems (Gandhi, 2008; Gerschewski, 2013).

[8] These resources may also provide novel opportunity structures for mobilisation (Meyer, 2004; Meyer & Staggenborg, 1996).

[9] Several case studies suggest that opposition actors use online communication to mobilise for protest or other anti-regime efforts outside election contexts (e.g. Eltantawy & Wiest, 2011; Tufekci & Wilson, 2012).

However, co-optation becomes expensive with the increasing size of the so-called "winning coalition", which is the part of society on whose support the government relies (Bueno De Mesquita *et al.*, 2003). Instead, it can be more efficient to use targeted repression as "the cost to buy support from radicals can be significantly higher than that to imprison them" (Xu, 2020: 4). Internet access has equipped governments with new tools to monitor regime dissent and forestall mobilisation efforts by opposition actors. King, Pan and Roberts (2013) argue that governments use information from online communication to learn about and localise anti-regime efforts (cf. Qin, Strömberg, & Wu, 2017). While originally applied to government behaviour in China, studying online discourse may prove particularly useful to governments in electoral autocracies, as elections present a key moment of political uncertainty in which mobilisation may threaten a regime's survival. However, as described above, when government authorities commit electoral violence, they face the risk of countermeasures precisely in those areas in which opposition supporters have access to internet technologies and hence the ability to document and mobilise against violent behaviour. In consequence, governments may disrupt internet access to facilitate the use of electoral violence.

2.3.2 Deterring mobilisation and hiding violence: The role of internet disruptions

In recent years, authoritarian governments frequently disrupted access to the internet, often during elections (Marchant & Stremlau, 2020; Freyburg & Garbe, 2018).[10] Those disruptions occur in relatively well-connected countries like Iran (Newman, 2019) but also happen in countries like Mauritania where less than a fifth of the population is connected to the internet (Dahir, 2019). Internet disruptions may affect the occurrence of electoral violence in two ways. First, the discontinuation of internet access prevents opposition supporters from effectively using internet access to address electoral violence. Second, and in turn, government authorities can commit violence without facing public exposure and risking their legitimacy.

Given that *opposition actors* in well-connected areas determine their course of action under the condition of access to internet services, its disruption may have severe consequences for their effective response to electoral violence. Specifically, it may paralyse the communication of critical incidents at polling stations and the mobilisation among opposition supporters, thus hindering opposition actors from preventing electoral violence. It is already difficult to effectively mobilise offline due to resources constraints and a lack of information about the number of complicit fellow citizens. However, it is presumably even more difficult to revert to offline mobilisation on short notice when people relied on internet access for their

[10] Freyburg, Garbe and Wavre (2021) argue that governments cannot simply manipulate internet access but rely on the companies providing internet access on their territory. Freyburg and Garbe (2018) demonstrate that governments directly owning stakes internet service providers, have a higher capacity to disrupt internet access.

mobilisation strategies but face an internet disruption.[11] People may eventually develop alternative means of connecting to the internet during long-term internet restrictions.[12] Yet, establishing alternative forms of mobilisation takes time and resources that might not be available, at least not on short notice on the polling day itself.

Governments, in turn, have better chances to commit violence without risking denunciation of their actions if internet access is disrupted during elections. In particular, they can commit targeted acts of state violence without risking unfavourable consequences of ICT use by the opposition (Gohdes, 2015a; Kasm, 2018). Assuming that governments frequently monitor online behaviour to forestall where anti-regime mobilisation is likely to occur, they may implement short-time disruptions of internet access to prevent people from monitoring their actions and hence obscure the use of state violence. By banning access to widely used online platforms, governments hinder the opposition from documenting state violence and effectively challenging their use of coercive force.

Overall, existing literature suggests that access to the internet encourages opposition supporters in authoritarian-developing regimes to participate in mobilisation online and substantially facilitates the organisation of mobilisation offline. These insights are supported by original evidence from Uganda indicating that opposition supporters are more likely use ICT to mobilise voters and report on electoral malpractice.[13] Yet, in many developing, and especially African countries, internet access is still scarce and subject to intra-country variation (ITU, 2021; Vimalkumar, Singh, & Sharma, 2020). Therefore, the extent to which citizens use internet access to monitor and respond to electoral violence should vary depending on how well-connected their geographic area is. That is, opposition supporters who live in highly connected areas should be more likely to use internet access for mobilisation during elections than those in less well-connected areas. In consequence, opposition supporters in well-connected areas are also more likely to be affected by electoral violence. Similarly, if governments strategically use information from internet activity to identify and ultimately repress regime opponents, we should expect electoral violence

[11] In this regard, they likely differ from citizens in less well-connected areas who, in the absence of internet access, are prepared to use analogue forms of addressing electoral malpractice such as mobile telephony (Cheeseman, 2008), local radio stations (Ayittey, 2011), or setting up physical networks of opposition supporters (ACE, 2020).

[12] During Cameroon's shutdown in 2017 targeting the Anglophone region, Cameroonians set up so-called "internet refugee camps" close to the borders where people could get internet access from neighbouring regions (Ritzen, 2018).

[13] The survey data collected for the purpose of this study (see methods section) suggests that opposition supporters are more likely to use ICT to challenge electoral malpractice and mobilise voters than citizens who do not support any of the opposition parties during Uganda's 2016 presidential elections. Respondents supporting opposition parties declared a higher propensity to use social media to report election malpractice and to communicate their participation in the elections, even when accounting for the influence of several individual characteristics and including constituency random intercepts (see Appendix B2 for regression tables).

to be higher in areas where opposition supporters have greater internet connectivity. Therefore, I expect that:

> *If internet access is disrupted, levels of electoral violence will be higher in areas with increasing opposition support and internet access.*

2.4 The Case of Uganda's 2016 presidential elections

Uganda's presidential elections in 2016 were the third multiparty elections since the National Resistance Movement (NRM) and Yoweri Museveni took power in 1986. With a reform in 2005, the government established a multiparty system and thus allowed for (minimal) party competition. Even though previous elections were not held under free and fair conditions (Levitsky & Way, 2010; Schedler, 2006), the opposition was a credible challenger to incumbent ruler Museveni. According to opinion polls before the 2016 elections, the opposition party Forum for Democratic Change' (FDC) popularity peaked (Beardsworth, 2016). Consequently, the re-election of the incumbent president was more contested than during any of the previous elections.

In the years before the election, the internet had become an important "tool for social, economic, and human rights development in Uganda" (CIPESA, 2016). Due to increased connectivity, especially through mobile phones, it also provided individuals with new means to participate in politics (Grönlund & Wakabi, 2015; Grossman, Humphreys, & Sacramone-Lutz, 2014). Especially for opposition campaigners, social media appeared to be an important tool ahead of the 2016 elections as, following the Public Order Management Act, anyone holding a public meeting or rally needed to inform the police, which "ha[d] always restricted members of the opposition from making public consultations with citizens" (Enenu, 2016). Furthermore, the use of social media for real-time reporting became pressing due to violence during election campaigns, "especially against opposition candidates" (Ssekika, 2016), in particular after the police was equipped with new anti-riot gear. This act was said "to intimidate opponents of President Yoweri Museveni" (Biryabarema, 2016). For opposition parties, social media thus represented a "crucial" channel to communicate and share information (*Presidential, parliamentary elections in embarrassing mess*, 2016).

A few days ahead of the 2016 elections, the Electoral Commission (EC) announced the ban of smartphones at polling stations (Karugaba, 2016; Musisi, 2016). This ban was regarded as a strategic move to "limit information flows" (Musisi, 2016). In response to the smartphone ban, opposition candidate Amama Mbabazi publicly encouraged all voters to ignore the ban and "go with their phones and cameras, and feel free to record anything they think is going wrong" (as cited in Kaaya, 2016). There was already a restriction of communication during the previous presidential elections in 2011, at a time when access to the internet was still relatively low. Back then, the government had ordered telecom operators

to ban specific keywords on SMS, including "Egypt", "bullet", and "people power" (Biryaberema, 2011). It appears as if the government's announcement of banning smartphones (rather than impairing their pro-opposition use) and previous experience with rather old-fashioned censorship may have provided opposition supporters with a false sense of security. The disruption of social media on polling day was indeed the first time that internet access was restricted nation-wide at a large scale (Kembabazi, 2016). This is supported by media coverage in major Ugandan news outlets, none of which mentioned an internet disruption in the months ahead of the election.[14]

Uganda's 2016 presidential elections provide an 'easy' case (Seawright & Gerring, 2008) to better understand ICT use and digital repression at election times for three main reasons: First, most internet disruptions on election day take place in electoral autocracies, such as Uganda (Letsa, 2019)—that is, regimes that allow for minimum multiparty competition without granting free and fair de-facto multiparty elections (Lührmann, Lindberg, & Tannenberg, 2017). Second, Uganda ranks among the third of countries with the highest levels of electoral violence[15] and irregularities (see Appendix B3); therefore, it represents a group of SSA countries notoriously affected by electoral malpractice. Third, regarding digitalisation, Uganda is representative of many SSA countries, where mobile internet connectivity substantially increased since 2014, with more than one-third of the country's population online (Bahia & Suardi, 2019).

2.5 Research design

2.5.1 Empirical strategy

I apply a cross-sectional research design to examine internet use and electoral violence across constituencies during Uganda's 2016 elections combining survey with election monitoring data. I estimate the influence of the interaction between the proportion of opposition supporters and internet access on electoral violence. Specifically, I analyse how local internet access and the proportion of opposition supporters influence the likelihood of electoral violence in a sample of 195 polling stations across 70 constituencies.

[14] I systematically searched articles from major newspapers in Uganda using the information research tool Factiva (keywords: "internet shutdown OR internet outage OR internet blackout OR social media blocking OR social media shutdown OR social media blackout"; newspapers: New Vision, Daily Monitor, The Red Pepper, The East African, East African Business Week, The Observer; date: 01.01.2016-07.02.2016). The search resulted in 0 articles.

[15] During the 2016 elections, electoral violence was "most visibl[e] as repeated harassment and arrests of opposition politicians and supporters" (Sjögren, 2018: 57).

I use generalised linear mixed models (GLMMs; Bates et al., 2015) and pairwise model comparisons comparing the model with the predictor of interest to a reduced model including main effects only.[16] To rule out collinearity, I determine Variance Inflation Factors (VIF, Field, 2009) for a standard linear model excluding the random effect (all VIFs < 2). Descriptive statistics for all variables included in the analyses are provided in Table 2.

To contextualise the findings, I interviewed 25 opposition and government politicians, activists, and journalists in three electoral districts—Kampala, Gulu, and Kitgum—in October and November 2018 (see Appendix B5). Those districts tend to be opposition-leaning but vary with regards to their internet coverage from high (Kampala) to intermediate (Gulu) and low (Kitgum) connectivity (GSMA Intelligence, 2019). Besides, I use information from media reports of major news outlets in Uganda, including the Daily Monitor, New Vision, and The Observer, two weeks before and after the elections.[17]

Table 2. Descriptive statistics

Variable	Min-Max	M (SD)	N
Polling station level			
violence (t1)	0-1	0.31 (0.46)	887
violence (t2)	0-1	0.33 (0.47)	887
share of opposition votes 2011 (in %)	0-0.9	0.32 (0-0.19)	649
Constituency level			
opposition support	0-0.55	0.23 (0.14)	82
internet access	0-0.67	0.27 (0.16)	82
economic status	0-0.82	0.16 (0.14)	82
education	1.31-4.69	2.5 (0.65)	82
share of urban voters (in %)	0-1	0.41 (0.42)	82

Note: M = mean; *SD* = standard deviation; t1 = violence during polling; t2 = violence during vote counting.

2.5.2 Independent variable: Opposition strength and access to internet

For internet connectivity and opposition strength, I aggregate original data from a regionally representative survey conducted in April 2019 by the research institute Research World International LTD (see Appendix B6) covering 2'042 respondents across 82 constituencies in Uganda. The survey, conducted three years after the elections, relies on retrospective self-reporting that might be subject to memory bias,

[16] Visual inspection of the distribution of all best linear unbiased predictors (BLUPS) suggests no violation of the assumption of gaussian distribution (see Appendix B4). I further assess model stability for all models by comparing the estimates obtained from a model based on all data with those obtained from models with the levels of the random effects excluded one at a time (Nieuwenhuis, Te Grotenhuis, & Pelzer, 2012). The models remain fairly stable with regard to the variables of interest.

[17] I systematically selected articles from major newspapers in Uganda using the information research tool Factiva (keywords: "elections AND internet OR ICT OR social media OR mobile OR phones"; newspapers: New Vision, Daily Monitor, The Red Pepper, The East African, East African Business Week, The Observer; date: 03.02.2016-05.03.2016). The search resulted in 185 articles.

among other possible bias (Stone *et al.*, 2007, 12). Reliability assessments using data from the Afrobarometer and the World Bank suggest minimal bias (see Appendix B7).[18]

The first key independent variable 'opposition support' is based on party preferences ahead of the 2016 elections. Data was coded binomially, with support for the ruling party NRM or support for no specific party (coded with 0) and support for any opposition parties (coded with 1).[19] The second key independent variable 'internet connectivity' assesses whether people had internet access before the 2016 elections (access coded with 1 versus no access coded with 0). I calculate the proportion of individuals with internet access and opposition support, respectively, per constituency. In the analysis, I include the interaction term of opposition support and internet access.

2.5.3 Dependent variables: Internet use & electoral violence

'Electoral violence' is operationalised with four indicators based on items from election monitoring data collected by the Citizen's Elections Observers Network-Uganda (CEON-U), a consortium of 18 civil society organisations funded by the Democratic Governance Facility (DGF) and the National Democratic Institute (NDI). CEON-U trained more than 1'000 election observers who collected data at a sample of around 900 randomly chosen polling stations in 285 constituencies during Uganda's 2016 elections on polling day. The observers recorded their observations on standardised checklists containing 50 questions. For electoral violence, the checklist contains two questions capturing the presence of violence ("Were there any incidents of intimidation, harassment or violence against any of the following? (election officials, party agents, observers, voters)") as well as the presence of unauthorised groups (e.g., police, military, or crime preventers) at polling stations. Observers answered these questions *during the polling process* (t1) and *vote counting* (t2) on the same day. For each point of measurement, I combine these two indicators into one variable for violence (with the presence of any form of violence or intimidation at a polling station = 1).

2.5.4 Controls

I account for four additional factors that might be systematically related to the level of violence. First, I include the constituencies' mean level of education, which is expected to be positively related to the likelihood of vote-buying and intimidation (Bratton, 2008). Education is measured on a scale from 0 (no formal schooling) to 8 (Doctorate). Second, I include the constituencies' mean socio-economic levels as

[18] I compared the survey data with 2015 Afrobarometer data for opposition support and internet access and with the 2015 World Bank indicators for education, respectively. Data on internet access ($r(40) = .56$, $p < .001$) and opposition support ($r(40) = .42$, $p < .001$) are significantly correlated with the Afrobarometer data; there is no significant difference in education between the two datasets ($z = 0.881$, $p = .378$).

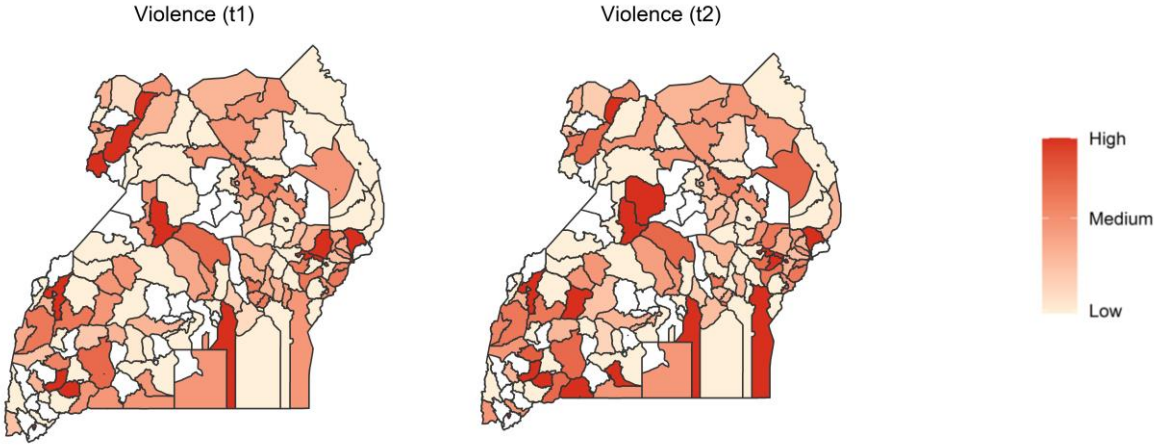
19 To be conservative, I focus on opposition supporters versus government supporters and non-partisan citizens as African countries are characterised by low partisan attachment to a political party (Kuenzi & Lambright, 2011: 779).

previous studies suggest that less resourceful people are more prone to engage in political violence (Arriola & Johnson, 2012). The socio-economic level is measured on a scale from 0 (low income) to 2 (high income). Third, I include the share of respondents located in urban constituencies as electoral violence might be more prevalent in rural areas where state agencies face less risk of exposure (Gonzalez-Ocantos *et al.*, 2019). Fourth, I include the share of opposition votes from the preceding presidential elections in 2011 per polling station as the government might strategically use this information to target expected opposition strongholds.[20] Finally, I include constituency as random intercept to account for within-constituency effects that might occur due to varying ethnic and political legacies, among others (Stegmueller, 2011).

2.6 Results

Evidence from the election monitoring data underlines the variation in electoral violence across constituencies. Figure 6 indicates that violence *during polling* (t1) and *vote counting* (t2) were not equally present across the country. Several places with a high number of polling stations affected by violent incidences *during polling*, such as Chua or Chekwii, remained free from (observed) violence *during vote counting*. Overall, the mean share of polling stations affected by violence during polling per constituency ($M = 0.33$, $SD = 0.34$) was similarly high as the mean share of polling stations affected by violence during vote counting ($M = 0.34$, $SD = 0.35$).

Figure 6. Electoral violence in Uganda, 2016



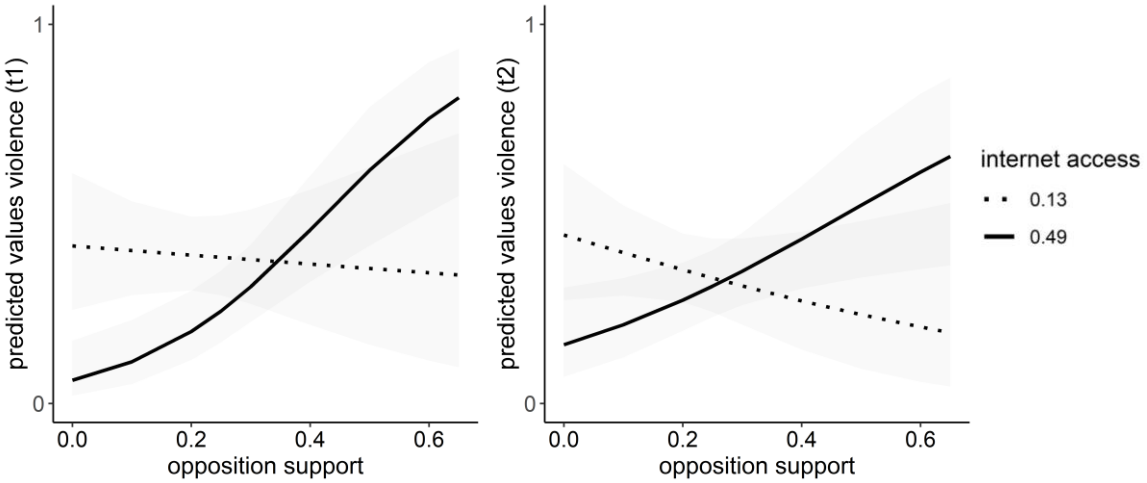
Note: Levels of violence at county-level. Data for county boundaries comes from the (Humanitarian Data Exchange, 2018). Counties with missing values are shaded in grey.[21] Levels of violence were assessed during polling (t1) and vote counting (t2) on polling day.

[20] Data comes from the Electoral Commission in Uganda and is publicly available online: https://www.ec.or.ug/2011-general-election (19.02.2021).

[21] The Ugandan Bureau of Statistics originally provides data. The shapefiles provide data for county boundaries in 2006. Due to the frequent changes in administrative boundaries in Uganda (Grossman & Lewis, 2014), some areas may appear in grey even though data election monitoring data is available.

Results from the GLMMs indicate that electoral violence is higher in areas with increasing internet access and increasing opposition support (see Figure 7). For both violence *during the polling process* ($\chi^2(1) = 6.27$, $p = .01$) and *during vote counting* ($\chi^2(1) = 4.39$, $p = .04$), the model comparisons reveal a significant effect of the interaction between the proportion of opposition supporters and internet access (see Appendix B8). That is, the occurrence of violence at a polling station depends on the interplay of opposition supporters and internet access in the respective constituency. To assess whether these findings are driven by dynamics in Uganda's most populated district, I exclude observations from the capital Kampala (n =32). For both time periods (i.e., violence during polling and vote counting), the effects remain significant (see Appendix B9).

Figure 7. Marginal effects of opposition support on violence conditioned by internet access



Note: Marginal effects at the mean, i.e. with all control variables in the model held constant, with 90 per cent confidence intervals. The predicted values are grouped for internet access one standard deviation below (= 0.13) and above (= 0.49) the mean (= 0.31).

2.7 Understanding the impact of the internet disruption

Interviews with politicians, activists, and journalists emphasise the potential of ICT use to address electoral malpractice, yet also highlight how an internet disruption hinders the opposition to realise this potential. In particular, insights from the interviews outline: (1) The ways in which the opposition prepared for the elections using social media; (2) suspected repression by government authorities targeted at the opposition; and (3) likely consequences of the internet disruption for the opposition's ability to mobilise against electoral malpractice.

First, social media played a crucial role in mobilising voters and addressing electoral violence for both citizens and opposition parties. An election observer in Kampala stressed that many citizens, due to heavy manipulation of the distribution of ballot papers ahead of the elections, had decided to keep track

of what was going on.[22] As expressed by one civil society member in Kampala, the advantage of social media is their ability to report things "the exact way you see them […] which gets the observation of an electoral process to a whole new level".[23] Furthermore, social media played a crucial role in the opposition's strategy to address electoral malpractice. As indicated by several of my interviewees, the opposition party FDC had trained volunteers intending to install ten people–the Power 10 (P10)–at each polling station in the country (*FDC disregards EC on anti-vote-rigging team*, 2016). Their main aims were to "mobilise people to go and vote, monitor the electoral process and observe the ballot counting process to foil vote-rigging" (Oluka, 2016). A high-level FDC member in Kampala explained that the P10 teams were instructed to use WhatsApp to send pictures of the declaration of results (DR) forms to the FDC's headquarter in Kampala to monitor the tallying process.[24] The aim was to get an independent overview of vote counts from each polling station in the country. The government denounced the P10 teams as "orchestrated by the opposition to rig" (Kakaire, 2016).

Second, several respondents indicated that targeted repression played a role both ahead of the elections and on polling day. A journalist in Kampala outlined that the lines of opposition candidates were routinely intercepted.[25] A local politician in Gulu claimed that opposition candidates were often intimidated via text messages directly sent to their mobile phones and a local politician from Gulu said that his mobile money account was blocked ahead of the elections.[26] Intimidation was also used to prevent mobilisation efforts: A local FDC politician in Kitgum stressed that, ahead of the elections, any gathering or rallies were closely monitored and forbidden by the police.[27] According to an FDC politician in Gulu, the police chased people who were opposition leaning to keep them from voting on polling day.[28]

Third, as outlined by several respondents, the internet disruption on polling day prevented opposition forces from challenging electoral malpractice. According to an independent politician in Gulu,[29] opposition parties could not receive information about critical incidents at polling stations nor provide appropriate support in time. A high-level politician from Kampala underlined the importance of the shutdown to prevent people from mobilising.[30] He noted that in contrast to Egypt, where people rely on established organisational structures offline, "there is no Tahrir Square" in Uganda, making it extremely difficult to

[22] Civil Society Organisation (UG1), 23.10.2018.
[23] Civil Society Organisation (UG23), 6.11.2018.
[24] FDC Politician (UG5), 29.10.2018.
[25] Journalist (UG3), 23.10.2018
[26] Independent Politician (UG6), 29.10.2018; DP Politician (UG17), 2.11.2018.
[27] FDC Politician (UG15), 2.11.2018.
[28] FDC Politician (UG9), 31.10.2018.
[29] Independent Politician (UG6), 29.10.2018.
[30] Independent Politician (UG4), 29.10.2018

mobilise larger groups in the absence of social media. Another opposition politician from Kampala also stressed that especially in opposition strongholds, such as Kampala, Wakiso, or Mukono, polling materials were delivered late, leaving many voters angry and without the opportunity to vote.[31] In those areas, he added, it would have been likely that people had gathered spontaneously if there had been the opportunity to mobilise via social media. On the other hand, in less connected areas in Kitgum, opposition agents used an analogue network of opposition actors moving from one polling station to another calling for remedy if they observed suspicious activities.[32] This account highlights that opposition actors in less connected areas may still prepare themselves to use analogue forms of communication when responding to violence and intimidation at polling stations. Several interviewees further highlighted the shutdown's impact on the opposition party's ability to tally the results independently. Due to the shutdown of the messaging service WhatsApp, the FDC did not manage to tally the results on polling day. Instead, the individual P10 teams deployed at polling stations had to provide hard copies of the DR forms. It ultimately took more than two weeks to gather part of the DR forms for the FDC's own tallying. The delay contributed to preventing the FDC from filing a petition to challenge the results, which needs to be submitted ten days after the election results are declared (*FDC to crack regime arrogance & impunity - Mugisha Muntu*, 2016).

2.8 Discussion and conclusion

Evidence from Uganda is useful to better understand how ICT can shape elections in electoral autocracies in the region: First, ICT can be strategically used by opposition supporters to report on election malpractice in real-time, share information about critical incidents at polling stations, and mobilise for support in cases of emergency. Second, governments may use ICT access to identify opposition strongholds and commit targeted state violence. Finally, a disruption of ICT access on polling day may hinder opposition supporters from effectively responding to electoral malpractice. These insights cannot automatically be applied to other cases. Yet, they provide a fruitful starting point to understand the role of ICT in the context of authoritarian elections in SSA and complement prior research on the timing and targeting of state repression during elections by acknowledging the role of ICT (Bhasin & Gandhi, 2013).

While the statistical analysis indicates that electoral violence is more prevalent in areas, in which opposition supporters usually benefit from (greater) internet access, insights from the qualitative interviews illustrate potential mechanisms. The disruption of social media access appeared to prevent people from mobilising and hindered more strategic monitoring of electoral malpractice, especially in areas in well-

[31] FDC Politician (UG5), 29.10.2018.
[32] FDC Politician (UG15), 2.11.2018.

connected opposition strongholds. This finding suggests that, due to their reliance on internet access, opposition supporters in well-connected areas may be less capable of effectively countering electoral violence than opposition supporters in less connected areas. This finding calls for a more thorough understanding of the extent to which mobilisation online substitutes rather than complements mobilisation offline. Besides, the findings suggest that government authorities strategically use internet access to identify opposition strongholds. The Ugandan government has heavily invested in surveillance gear since 2011, including high-level spyware such as UK product FinFisher "to conduct targeted communications surveillance of political opponents" (Privacy International, 2015: 40). Similar trends can be observed in other sub-Saharan African countries (Sutherland, 2019) and call for a more thorough investigation of digital state repression in the region.

These findings contribute to the growing discussion about mobile technology and its potential for political participation in the Global South (Martin, 2014; Kamau, 2017; Bosch, 2013). Given the diverse opposition landscape in Uganda (Beardsworth, 2016) on the one hand and poor connectivity compared to other SSA countries (Gillwald *et al.*, 2019) on the other, the findings may not be directly applicable to other cases. Yet, similar events in SSA underline the importance of the findings for trends in the region: Burundi's 2020 presidential elections, where access to social media was blocked in the early morning of polling day, were also accompanied by intimidation of voters and polling agents as well as allegations of vote-rigging (Follow, 2020). During Mali's 2018 election, where major social media outlets were blocked, state violence "undoubtedly contributed to the low turnout" (Global Voices, 2018). These trends are particularly worrisome as internet disruptions are often used under the pretence of countering violence (Gohdes, 2016) but may be used as a strategic tool to commit human rights violations (Gohdes, 2015b).

A limitation of this study is a potential selection effect that further studies might explicitly address. Eventually, higher levels of electoral violence might occur in areas with more opposition support and more internet connectivity for different reasons. For instance, due to its information and mobilisation potential, access to ICT may change citizens' "commitment to democratic governance" (Nisbet, Stoycheff, & Pearce, 2012: 245) and increase their subjective perception of self-efficacy (Young, 2020). They might hence be qualitatively different from other opposition supporters, posing a higher threat to regime survival. In consequence, the interaction between the proportion of opposition supporters and people with internet connectivity needs to be interpreted with caution. In addition, this study does not systematically assess the consequences of the shutdown for electoral conduct. Ideally, future analyses allow for a more systematic assessment of an internet disruption's effect, e.g. through a quasi-experimental design comparing electoral malpractice across districts with and without internet disruptions. While internet disruptions, in particular during elections, are usually nation-wide, governments sometimes target specific

regions only (Human Rights Watch, 2020). Besides, little variance in the likelihood for electoral violence can be explained with internet access and opposition support, notably 4 percent for violence during polling and 3 percent for violence during vote counting (Nagelkerke's R Squared). This low rate of explained variance is not surprising given that I use data aggregated to the constituency-level to predict outcomes at the level of polling stations. Future studies may draw on more observations to predict electoral malpractice in aggregated locations, such as districts or constituencies, rather than at the level of polling stations. Empirical studies further demonstrate that observers can reduce the occurrence of violence or fraud at polling stations (Asunka *et al.*, 2017). While any bias in electoral violence could be considered systematic due to an observers-only sample, patterns might differ in a sample of polling stations without election observers. Therefore, to estimate levels of electoral violence across different locations, future studies could complement observer data with citizen or media reports.

Nevertheless, findings from this study highlight the potential of internet access to challenge electoral violence, yet also caution that "it is too soon to celebrate the 'opportunities' created by new media technologies" (Mutsvairo, 2016: 8). Given the increasing trend among African authoritarian governments to disrupt internet access at election times (CIPESA, 2019), the presented study is a crucial first step in carefully evaluating internet use by opposition and government actors and its consequences for electoral conduct. Overall, there remains much to be learned about the role of social media during politically contested times (Zeitzoff, 2017). A growing number of studies examines the effects of internet penetration on democratisation (Rød & Weidmann, 2015), political violence (Pierskalla & Hollenbach, 2013), and protest behaviour (Weidmann & Rød, 2019). Yet, only if we understand how ordinary citizens and political opponents use social media and other forms of ICT in times of political contention, we can interpret the effects of internet coverage, or a lack thereof, in meaningful ways.

TELECOMMUNICATIONS OWNERSHIP AND CONTROL (TOSCO). A NEW DATASET TO EXPLORE THE POLITICAL POWER OF INTERNET BUSINESS IN AFRICA, 2000-2019

Joint work with Tina Freyburg and Véronique Wavre

Revise and resubmit at *Review of International Organizations*[33]

Abstract

The internet is built on a physical infrastructure owned by a variety of state and private actors, foreign and domestic, with multiple interests. This paper presents TOSCO, a new dataset on ownership of internet service providers (ISPs) that allows for comparative large-*N* analysis of the determinants and effects of varying ownership structures and identities in the transforming context of African countries from 2000 to 2019. Building on a detailed discussion of the conceptualisation and operationalisation of ownership as a variable, we demonstrate its usefulness with descriptive statistics and regression analyses using replication data from previous research on the internet's democratising effects. Our results suggest that ISP ownership is statistically significantly linked to change in a regime's democratic quality, with state ownership being negatively associated. TOSCO is useful to scholars and practitioners working on the determinants and effects of the provision, use and control of internet services in Africa, and beyond.

[33] Submitted in May 2021

3.1 Introduction

Both the scientific and the public sphere remain fascinated by two apparent contradictory trends: 'The internet'—familiar shorthand for information and communication technologies (ICT)—enabling repressive regimes to impose further restrictions on civil liberties (e.g. Gohdes, 2015b; King, Pan, & Roberts, 2013; Lutscher *et al.*, 2020; Rød & Weidmann, 2015); versus ICT facilitating anti-government movements and enabling democratic change (Acemoglu & Robinson, 2000; Alozie, Akpan-Obong, & Foster, 2011; Freund & Weinhold, 2002; Howard & Mazaheri, 2009; Vu, 2011). Yet, the debate has advanced beyond the simple question of whether the internet is a tool of liberation or one of surveillance and propaganda (Deibert & Rohozinski, 2010; Deibert *et al.*, 2008). The scientific community is now developing theory and collecting empirical data that attest to the circumstances under which ICT can empower opposition forces or the incumbent ruler (Keremoğlu & Weidmann, 2020). The question of who determines who gets access to what internet services is essential in this debate.

Indeed, most accounts recognise that internet services are no resource that governments have necessarily and automatically control over. They acknowledge that the incumbent mostly relies on the internet-providing telecommunications companies to delay, prevent or manipulate the access to internet services since it is they who control the gateway through which all digital information and communication must pass (DeNardis, 2014: 11; cf. Goldsmith & Wu, 2006: 73). Milner (2006: 185), for instance, refers to China as an example in which internet service providers (ISPs) are "force[d] […] to monitor the Web for" the government. Interconnected across the globe via copper cables, fibre optic cables, or radio waves, the small local networks of computers on which the internet relies belong to various ISPs that enable 'last-mile'-connections to end-users. With ISPs there hence exists an industry-wide capacity to grant and restrict access to manifold internet-based services on which an increasingly digitised economy and society relies. The potential for using this capacity may depend on the nature of those who own ISPs.

The key theoretical problem with existing accounts of the determinants and effects of internet penetration lies in the implicit assumption that the incumbent government can make any internet-providing company comply with its requests. However, and as Vendil Pallin's (2017) case study on Russia discloses, a government's leverage over ISPs depends on its relationship with the owner of these companies. The challenges and risks a government faces when seeking to extend its repressive control to foreign-owned companies differ from those associated with companies either owned by the state or by someone close to the incumbent (Freyburg & Garbe, 2018).

Yet, the cross-sectional, time-series data at company-level needed to systematically explore these and other questions is, to date, largely missing. The "extremely difficult and tedious" (cf. Schneider, Fink, &

Tenbücken, 2005: 706; La Porta, Lopez-De-Silanes, & Shleifer, 1999: 474) compilation of such historical and detailed data may be one reason why political scientists tend to treat the internet as a 'black box', largely neglecting its inner working and corresponding conditions of ownership and control (Wilson, 2015). With this paper, we introduce the first large-scale dataset on Telecommunications Ownership and Control (TOSCO) to help narrowing this gap.

TOSCO makes in particular three contributions to data in this area. First, it provides detailed disaggregated information about ISP ownership at the level of shareholders that allows tailoring the definition of ownership to the needs of the researcher or practitioner (e.g., foreign shareholders; state ownership). The data also lends itself for networked analyses, enabling to follow the development of specific actors or companies across countries and over time. Second, the detailed coding descriptions that document sources and coding choices allow tracking individual coding decisions and context. Finally, providing the autonomous system (AS) number for each ISP in the dataset, as well as the organisation ID assigned by the internet registry AFRINIC, allows exploring the relationship between ISP ownership and internet activity measured at the level of AS, among other relationships.

We focus on the African continent for predominantly two reasons. First, this region of the world is especially marked by economic and political transitions that we expect to drive cross-national variation in ISP ownership over time (Hadenius & Teorell, 2007; Magaloni & Kricheli, 2010; Levitsky & Way, 2010; Resnick & Van de Walle, 2013; Albiman & Sulong, 2016). A snapshot of 2019 illustrates that TOSCO includes liberal democracies such as Tunisia with de-facto free and fair multiparty elections and other crucial democratic institutions and liberal principles, as well as closed autocracies like Eritrea with no such institutions or principles (cf. Coppedge *et al.*, 2020b); likewise for economic development, the Gross Domestic Product (GDP) per capita is ranging from 8'132 US$ (current) in the Republic of Equatorial Guinea to 261 US$ (current) in Burundi (World Bank, 2020b). In light of this transforming context, TOSCO allows to investigate crucial questions of economic development and authoritarian survival associated with an increasing internet connectivity that are also relevant in other regions of the Global South.

Second, while the diffusion of mobile telecommunications services has made a substantial contribution to economic growth worldwide, the effect is particularly substantial across African countries (Lam & Shiu, 2010: 192). In Africa, like in the Global South in general, countries rely on foreign investment in internet infrastructure if they wanted to foster the stimulating effect of ICT on economic development (Jin & Cho, 2015). In fact, several of the multinational corporations providing internet access in Africa, including Airtel, Etisalat, Ooreedo or Viettel, have subsidiaries in other developing regions as well. Furthermore, the centralisation of Africa's telecommunications sector is typical for countries in the Global South where few ISPs tend to control internet traffic for larger parts of the population (Acharya, Chakravarty, & Gosain,

2017; Main, 2001). Research on the African telecommunications sector may therefore credibly set the stage for cross-regional comparisons.

The careful conceptual framework backing this dataset is an essential first step in mapping and understanding the empirical patterns of the politics involved in internet infrastructure. A better understanding of the determinants and effects of ownership in a politically and economically sensitive sector such as telecommunications is not only a valuable contribution to our knowledge about the impact of internet penetration; it is also crucial for the work of practitioners and policy-makers interested in exploiting the development potential of investment in ICT.

While the compilation of the data is primarily motivated by questions about the link between ownership of telecommunications companies and state control of the internet, TOSCO enables cross-sectional, time-series large-*N* analysis of various economic, social and political determinants and effects of ISP ownership. Questions to be explored may include some of the following: What role do national political and economic factors play in the privatisation of the telecommunications sector? How does the international and transnational integration of markets and polities affect a state's capacity to maintain control of the digital flow of information and communication? And, what difference does telecommunications ownership make in terms of political liberalisation, economic development, and citizens' abilities to use ICT for the purpose of anti-regime protests? TOSCO further allows addressing key issues in a context in which the internet is increasingly used not only for communication and information purposes but also for e-commerce and ICT-based public services such as e-health.

In what follows, we first conceptualise ownership as a variable, before we describe the dataset and present some descriptive patterns. We subsequently demonstrate its usefulness with a regression analysis that is informed by research on the effects of internet provision on a regime's democratic quality (Rød & Weidmann, 2015). In so doing, we show some ways of how our data can be aggregated, indicating the flexibility in using the dataset, and suggest avenues for further research.

3.2 Conceptualising ownership as variable in political science research

Corporate ownership as a variable is gaining prominence in political science research, as our systematic literature review of top political science journals[34] between 1945 and 2019 indicates. Out of the identified

[34] We searched the Web of Science during the timespan from 1945 to 2019 using the search term "TS=(owner* AND (state OR firm OR company)) AND SO=(American Journal of Political Science OR American Political Science Review OR Annual Review of Political Science OR British Journal of Political Science OR European Journal of Political Research OR Political Science and Research Methods OR Journal of Politics OR Political Analysis OR International Organisation OR World Politics OR International Studies

42 articles that deal with ownership as a property of companies, more than 90 percent have been published since the year 2000. The few that deal with the telecommunications sector focus primarily on explaining privatisation and its effects (Durant, Legge, & Moussios, 1998; Jho, 2007; Mariotti *et al.*, 2015; Schneider, Fink, & Tenbücken, 2005).

Remaining studies concentrate on the ownership of media or natural resources. These studies corroborate systematic relationships between owner identities and the outcome of interest. Media reporting on specific events, such as the US Supreme Court rulings or electoral campaigns, has been shown to vary depending on the financial interests of their corporate owners (e.g. Bailard, 2016; Dunaway & Lawrence, 2015; Hughes & Lawson, 2005; Markus & Charnysh, 2017). Wegenast and Schneider's (2017) study of deposits of natural resources in sub-Saharan Africa reveals that state repression as answer to societal dissent is particularly likely if oil fields are majority-owned by international companies (cf. Luong & Weinthal, 2006). While this political science research highlights the relevance of ownership structures, it largely neglects to theorise the (political) power of a company's shareholders.

3.2.1 The power of shareholders

A review of the business literature reveals that a firm's ownership and governance structure is pivotal in determining its corporate strategy. Specifically, a company's shareholders delegate decision-making authority to managers with the expectation that those will decide and act in the shareholders' best interests. Shareholders have the right to elect the members of the board of directors (BoD), to appoint the management team, to approve mergers, and to appropriate a company's residual earnings, among others (Hansmann, 2013: 897). The BoD then is tasked with designing mechanisms that protect shareholder interests and putting those mechanisms into place (Walsh & Seward, 1990). Since the BoD (and the chief executive officer, CEO) are accountable to the shareholders at all times, it is the shareholders that stipulate, albeit indirectly, the strategic decisions of a company (Leech, 2013). Both the identities of a company's owners as well as their concentration, relating to the number of shareholders and their relative shares, are seen as having important implications for a company's corporate strategy, managerial decision-making, and performance (Sur, Gassmann, & Zhang, 2019; Jamali, Safieddine, & Rabbath, 2008; Thomsen & Pedersen, 2000; Shleifer & Vishny, 1997).

Yet, studies of the political power of business have hitherto only "insufficiently appreciated" (Gourevitch & Shinn, 2005: 13) the internal structure of business corporations (cf. Dahl, 1959). Taking the company as

Quarterly OR Governance OR Comparative Political Studies OR Journal of Peace Research OR Journal of Conflict Resolution OR Conflict Management and Peace Research OR Socio-Economic Review OR Review of International Organisations OR Journal of European Public Policy OR European Union Politics OR West European Politics OR Journal of Public Administration Research and Theory OR Political Geography OR Political Communication)".

unit of analysis, they commonly distinguish between an instrumentalist and a structuralist understanding of power (Fuchs, 2005; Culpepper, 2010). The instrumentalist understanding emphasises voluntary actions, such as lobbying and campaign donations, and their potential effect on policy output; the structuralist perspective views business actors as exercising power by threatening or imposing costs for unpopular policy options, due to the dependence of political actors on their investments, service provision, and jobs. We propose that this analytical work on business power can be productively combined with the contemporary power literature in order to capture dynamics associated with varying ownership structures.

Contemporary discussion of political power revolves around Pitkin's (1972: 277) conceptual distinction between the power *over* (i.e. influence) and the power *to* (i.e. capacity; Göhler, 2009: 35). Applying it to the sphere of corporate ownership, we associate the concept of 'power-to' with an instrumentalist understanding of power as a shareholder's ability to achieve a certain goal by defining the firm's corporate strategy (which, in turn, may inform its political impact). What goals are pursued by a shareholder depends on its specific identity. An individual or family with direct links to the incumbent might have a greater ability to influence policy, compared to a foreign private company with no such ties.

'Power-over' resonates with structuralist thinking in acknowledging the means and resources needed for a shareholder to achieve its goals, such as the voting power defined by the number of shares held in a company. Having power-over implies having the ability to reduce the chance of the other shareholders, with potentially conflicting interests, to influence the firm's corporate strategy (and its political impact). This chance depends on the way in which ownership is concentrated or dispersed across different shareholders. The "two faces of power" (Bachrach & Baratz, 1970) are related in that a shareholder's power-over can define the extent to which it may actually be able to use its power-to; yet, in some circumstances a shareholder might be in a position to influence corporate strategies and public policies even if it holds minority shares only, precisely because of the capacities associated with its owner identity. This, however, is in part an empirical rather than a purely conceptual question.

3.2.2 Variations of owner identities: The power to determine corporate decisions

In line with Jensen and Meckling's (1976) agency theory, there is good reason to believe that the agent (i.e. the management) will not always act in the best interests of the principal (i.e. the shareholder). Agency costs may mainly occur when shareholders and management share no identity and hence may pursue different strategic goals. Taking an example from the telecommunications sector, a state government might request the management of an internet-providing company to manipulate its services for political reasons, such as blocking of social media at politically contentious times. While the

management might prefer not to implement decisions associated with loss of revenue, the shareholders' preferences can be expected to depend on their respective owner identity. If the state holds itself shares in the company, the principal is likely to favour compliance with the request, in contrast to a privately owned company committed to corporate social responsibility principles (Freyburg & Garbe, 2018).

Drawing on business studies, we distinguish between four main types of owner identities in our dataset: the state, a single individual or family, a private corporation, and a financial institution (cf. Holderness, 2009; Nofsinger & Sias, 1999; Thomsen & Pedersen, 2000). These ideal-typical shareholder types vary not only in their goals and risk propensities but also differ in their capacity to control the management and thus in their power to achieve the preferred results, as summarised in Table 3 (cf. Strange, 2018: 1235). We assume a shareholder's power to achieve its goals to be higher the more it has control over the management.

Table 3. Properties of owner identities

	State	Individual/Family	Corporation	Financial institution
Goals	political objectives	wealth maximation	profit maximation	asset maximation
Attitudes toward risk	willing	averse	neutral	willing
Control over management	high	high	medium	low

State-owned firms are typically run by bureaucrats equipped with concentrated control rights and objectives dictated by political interests (Tusiime, Nkundabanyanga, & Nkote, 2011: 252; Shleifer & Vishny, 1997).[35] The incumbent government selects the board and top management and can replace them at any time. State-owned firms are not necessarily interested in maximising efficiency or profit but may pursue other, socio-political or even ideological goals such as the protection/discrimination of vulnerable minorities or the creation/maintenance of jobs (Hart, Shleifer, & Vishny, 1997). In that sense, state ownership may have a regulatory function (Thomsen & Pedersen, 2000: 694; Wavre, 2018, 2020), but can also serve to gain electoral votes (Villalonga, 2000). "[N]either exclusively profit driven, nor bound by hard budget constraints" (Cannizzaro & Weiner, 2018: 177), state-owned firms tend to be willing to take more risks as it is the public who ultimately "pays for the losses" (cf. Cuervo-Cazurra *et al.*, 2014; La Porta, Lopez-De-Silanes, & Shleifer, 1999: 476).

For a *single private individual or family* owning shares of a company, the entrepreneur's personality and interests typically define its business interests (Miller, 1987: 693). This is often strengthened by a double role for the individual/family as both owner and manager (Thomsen & Pedersen, 2000: 693) (Thomsen

[35] State governments can own shares of a company either directly (i.e. by the central government itself) or indirectly (i.e. through other state-owned companies like pension funds, national banks, political parties or other state-owned institutions such as the National Petroleum Corporation in Ghana).

and Pedersen 2000:693). The resources brought to the company by the investor are linked to individual-specific concerns, including family values and the protection of capital (Sur, Lvina, & Magnan, 2013: 376; Arregle *et al.*, 2007). Individual/family owners are typically considered as being risk-averse and driving firm strategy to be conservative. They aim at ensuring the survival of the company, with the goal to pass direct control on to later generations (Miller, Le Breton-Miller, & Lester, 2010: 203). Viewing "their images and reputations as inextricably connected to the firms they own [, individuals/families tend to be] unwilling to damage those reputations through irresponsible actions in part of their firms" (Dyer & Whetten, 2006: 797).

Corporate owners are conventional business corporations that pursue traditional economic goals, notably profit maximation, and are interested in firm-specific concerns, such as the generation of capability or the "uninterrupted supply of goods and resources" (Sur, Lvina, & Magnan, 2013: 378). Often, investment decisions by corporations are motivated by strategic objectives such as prospective mergers or branding (Dam & Scholtens, 2012: 236). Telecommunications companies tend to invest in firms related to the telecommunications sector. In consequence, corporate owners commonly have the relevant expertise and know-how that allows them to not only contribute financial resources but to also provide managerial expertise as well as technical and organisational resources (Sur, Lvina, & Magnan, 2013: 379; Douma, George, & Kabir, 2006: 643). The advantages of facilitated knowledge transfer often comes at the cost of "deficient mutual monitoring" (Thomsen & Pedersen, 2000: 694). While corporate owners are portrayed as generally risk-neutral, they are seen as cautious in their investment strategies (Cannizzaro & Weiner, 2018). They do not enter and leave a market rapidly but expand activities following long-term business-plans.

Finally, *financial institutions*, such as mutual funds, hedge funds, or insurance companies, invest in potentially profitable companies to arrive at financial returns in the best interest of their ultimate investors. As "delegated monitors" (Dam & Scholtens, 2012: 236), financial-institutional owners emphasise financial controls over strategic controls (Yan & Zhang, 2009) and rather keep an "arm's-length relationship" (Thomsen & Pedersen, 2000: 693) with the management. Their main goal is less the monitoring of the company's strategies, but rather to safeguard and enhance their financial investment (Sur, Lvina, & Magnan, 2013: 376). As Johnson and Greening (1999) found, in the case of pension fund groups, this can mean that institutional investors are likely to embrace concepts of corporate social responsibility in response to their customers' expectations. While the risk propensity of institutional shareholders depends on the type of institution—e.g., hedge funds search for quick profits while pension funds are interested in long-term outcomes (Boss *et al.*, 2013), each of them is likely to have well-diversified portfolios. If an institutional investor is dissatisfied with a company's share performance, it can relatively easily just sell its

stakes (Douma, George, & Kabir, 2006: 643). This makes institutional investors "effectively risk-neutral and more willing to accept increased risk exposure" (Strange, 2018: 1234).

While sharing important key features, each of these four groups of shareholders is no homogeneous unit. Their goals and activities are likely to depend on the social, economic and political environments from which they originate (Strange, 2018: 1236; Estrin *et al.*, 2016). We therefore include the shareholders' headquarters, which we define as the country in which the company was originally founded and is registered (Birkinshaw *et al.*, 2006: 684). The location of the headquarter matters in several ways: It allows to distinguish between domestic and foreign owners and, relatedly, to consider factors including the democratic quality of political rule and the jurisdiction to which a company is subject.

Accounting for the company headquarter allows us to capture that a company can become subject to two potentially conflicting laws: the local laws of the country in which it operates and the national laws of the country in which it is registered. This may matter regarding corporate responsibility and a firm's legal obligations. A case in point are firms with headquarters in a member state of the European Union (EU), which are subject to the 2012 regulation on jurisdiction in civil matters[36] according to which victims of human rights abuse committed by corporations can bring a tort claim against a company domiciled in the EU, even if the harm that provides basis for the claim occurred outside of the EU (Van Dam *et al.*, 2017). Differences between state-owned and privately-owned companies in the goals, and in the capacities to reach them, might vanish if both come from home countries with similarly high government quality (Estrin *et al.*, 2016; Grøgaard, Rygh, & Benito, 2019).

3.2.3 Ownership concentration: The power over corporate decision-making

Pursuing the principal-agent logic, the principal A may be the shareholder exerting power over the agent B, i.e. the company's management. The most straight-forward channel of a particular shareholder's power over a company's course of action is for this shareholder (A) to directly own at least 51 per cent of the shares in the company (B). By this logic, power-over considers the concentration of ownership, in particular the percentage of shares that a certain shareholder, such as the state, owns in a company. The extent to which an owner can reach its goals depends on the relative number of shares it owns.

Next to the single-controlling shareholder that can virtually define a company's corporate strategy, the majority shareholder has decisive influence in the business operations and strategic direction of the company by virtue of controlling more than half (> 51 per cent) of the voting interests (Thomsen & Pedersen, 2000). As Holderness and Sheehan (1988: 319) observe, "majority shareholders are usually directly

[36] EU Regulation No. 1215/2012 of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast), OJ L 351/1, 20 December 2012.

involved in firm management. That is to say, majority shareholders do not merely monitor management teams, they lead them". As such, the majority-shareholder model provides an important corrective to suggestions of global managerial dominance divorcing control ownership and control (cf. Gourevitch & Shinn, 2005: 5).

Dispersed owners have less capacity to influence the management individually (Armstrong, Guay, & Weber, 2010: 210). Lloyd, Modani and Hand (1987) distinguish between strong owner control, if one party holds more than 30 percent stock ownership; weak owner control if 10 to 30 percent stock ownership is owned by one party; and managerially controlled firms if no party holds 10 percent or more. In sum, ownership concentration can range from one single controlling shareholder that "dictates corporate policy […] by managing the firm directly […to dispersed ownership with several shareholders…] too small and disorganised to impose their will" (Bennedsen & Wolfenzon, 2000: 114). While blockholding owners can exercise power over a company, the extent to which individual owners in dispersed settings can achieve their goals depends on the exact composition, as well as their respective identities.

Providing the exact share that each shareholder holds in a company, the TOSCO dataset also allows to consider small investors (also known as 'public float') who individually own less than 5 percent of firm equity and purchase their shares on local or international stock exchanges (Holderness, 2009). Conceptually, these small investors present no separate type of ownership because each of the four types can be at least partially traded on the stock exchange. Together, however, they may represent significant shares of a company's total ownership. For instance, in 2019 Vodafone UK is owned to almost 77 percent by individual small investors that trade at the London Stock Exchange. Typically, these small investors have only limited interest in getting involved in the management of a company but focus mostly on diversifying their investment portfolios (Thomsen & Pedersen, 2000; Connelly *et al.*, 2010).

3.3 The TOSCO dataset

TOSCO covers the ownership of commercial ISPs in all 49 independent mainland countries plus Madagascar[37], that is 44 sub-Saharan and the five North African countries, from 2000 until 2019. The internet is said to have arrived to Africa (precisely South Africa) in 1991; yet, it is not before the early 2000s that it became accessible to a larger population across the whole continent (Aker & Mbiti, 2010; Commander, Harrison, & Menezes-Filho, 2011; Nyirenda-Jere & Biru, 2015). The total number of ISPs included in TOSCO is 196 which amounts to 3'122 company-years over the time period covered, considering that not all

[37] Due to data availability and connectivity, we exclude the small islands Cape Verde, Comoros, Mauritius, La Reunion, Sao Tome and Principe, and the Seychelles.

companies existed over the whole period. While 108 companies were operative in Africa in 2000, it was 162 in 2019. The time dimension allows capturing interdependences and hierarchies among ISPs.

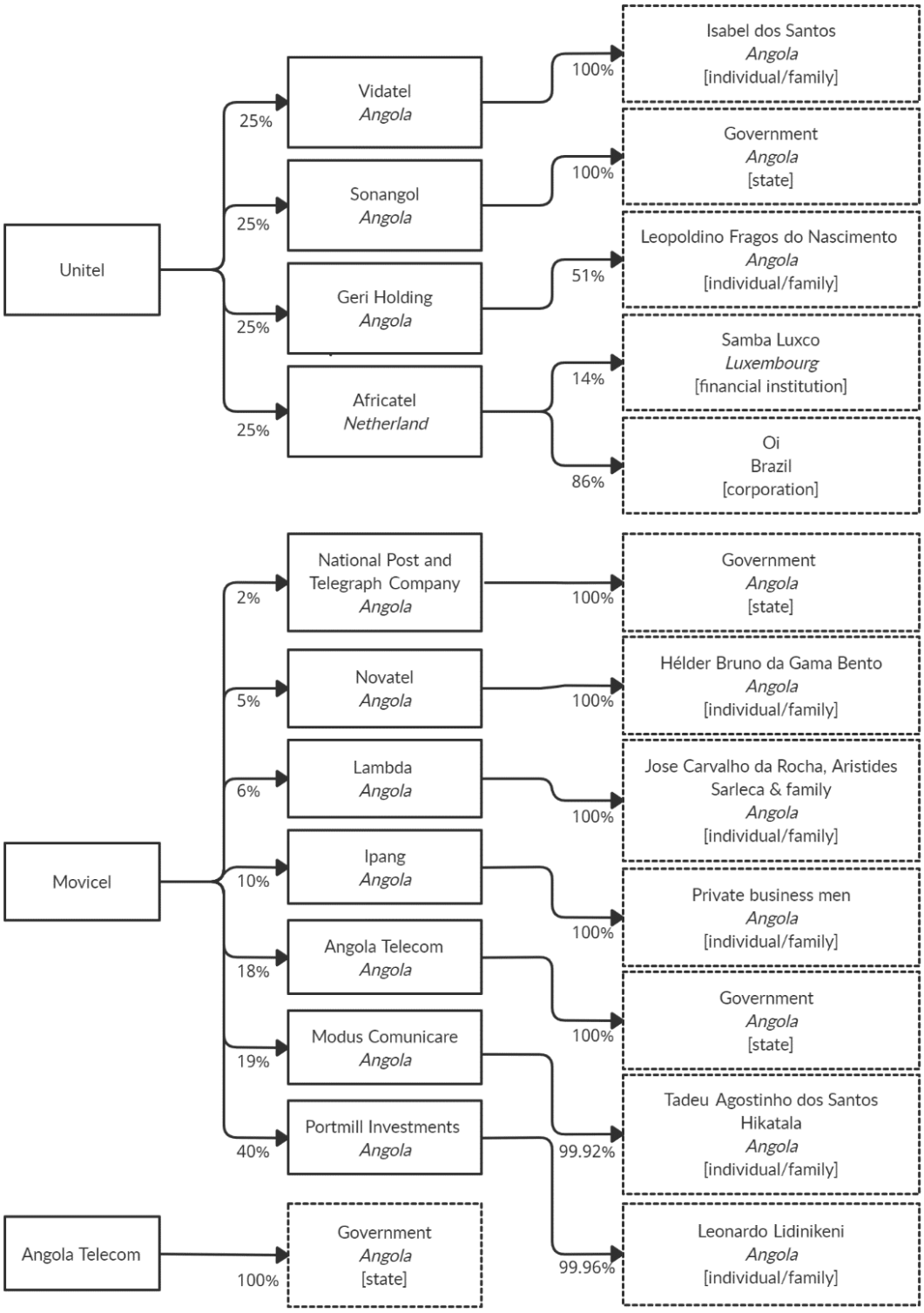
TOSCO includes all telecom companies that are members of the Global System for Mobile Communication (GSM) Association and started providing internet with second generation (2G) standards. These companies generally cover most of a country's population, especially in contexts, such as those prevailing on the African continent, where most consumers access the internet through their mobile phone, hence using GSM (mobile) technology. We add the 14 operators that provide access through fixed lines, which often used to be the state-owned monopoly providers. We exclude companies that provide 2G through Code Division Multiple Access (CDMA), a cell phone service technology competing to GSM, as well as companies that only provide 3G (UMTS) and/or 4G (LTE/WiMax) services. The reason being that these companies only comprise small parts of a country's internet user base; the latter two also usually run on top of the infrastructure of GSM providers. Mobile virtual network operators (MVNO) are therefore omitted, too. Overall, we concentrate on ISPs that are telecom companies with a physical presence in the territory on which they operate and that hold official state licenses to operate cables and possess communications infrastructure.

3.3.1 The structure of the TOSCO dataset

Our unit of analysis is the individual shareholder. For each ISP in a country, we consider all shareholders and their exact shares (first shareholder level), plus, if applicable, the shareholders owning each of these shareholders and their exact shares (second shareholder level). The data determines 539 shareholders in total; 244 at the first level and 295 at the second level. Overall, we only miss information for less than 10 percent of the company-years.

To give an example, in 2019 Angola, access to the internet was provided by three companies (see Figure 8): Unitel, Movicel and Angola Telecom. Looking at their respective shareholders reveals that the state is indeed involved in all three companies. Angola Telecom is 100 percent state-owned. The country's largest ISP Unitel is owned by four shareholders with each 25 percent of the shares, namely Africatel (Netherlands), Sonangol (Angola), Geni Holding (Angola) and Vidatel (Angola). Vidatel is owned 100 percent by Isabel dos Santos, the daughter of José Eduardo dos Santos, then president of Angola; the state oil company Sonangol is 100 percent owned by the Angolan state; and, Geni Holding is majority-owned by General Leopoldino Fragoso do Nascimento, then member of the government and known as one of the closest allies to the former president.

Figure 8. Structure of telecommunications ownership in 2019 Angola



As concerns Movicel, 20 per cent of its shares is owned by the Angolan state, through Angola Telecom and the National Post and Telegraph Company. The remaining 80 per cent is split between five ostensibly private Angolan companies; yet, four of them are majority-owned by the president's entourage. The majority shareholder of the investment company Lambda includes the Minister of Telecommunications and Information Technologies José Carvalho da Rocha. Portmill Investments, Novatel and Modus

Comunicare are owned by high-ranked military officials that served in the presidential guard. This example demonstrates the importance of the second shareholder level, as well as the biographic information about individual owners, for any study of the influence of specific actors, notably the state.

3.3.2 Data sources and coding decisions

The data included in TOSCO comes primarily from company and market analysis software (e.g., Thomson and Reuters' Eikon [eikon.thomsonreuters.com] and Orbis [orbis.bvdinfo.com]), specialised blogs (e.g., Research ICT Africa [www.researchictafrica.net]), news websites like All Africa [AllAfrica.com] and Quartz Africa [https://qz.com/Africa], and Bloomberg Snapshot repositories [www.bloomberg.com]. This information is triangulated with the annual reports provided by the telecommunications companies and data from market research and analysis companies, in particular TeleGeography [www.telegeography.com], which are limited to the dominant companies. All empirical information we use is publicly available online. For each data entry, the corresponding sources are reported and saved as .pdf-file. In order to ensure data accuracy, we ran several cross checks, and all cases were independently coded by at least two trained research assistants; any discrepancies or uncertainties were discussed in the team at a weekly basis.

While we coded the ownership of each company with greatest care, for some cases, the actual ownership situation may be more complex than it appears in our data. Four reasons can be highlighted here. First, for the concerned countries, (reliable) data tend to be generally scarce; it is an open secret that data on socio-economic indicators in African countries is thin (Przeworski *et al.*, 2000: 117). This holds also true for publicly available information about ownership of individual telecommunications companies. Examples include opaque ownership structures such as the one in Somalia where a functional state government is absent, and part of the public infrastructure, including telecommunications, are allegedly owned by warlords with connections to Al-Shabaab such as Ali Ahmed Nur Jim'ale (Iazzolino, 2015); and, cases in which the state administration lacks the capacity to make all companies register their shareholders, let alone make this information electronically available. In cases, in which it was impossible to rely on trustworthy sources to code all shareholders, we report the missing ones as 'unknown' so that its share can still be considered when determining properties such as the ownership concentration in a country.

Second, since in the early 2000s, the internet was only starting to reach the greater public in some African countries, transactions or company reports were neither made public back then nor uploaded ever since. To interpret certain key transactions that happened in the early 2000s, we had to rely on a limited number of news articles, with fewer possibilities to triangulate the information.

Third, we aim to keep complex transnational corporate structures as parsimonious as possible. Specifically, if a company is ultimately owned 100 per cent by a parent company with the same company brand, we directly refer to this parent company as ultimate beneficiary and do not include (sub-)regional subsidiaries as shareholders. An example is the French telecommunications giant Orange, which operated through various (sub-)regional subsidiaries before it opened an operational head office for the Middle East and Africa in Casablanca, Morocco, beginning of 2020. Since in all these cases, Orange (France) is the ultimate beneficiary, we do not include the sub-regional entities but directly refer to Orange (France).

Fourth, and last, especially in non-democratic contexts, the distinction between firms that are owned by the state and firms owned by individuals/families is often blurred. The said individuals may occupy powerful positions in the government, have strong ties to influential government officials, or are close allies if not relatives of the incumbent (Arayssi & Jizi, 2019; Djankov *et al.*, 2003). To keep the owner identities analytically separate, we refrain from coding these as state-owned. Yet, we provide biographic details, where known, that allow to determine if the respective individual or family is a member of the immediate political entourage, as the example of Angola in 2019 highlights (see Figure 8).

3.3.3 Descriptive overview

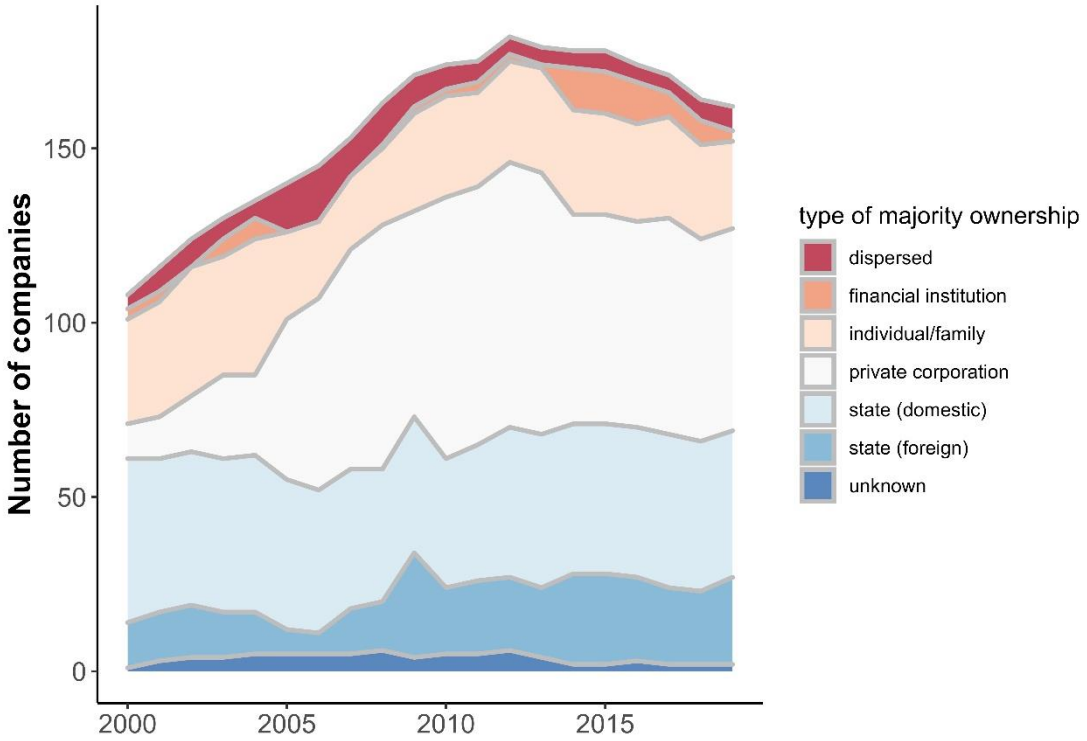
TOSCO allows for different ways of how to assess a company's owner identity and ownership concentration (based on the aggregated identity of its shareholders) as well as a country's ownership structure of the telecommunications sector (considering the aggregated identity of the companies). It can be screened on multiple criteria, including state involvement (e.g. indirect/direct), subsidiaries (e.g., number, country, foreign/domestic), and shareholders' political-economic background (e.g. democratic; ex-colonial; industrialised). Our granulated data at the shareholder level allows researchers to define the thresholds according to their research needs and interests.

In providing some descriptives, we demonstrate three select ways of aggregating or filtering our data.[38] First, we determine the majority type of ownership for each company and count the absolute number of companies per type in a given year as a means to showcase their distribution over time. Second, we focus on the extent to which the telecommunications sector of a given country in a given year is dominated by the state. Third, and last, we account for the transnational character of the sector by featuring those shareholders with the highest number of subsidiaries, including the location of their headquarters as well as those of their subsidiaries.

[38] Replication codes are provided in the supplemental materials.

Figure 9 shows the distribution of types of majority ownership (> 51 percent of the shares) across the African telecommunications sector over time. A company's owner identity is typically determined based on the respective individual or aggregated percent of shares hold (Sur, Gassmann, & Zhang, 2019).

Figure 9. Distribution of the identity of the majority owner, 2000-2019

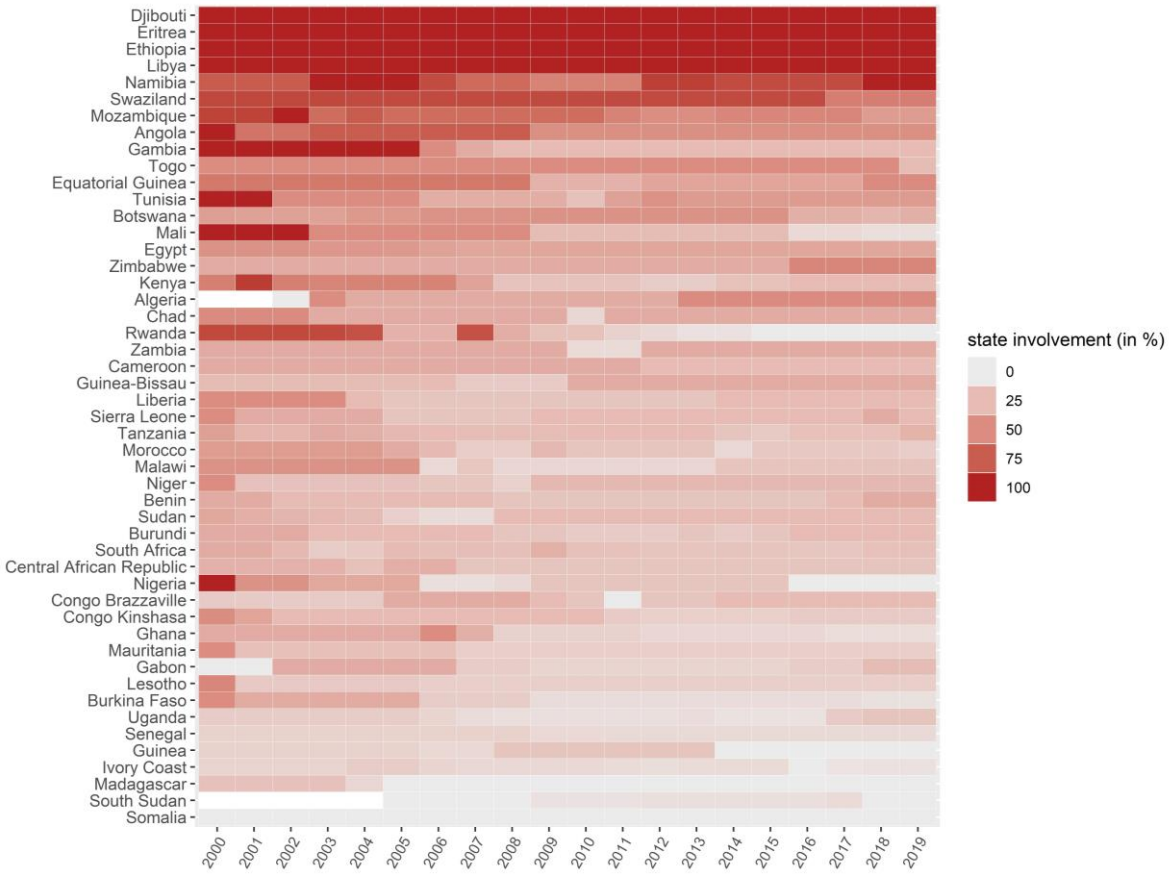


If no single majority holder exists, we identify the majority owner type based on the totalled shares of the dominant shareholder group. To give an example, if the sum of shares of all private-corporate owners collectively exceeds 50 percent, this company would be majority-owned by corporations. In the absence of any individual or collective majority owner type, we view a company's ownership as dispersed among a large number of small shareholders. Figure 9 corroborates that there are only few missing or 'unknown' values.

In Africa, as in most other parts in the world, the telecommunications sector was traditionally regulated by state-controlled monopolies. Figure 9 indicates that while, overall, the number of companies majority-owned by the domestic state remains relatively constant, in particular the number of companies owned by private corporations considerably increased over time. While 47 companies were majority-owned by the (domestic) state in 2000, the number went only slightly down to 42 in 2019; yet, since the number of total companies increased from 108 in the year 2000 to 137 in 2019, the relative number of state-owned companies decreased from about 44 percent in 2000 to 31 percent in 2019. The number of companies majority-owned by the state is somewhat higher if we take into account that some of the individually or

family-owned companies belong to the incumbent's political entourage (e.g., N_{2019} = 45). At the same time, the number of companies majority-owned by private corporations more than quintupled, from initially 10 to 58 in 2019.

Figure 10. Patterns of state involvement in the telecommunications sector, 2000-2019



Note: The darker the squares are shaded, the higher the degree of domestic state involvement among all ISPs in a country in a given year, e.g. dark red squares mark 100 percent state-owned telecommunications sector; empty squares for years with no operating ISPs.

Second, the retreat of the state from the telecommunications sector across the African continent is corroborated by Figure 10. The figure maps state involvement in domestic ISPs by summing up the stakes held by the state in individual ISPs and dividing them by the total number of ISPs in a given country-year. It turns out that in several African countries, the share of fully state-owned companies is still 100 percent. In Djibouti, Eritrea and Ethiopia, the government has always been the only shareholder of the only ISP operating in the country. In most other countries, however, the degree to which the state is involved considerably decreased with time. In Rwanda and Mali, for instance, the state has no majority in any ISP anymore. In Tunisia, in turn, the involvement of the state in ISPs operating on its territory first decreased and then—with a change in the political regime following the 'Arab Spring'—increased again.

Third, and last, Table 4 captures the increasing transnational character of the telecommunications sector on the African continent. In fact, and as the table indicates, several big companies with headquarters in Africa (e.g. MTN, Maroc Telecom and Econet), Europe (e.g. Orange and Vodafone), and beyond (e.g. Airtel and Africell) hold shares in various ISPs across African countries.

Table 4. Shareholders with at least four subsidiaries

Shareholder name	No. of subsidiaries	Headquarter	Subsidiaries	Majority owner type
MTN	16	South Africa	Benin, Cameroon, Congo Brazzaville, Ghana, Guinea, Guinea-Bissau, Ivory Coast, Liberia, Nigeria, Rwanda, South Africa, Sudan, South Sudan, Swaziland, Uganda, Zambia	corporation
Orange	17	France	Botswana, Burkina Faso, Cameroon, Central African Republic, Congo Kinshasa, Egypt, Guinea, Guinea Bissau, Ivory Coast, Liberia, Madagascar, Mali, Morocco, Niger, Senegal, Sierra Leone, Tunisia	corporation
Airtel	14	India	Chad, Congo Brazzaville, Congo Kinshasa, Gabon, Ghana (Airtel-Tigo), Kenya, Madagascar, Malawi, Niger, Nigeria, Rwanda, Tanzania, Uganda, Zambia	corporation
Maroc Telecom	9	Morocco	Benin, Burkina Faso, Central African Republic, Chad, Gabon, Ivory Coast, Mali, Niger, Togo	state
Econet	6	South Africa Zimbabwe	Botswana (Mascom), Burundi, Central African Republic, Lesotho, Rwanda, Zimbabwe	dispersed
Vodacom	5	South Africa	Congo Kinshasa, Lesotho, Mozambique, South Africa, Tanzania	corporation
Vodafone	4	United Kingdom	Egypt, Ghana, Kenya, South Africa	corporation
Africell	4	Lebanon	Congo Kinshasa, Gambia, Sierra Leone, Uganda	individual/ family

Note: Entries ordered by number of subsidiaries, both majority- and minority-owned subsidiaries; 'dispersed' refers to companies with no majority owner type.

The share of companies with a headquarter abroad increased from 51 per cent in 2000 to 66 percent in 2019. Due to an increasing awareness of the inefficiency of monopolist (state) operators and technological changes, many countries started liberalising their markets in the 1990s (Alemu, 2018; Laffont & Tirole, 2000: 3). This trend came along with privatisation but also internationalisation. Telecommunications

turned into a "booming sector at the heart of economic development" (Alemu, 2018: 2), attracting major foreign investments from abroad. In view of the political and economic sensitivities associated with infrastructure ownership, privatised and/or foreign ownership provides a "barometer of states' willingness to share authority with others" (Doh, Teegen, & Mudambi, 2004: 234; cf. Mudambi, 2003).

3.4 Telecommunications ownership and the political effects of the internet

We demonstrate the explanatory potential of the TOSCO data with regression analyses on the factors influencing the effect of internet penetration on democratic change. Returning to the central debate on internet technologies challenging versus strengthening authoritarian rule (see introduction), we propose that the political effects of the internet systematically vary with the ownership of those companies providing internet access, controlling for a country's level of internet penetration (Freyburg & Garbe, 2018). In particular, we expect the democratising potential of the internet to depend on the extent to which the state owns the internet infrastructure in a country. To empirically test this expectation, we revisit the study by Rød and Weidmann (2015) on the effects of internet penetration on democratic change.

Rød and Weidmann (2015) approach this question by way of a two-step analysis. First, they examine, and demonstrate, that the internet is more likely to expand in regimes experienced in the censorship and control of traditional media. Second, they explore how internet expansion affects changes toward democracy. Here, they find no evidence that "democracy advances in autocracies that expand the Internet [and if] anything, the relationship is the opposite." (ibid.: 348). In developing their argument, they acknowledge that "[c]onveniently for autocrats, online services are often provided by state-run telecommunications agencies" (ibid.: 340), which they assume to facilitate government control of internet-based communication; they further notice "that even when the suppliers of Internet connections are privately owned, they are often obliged to comply with government requests" (ibid.). Yet, they do not put this observation to a systematic, empirical test. Our data allows to examine the effect of state ownership of telecommunications companies on democratisation, while considering the level of internet penetration.

In more detail, following the *power-to* logic, we propose that if the state has substantial influence over the internet-providing companies, it has a higher capacity to control internet-based communication and information and hence to use internet services for its own benefits. State governments can use their shares in ISPs to exert direct influence over the company's behaviour and make it comply with requests that may benefit the ruling elite. Depending on a government's needs to control information flows (Hellmeier, 2016), this may include more direct forms of control such as the disruption of internet access during critical events, notably elections (Freyburg & Garbe, 2018; Rydzak, Karanja, & Opiyo, 2020) and

censorship of content deemed critical of the government (Deibert *et al.*, 2008), or more subtle forms of control, such as the surveillance of crucial opposition actors (Michaelsen, 2016).

In line with the *power-over* logic, we expect that the more the state is involved in the ISPs operating on its territory, the more likely it can effectively control and manipulate digital flows of communication and information. If a state has substantial control over the telecom sector by holding majority-shares in most, if not all ISPs, it should be able to effectively implement technical information control; internet coverage should hence decrease chances for democratic change. We expect the effect of internet ownership to be independent of the level of internet penetration. Ethiopia, for instance, has one of the worldwide lowest levels of internet penetration and use and still experienced at least six internet shutdowns between 2016 and 2019, for various reasons. Even in countries with low internet penetration, governments have incentives to control internet access, partially because access is usually reserved to urban and political (opposition) elites (Nisbet, Stoycheff, & Pearce, 2012). Taken together, we therefore expect: *The more shares the state owns in companies providing access to internet services on its territory, the lower the likelihood of democratic change in that country.*

To test our argument, we replicate Rød and Weidmann's (2015) study on a sub-sample of African countries between 2000 and 2010 ($N = 340$), using their replication data and code—yet, we include a variable Share of state-owned enterprises (SOE) that indicates the share of ISPs that are majority-owned by the state in a given country-year (see Figure 10). As Rød and Weidmann (2015), we use random effects logistic regressions with indicators of democracy derived from Polity IV (Marshall, Gurr, & Jaggers, 2014) and Geddes, Wright and Frantz (2014, 2016) as dependent variables, % Internet penetration and Change (Δ) in internet penetration from one year to the next as independent variables, plus a number of controls likely to influence democratisation, such as financial capabilities and wealth, domestic unrest, regime type, and the size of the population (Rød & Weidmann, 2015: 343). In line with the original study, we run the models using first Democratic change (Polity IV) as dependent variable, which is operationalised as dichotomous variable taking the value 1 if a regime moves in a democratic direction and 0 otherwise, and then Democratisation, which is a dichotomous variable indicating transitions to democracy as operationalised by Geddes, Wright and Frantz (2014, 2016). Table 5 presents the results of the regression analyses with Democratic change (Polity IV) as dependent variable. [39]

As expected, the share of state-owned ISPs per country-year has a statistically significant negative effect on democratic change both in the model controlling for internet penetration rates from the previous year

[39] If Democratisation (Geddes, Wright and Franz) is used as dependent variable, none of the independent variables—% Internet penetration, Change in internet penetration, and Share of SOE—turns out to be significant, see Appendix C1.

(Model 3) and for a change in internet penetration rates (Model 4). In contrast to the results in the original regression analyses by Rød and Weidmann (2015) on autocracies worldwide, Change in internet penetration turns out to have a significant negative effect on democratic change in the African sub-sample (Model 2), while the effect of internet penetration in the previous year remains insignificant (Model 1). This mixed pattern remains robust if we include our SOE variable, suggesting that rather than internet penetration per se, it is the involvement of the state in companies providing access to the internet that can explain receding democratisation in some countries.

Table 5. Estimated effect of state-owned ISPs on democratic change in Africa

	Model 1	Model 2	Model 3	Model 4
% Internet penetration$_{t-1}$	-0.01 (0.08)		-0.04 (0.08)	
Δ Internet penetration		-1.49 (0.75)*		-1.61 (0.73)*
share of SOE			-2.71 (1.15)*	-3.00 (1.20)*
ln(GDP pc)$_{t-1}$	-0.80 (0.41)*	-0.51 (0.41)	-1.06 (0.44)*	-0.80 (0.45)
GDP pc growth$_{t-1}$	3.31 (3.53)	2.85 (3.62)	4.06 (3.68)	3.93 (3.77)
ln(Trade openness)$_{t-1}$	-0.05 (0.53)	0.00 (0.53)	-0.05 (0.55)	0.01 (0.55)
ln(Oil/gas income)$_{t-1}$	0.04 (0.03)	0.04 (0.03)	0.04 (0.03)	0.04 (0.03)
Ongoing civil war	-0.50 (0.51)	-0.51 (0.51)	-0.37 (0.53)	-0.35 (0.53)
Military regime	2.49 (0.88)**	2.54 (0.88)**	2.04 (0.95)*	2.03 (1.00)*
Personalist regime	0.35 (0.48)	0.22 (0.48)	-0.49 (0.58)	-0.75 (0.60)
ln(Total population)$_{t-1}$	-0.34 (0.27)	-0.22 (0.27)	-0.48 (0.29)	-0.37 (0.30)
% Rural population$_{t-1}$	1.21 (2.42)	1.12 (2.53)	0.57 (2.43)	0.78 (2.56)
(Intercept)	7.55 (6.73)	4.28 (6.93)	13.07 (7.32)	9.94 (7.61)
AIC	217.74	210.82	212.56	204.04
BIC	279.00	272.08	277.55	269.03
Log likelihood	-92.87	-89.41	-89.28	-85.02
No. of observations	340	340	338	338
No. of countries	37	37	37	37

Note: Standard errors in parentheses. Time since transition (as well as its squared and cubed transformation) not displayed. Monarchies are also not displayed due to their low occurrence ($n = 2$) and large standard errors. In the models including the *share of SOE* (i.e. state-owned ownership), two observations are excluded as there were no ISPs operating in Algeria in 2000 and 2001. *$p < .05$, **$p < .01$,***$p < .001$.

3.5 Discussion and outlook

Largely out of public view, beneath the layers of application and content, the internet has a complex technical architecture. It is specifically this physical infrastructure that, connecting the individual customer to the internet, is key to controlling the flow of digital information and communication. Internet service providers (ISPs) with control over the physical infrastructure can extend that control into applications and content. Therefore, a state government's ability to control access to the internet and its use, or its interruption, depends on the extent to which it controls the ISPs that grant internet access to customers on its territory. To better understand how technology, politics, and economy are interacted, we suggest taking into account the role of those ISPs that provide last-mile connection to end-users. We

therefore propose that the ownership structure of ISPs is key to explaining the determinants and the effects of the internet, notably the potential of internet diffusion for democratic change. Yet, existing studies commonly miss to consider this factor in a systematic manner.

In this paper, we presented TOSCO, a dataset that maps the owner identity of all ISPs operating on the whole African continent between 2000 and 2019. In Africa, the number of people with access to internet has grown tremendously over the last decade. New opportunities in communicating and accessing information are expected to challenge Africa's long-lived autocrats. The rising number of recent internet shutdowns indicates that incumbent rulers may indeed attribute some danger to this new technology. At the same time, authoritarian rulers seek investment in modern information and communication technologies as a means to stimulate economic growth and to cope with social and economic grievances if perceived as threats to their regimes' stability. Findings from our replication of the study by Rød and Weidmann (2015) on a sub-sample of African countries, and including our estimate of majority-state involvement, indeed suggest that the internet's effect on democratisation depends on the extent to which domestic internet infrastructure is state-owned.

While TOSCO allows to enter new ground in the analysis of the determinants and consequences of internet penetration, taking into account a pivotal factor of internet control—infrastructure ownership, we need to acknowledge that the African telecommunications sector is currently experiencing drastic changes in the provision of internet infrastructure, with foreign companies investing in the hardware that is used by ISPs (e.g. fibre optics, copper cables, towers). For example, Chinese companies have built large networks of fibre optics in Africa, on which many local ISPs rely (Gagliardone & Geall, 2014), and content providers like Google, Facebook, or Amazon seek to set up their own independent networks (Nothias, 2020). It yet remains to be studied whether and how the increasing fragmentation of internet infrastructure and the role of new players emerging in the field will change ISPs' control over access to the internet in the long run. In any case, these developments signal that the telecommunications sector in African countries, and in particular the question of who owns and therefore controls the infrastructure, continues to be an exciting laboratory for studies of the determinants and effects of internet penetration.

POLITICAL DETERMINANTS OF FOREIGN INVESTMENT IN INTERNET INFRASTRUCTURE IN AFRICAN AUTOCRACIES

Abstract

This study examines the determinants of foreign direct investment (FDI) in internet infrastructure in autocracies, a sector that can be considered crucial for authoritarian survival in the 21st century. Setting up internet infrastructure is costly, which is why many developing countries rely on FDI to expand internet provision. Assuming that autocrats hesitate to give up control over information and communications infrastructure, I elaborate on factors that (1) likely put pressure on authoritarian governments to accept FDI in the telecom sector and (2) lead to variation in their openness toward foreign-autocratic versus foreign-democratic investors. I argue that a government's reliance on repression of the population and co-optation of the opposition influences not only their openness to FDI in the telecom sector *per se* but specifically their openness to FDI from foreign-autocratic or foreign-democratic investors. Empirically, I study the ownership of all internet service providers in authoritarian African countries between 2000 and 2019. The results suggest that the proportion of internet service providers owned by foreign-autocratic investors is higher in countries relying on repression but not co-optation. Overall, the results point to the political drivers of FDI in internet infrastructure, including its potential for authoritarian collaboration and its consequences for access to information.

4.1 Introduction

In the early days of the internet, many scholars believed that the internet would be a "liberation technology" (Diamond, 2010), challenging authoritarian rule because of its decentralised and supposedly control-frustrating nature (Boas, 2006). Indeed, authoritarian rulers seemed to be less keen on adopting internet technologies in the early 2000s (Milner, 2006). However, an increasing body of literature suggests that many authoritarian rulers have discovered the potential benefits of the internet for authoritarian survival. Different techniques allow governments to control and manipulate internet content and monitor online activities of individuals (King, Pan, & Roberts, 2013; Michaelsen, 2016). This pattern is reflected by Stier's (2017) finding that authoritarian governments have caught up in adopting internet technologies and, in some cases, even outperformed Western democracies. Also, due to their economic potential, it seems to be "rational for autocratic rulers to encourage [ICT] use in economy and society" (Stier, 2017: 25; Rommel, 2018). Hence, as Boas (2006: 9) suggests, "in order to reap the benefits of the technology while avoiding what they see as negative ramifications, [authoritarian] leaders would prefer to exert greater centralised control over Internet use". But how can governments exert such centralised control over internet access and use?

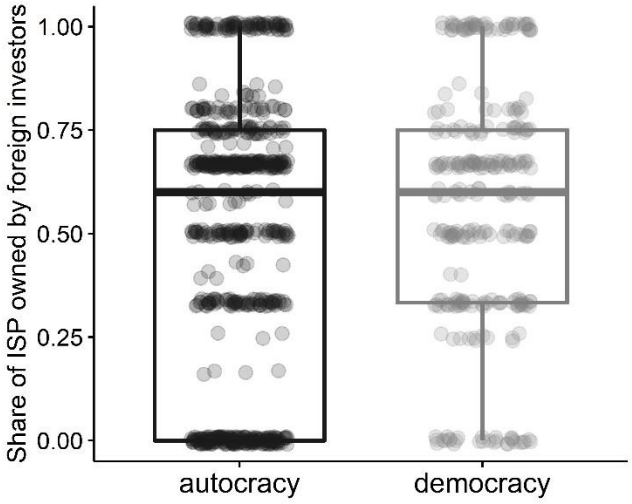
As more technically oriented scholars acknowledge, despite its decentralised nature, the internet's infrastructure is organised in a fairly hierarchical way that allows for centralised control over local networks. This infrastructure is commonly provided and run by internet service providers (ISPs), who are the gateways through which citizens can connect to the global internet. Thus, ISPs can be seen as bottlenecks for internet control (DeNardis, 2012). A study by Freyburg and Garbe (2018) suggests that governments are most successful at controlling access to the internet if they directly own the ISPs operating on their territory or cooperate with local business elites. Consequently, we would expect authoritarian governments to be less open to non-state actors, particularly foreign companies, to invest in and run internet infrastructure on their territory.

However, and surprisingly, in some African autocracies, the telecom sector is owned 100 per cent by foreign investors, whereas in other African autocracies, it has remained completely in the hands of domestic investors. Overall, the variability in foreign-owned ISPs is greater in authoritarian than in democratic regimes. Specifically, the variability in shares of local ISPs majority-owned by foreign investors is comparable, if not greater, in authoritarian (M = 0.49; SD = 0.34) than in democratic regimes (M = 0.57; SD = 0.29; see Figure 11).

The variance in foreign ISP ownership across African autocracies is mirrored by a variety of policies regulating foreign direct investment (FDI) in the telecom sector: Some authoritarian countries, like Eritrea or

Ethiopia, generally ban or restrict FDI in the telecom sector legally, whereas others indirectly discourage FDI in the telecom sector through regulatory charges (e.g., licensing fees). Zambia, for instance, which has no formal entry barriers to foreign investors, charges 12 million USD for a license to operate internet infrastructure (e.g. compared to 100'000 USD in Uganda), explaining why there is "still only one international gateway operator—the state-owned Zambia Telecommunications Company Ltd. (Zamtel)" (Williams, Mayer, & Minges, 2011). Other authoritarian countries like Gabon, Rwanda, or Mali, have strongly advocated for a liberalisation of the telecom sector. Against this variation of foreign investors in the telecom sector in African autocracies, this paper sets out to answer the following question: *Why do some authoritarian regimes hesitate to allow for foreign investment in the telecom sector, which is arguably most critical to authoritarian survival today, while others appear closed to foreign investment in this sector?*

Figure 11. Share of majority-foreign owned ISPs in Africa, 2000-2019



Note. Autocracies include all closed and electoral autocracies (*n* = 44); democracies include all electoral and liberal democracies (*n* = 24), using the *v2x_regime* variable from the Varieties of Democracy (V-DEM) dataset (Lührmann, Lindberg, & Tannenberg, 2017) for African countries between 2000 and 2019. Horizontal lines indicate the median; points indicate individual country-year observations.

Based on insights from scholarship of authoritarian survival (Gandhi, 2008; Bueno De Mesquita *et al.*, 2003; Magaloni, 2008), I focus on two mechanisms that are likely to explain the variation in authoritarian governments' hesitation to accept FDI in the telecom sector, namely repression and co-optation. In a second step, following recent scholarly work on authoritarian collaboration and diffusion (Erdmann *et al.*, 2013; Von Soest, 2015; Cooley, 2015), I argue that an authoritarian government's openness to FDI is likely to vary depending on the investor's origin. My findings suggest that the extent to which autocrats rely on repression and co-optation does not only influence their openness to FDI *per se*. Besides, governments that rely on repression appear to be more open to FDI from other authoritarian regimes, whereas countries in which power is shared with opposition forces are more open to FDI from foreign-democratic

investors. Overall, these finding suggest that authoritarian rulers who rely on repression and co-optation selectively attract FDI in the telecom sector from abroad.

In the following section, I discuss ownership of internet infrastructure and its importance for controlling access to information. Next, I develop a theoretical argument to explain differences in the prevalence of foreign shareholders in the telecom sector across authoritarian regimes. Subsequently, I test these expectations using cross-sectional time-series data of shareholders in the telecom sector across authoritarian African countries between 2000 and 2019 (Freyburg, Garbe, & Wavre, 2021), followed by a discussion and some conclusions.

Overall, my findings contribute to the study of authoritarian survival in a globalised and digitised world. I acknowledge that authoritarian governments may have strategic reasons to discourage FDI in the telecom sector to maintain control over internet access. At the same time, they are faced with institutional pressure to expand internet infrastructure by attracting foreign investors. My findings highlight that authoritarian collaboration can provide a channel to maximise the benefits from internet access while avoiding associated risks.

4.2 Internet infrastructure and control

Given the central role of companies providing access to internet services, governments give up some control over internet access when issuing licenses to (partially) foreign-owned ISPs. While common wisdom portrays the internet as decentralised and resistant to control, it actually relies on a fairly hierarchical architecture. At the local level, networks are typically run by ISPs that have control over both the physical infrastructure (e.g. cables, landing stations, radio towers) that is necessary to carry data across networks but also the IP addresses granted to individual customers. ISPs are centralised points of control or "gatekeepers" of the internet as they control the gateway through which data flows in and out (Lichtman & Posner, 2006; DeNardis, 2014:11). They are the ones to connect end-users to the internet and are hence in a powerful position to provide individual citizens with access to the global internet.

Most forms of manipulation to internet access are directly or indirectly carried out through ISPs. By disabling an autonomous system locally, its customers can effectively be cut from the global network. Blocking internet access can be achieved by powering down the network or manipulating the Border Gateway Protocol (BGP) tables—the protocol that is used to determine the routing of data traffic. In Cameroon, for instance, the government ordered ISPs providing internet access in the English-speaking regions of Cameroon to disrupt their services in 2017 (Nyokabi *et al.*, 2019). Also, in order to block specific websites, governments typically rely on ISPs. In Iran, the government banned access to several websites, including

social media platforms, by ordering ISPs to block IP addresses resolving to the banned domain names (Xynou *et al.*, 2017).

By granting foreign investors access to the telecom sector, governments partially give up control over access to information and communication online. While state ownership is the most direct form of controlling corporate decision-making (Freyburg, Garbe, & Wavre, 2021), political economists have emphasised the high costs of foreign relative to domestic ownership (Lecraw, 1984; Reuber *et al.*, 1973). Particularly in developing countries, foreign firms have better chances to exert political power over the government than domestic firms (Desbordes & Vauday, 2007). The presence of foreign firms can be challenging for the incumbent when the investor's goals are conflicting with their own. For instance, when investors come from countries with high corporate social responsibility standards, they may refuse to support policies that undermine human rights (Scherer & Palazzo, 2011). Concerning the telecom sector, this may prevent the government from effectively exerting control over internet infrastructure, as highlighted by an example from Guinea: The Guinean telecommunications regulator requested all ISPs in Guinea to set up a "center for control and oversight of traffic (voice and data)" (Human Rights Watch, 2016) that would direct all data traffic through a central server accessible to the Guinean government. Three out of four ISPs in Guinea owned by foreign investors (Orange, MTN and Cellcom) jointly resisted the government's request which they considered as a violation of the right to privacy (Micek & Kenyanito, 2016).

Given that foreign investors can undermine an authoritarian government's capacity to control internet infrastructure, I investigate why some autocrats accept FDI in the telecom sector and whether their openness to FDI is qualified by the investor's origin.

4.3 Theory

I define authoritarian regimes as those regimes in which the ruler cannot be removed from office by means of free and fair elections (Lührmann, Lindberg, & Tannenberg, 2017). Instead, authoritarian incumbents rely on various strategies to stay in power, including repression and co-optation of the opposition (Gerschewski, 2013). These strategies follow different logics but ultimately seek to stabilise authoritarian rule (Schneider & Maerz, 2017). I argue that the extent to which an incumbent relies on repression of their population and co-optation of the opposition has implications for their willingness to accept FDI in the telecom sector. On one hand, authoritarian rulers who rely on repression in the analogue world should be hesitant to give up control over access to and exchange of information in the digital space and, thus, be more reluctant to FDI in the telecom sector. On the other, governments that rely on formal co-optation of opposition actors should face more pressure to expand internet access and accept FDI in the telecom sector. Yet, foreign investors are no uniform actor, and even if autocrats are hesitant to accept FDI more

generally, they might be less hesitant to accept FDI from investors that come from authoritarian countries themselves.

4.3.1 Repression and co-optation

Repression is often regarded as the "defining feature of autocracies" (Gerschewski, 2013: 21) and can be summarised as the "actual or threatened use of physical sanctions against an individual or organisation […] for the purpose of imposing a cost on the target as well as deterring specific activities and/or beliefs perceived to be challenging to government personnel, practices or institutions" (Davenport, 2007: 2). Authoritarian governments often use repression, such as torture or killings, strategically when faced with civil unrest (Carey, 2010; Josua & Edel, 2015). Governments using repression are afraid of its exposure which may trigger unwanted responses in both the domestic and the international sphere. Domestically, when citizens experience mass repression, they are likely to engage in anti-regime protest (Carey, 2006; Pierskalla, 2009). Internationally, repressive governments may face a suspension of foreign aid or targeted sanctions, especially when their use of repression is well-documented and attracts media attention (Fuerrutter, 2021; Nielsen, 2014).

In a pre-digital era, both state and opposition actors operate in an environment "marked by limited information, limited capabilities, and uncertain payoffs" (Carey, 2006: 3). Increasing digitalisation offers chances and risks for the use of repression by government authorities. Concerning the risks, repression becomes more costly in the digital era as internet access permits individuals to record and share evidence of state violence and thereby mobilise people to protest against the regime (Karekwaivanane, 2019; Mutsvairo, 2016). By "documenting and digitally sharing evidence of police brutality, protesters translate[…] outrage over repression into additional support" (Christensen & Garfias, 2018: 2). Moreover, evidence of state violence can quickly be shared with the rest of the world, leading to increased pressure from the international community (Kasm, 2018).

At the same time, governments can also benefit from increased internet connectivity of their citizens. Leveraging internet infrastructure allows them to learn about anti-regime sentiment and monitor regime opponents. Such information can be crucial to forestall and prevent collective action (King, Pan, & Roberts, 2013; Qin, Strömberg, & Wu, 2017). It also enables authoritarian rulers to increase the precision of repression, making it politically less costly (Xu, 2020). In order to maximise the benefits of internet access, while reducing its risks, governments may strategically censor internet content that could trigger protest (King, Pan, & Roberts, 2013) or cut internet access for short periods to hide their use of repression and human rights violations (Gohdes, 2020).

Therefore, repressive governments should have an incentive to strictly control internet access so that they can use it for both surveillance and censorship or manipulation of access to (specific) internet services, when needed. Against this, I expect governments that rely on repressive tactics in the analogue world to be less willing to give up control over the internet's infrastructure. By admitting foreign firms to manage internet provision to large parts of the population, it becomes more difficult for a government to retain control over the exchange of digital information and communication. I, therefore, expect that more repressive regimes have fewer ISPs owned by foreign investors on their territory:

> *The more an authoritarian regime relies on repression, the smaller the proportion of ISPs owned by foreign investors that operate on its territory* (H1a).

As repression is costly, authoritarian governments increasingly seek to tie relevant actors to their regime by co-opting them in political institutions rather than to repress them (Gerschewski, 2013: 22). The role of political institutions in authoritarian regimes is subject to controversial academic discussions. More pessimist accounts see authoritarian institutions merely as a way to provide the incumbent with information about the opposition and as a forum to distribute spoils (Gandhi, 2008: 78; Geddes, 2006). More optimist accounts acknowledge that political institutions in dictatorships are not, as often claimed, mere window-dressing, but can "possibly perform […] some of the functions usually associated with democratic [institutions]" (Gandhi, Noble, & Svolik, 2020: 1363). I argue that, from both perspectives, we should expect that governments relying on the co-optation of the opposition in formal political institutions face more pressure to provide public goods. On one hand, by including the opposition in formal political institutions, it becomes more costly for the ruler to buy support in the form of private rather than public goods. On the other, if political opposition is included in formal institutions, they are given a channel to press for policies, such as public goods provision, that are otherwise considered too costly. Due to the increasing economic value of ICT, internet access can be considered one of the most important public goods in the 21st century (Stier, 2017; Garrity, 2017)[40]. In turn, due to the high costs of expanding internet infrastructure, governments facing pressure to provide public goods should be more likely to attract FDI in the telecom sector.

In more detail, by including opposition actors in formal institutions, the government increases the size of the so-called 'winning coalition' (Mesquita & Smith, 2009) on whose support an authoritarian ruler relies to stay in power. In order to buy their support, the government will "find it increasingly difficult to pay off

[40] Specifically, Garrity (2017) considers the internet as a global public good due to its positive externalities.

key supporters through protectionist […] policies" (Hankla & Kuthy, 2013: 494).[41] Instead, they may choose to distribute public goods that will not only benefit the winning coalition but society at large (Bueno De Mesquita *et al.*, 1999). Second, institutions in authoritarian regimes can still "constrain the executive and provide a forum for policy and political bargaining" (Bonvecchi & Simison, 2017: 522).[42] Empirical studies show that political institutions, notably legislatures, can bring national economic issues to the agenda and increase government spending on social welfare (Simison, 2020; Hanson, 2013). Overall, institutions then provide the opposition with a channel to put pressure on the government to expand public goods provision, such as internet access.

Setting up internet infrastructure such as copper and fibre involves high fixed costs, however (Greenstein, 2020). This is why in most Western countries, commercial firms gained increasing weight in the sector (Leiponen, 2006: 341), and the internet gradually turned into a largely privatised good (DeNardis, 2014). In turn, especially in developing contexts that are marked by a lack of financial resources and capital flight (Anyanwu, 2006; Ajayi & Ndikumana, 2014), many governments rely on FDI to expand internet access. Therefore, I expect that authoritarian regimes facing pressure from co-opted opponents in political institutions are more likely to accept FDI in the telecom sector:

> *The more an authoritarian regime relies on formal co-optation of the opposition, the higher the proportion of ISPs owned by foreign investors that operate on its territory* (H1b).

4.3.2 Authoritarian foreign investment

Foreign investors are no uniform actor, however. Rather, they differ in their goals and practices based on the location of a company's registered headquarter (Birkinshaw *et al.*, 2006; Freyburg, Garbe, & Wavre, 2021). Thus, I argue that an authoritarian governments' openness to FDI in the telecom sector should depend on the investor's origin. Even if the government generally hesitates to accept FDI, they might be willing to grant access to investors from other illiberal regimes. For example, Algeria has had a relatively high share of foreign investors in the telecom sector between 2000 and 2019. However, all foreign majority-shareholders come from other autocracies.

As demonstrated by the literature on authoritarian diffusion, collaboration with other authoritarian regimes mostly seeks to prevent or undermine Western efforts at democratisation through political,

[41] In their selectorate theory, Mesquita and Smith (2009, 171) argue that a government relies on a so-called winning coalition "whose support is essential for sustaining the incumbent in office". If the winning coalition is small, the leadership may distribute private goods such as favourable tax policies that will not benefit society at large but retain the support of the leadership's crucial allies. However, the bigger the winning coalition, the costlier it becomes for a government to provide private goods.

[42] More specifically, Teo (2019) argues that political parties incentivize the government to invest in social welfare by challenging the re-election of the incumbent.

economic, and social ties (Weyland, 2017; Schmotz & Tansey, 2018). Therefore, the collaboration with other authoritarian regimes can be interpreted as an act to strengthen their own regime's survival. Case studies underline that outward FDI from authoritarian countries may serve as a tool to stabilise authoritarian structures elsewhere (Bader, Grävingholt, & Kästner, 2010). China, for instance, appears to have intensified collaboration with many African countries that are "supportive of their own rule" (Von Soest, 2015: 629) and share common policy goals. Also, investors from the Gulf region increasingly invest in nearby countries to foster "autocratic stability in the neighbourhood" (Freyburg & Richter, 2015: 511)

It may be beneficial for repressive governments to accept FDI in internet infrastructure from regimes that are "like-minded" vis-à-vis state sovereignty and human rights (Taylor, 2006). As compared to investors from democratic regimes, they may face less legal and reputational pressure from their home countries and civil society actors (Freyburg & Garbe, 2018). For example, all telecom operators that are members of the Global Network Initiative, a forum that provides (and self-imposes) behavioural guidelines for ICT companies, are based in Western democracies.[43] In turn, repressive regimes should prefer FDI by foreign-autocratic investors and might even benefit from it if the investing company already has experience in implementing censorship and surveillance.

> *The more an authoritarian regime relies on repression, the higher the proportion of foreign investors from authoritarian regimes* (H2a).

The role that formal institutions may play in a regime's openness to FDI from other autocracies is more ambiguous. On one hand, if a government uses formal institutions mainly to pay off opposition actors, they may see investment from other autocracies as an opportunity to get financial means to appease the opposition. On the other, if the opposition uses their position in parliaments and parties to press for political concessions, they may seek to prevent the government from attracting FDI from other autocracies.

Specifically, authoritarian governments that use, if not establish political institutions with the aim to pay off potential rivals, may prefer investment from firms whom they expect to accept their system of co-opting opponents. Firms from authoritarian countries, in which corruption is often common practice, can be considered more supportive of the domestic regime's system of bribery (Ledyaeva, Karhunen, & Kosonen, 2013). They may even be willing to pay large sums in exchange for a monopoly license with a privileged position in the market (Lambsdorff & Cornelius, 2000). For instance, in Equatorial Guinea, FDI from Chinese state-owned companies is said to perpetuate the regime by Equatoguinean President Teodoro Obiang Nguema in which the "local politically and economically privileged classes are the main

[43] Information about the initiative's goals and members can be found on their website: https://globalnetworkinitiative.org/

beneficiaries of the growing Chinese presence" (Esteban, 2009: 685). In that case, authoritarian rulers with formal institutions more likely grant access to foreign investors if these come from other authoritarian regimes.

At the same time, however, if opposition actors use their position in parties and legislatures to challenge the regime, they might lobby against investment from other authoritarian regimes. Foreign-autocratic companies may aid a government to implement information controls (Freyburg & Garbe, 2018) that likely affect the opposition's chances to express grievances and organise protest (Christensen & Garfias, 2018). Therefore, they might consider foreign-autocratic investors to support the ruling class, and should be more reluctant to allow foreign-autocratic investors to enter the market. Since both mechanisms are theoretically plausible, this remains an empirical question, resulting in the following two competing expectations:

> *The more an authoritarian regime relies on formal co-optation of the opposition, the* ***higher*** *the proportion of foreign investors from authoritarian regimes* (H2b).

> *The more an authoritarian regime relies on formal co-optation of the opposition, the* ***lower*** *the proportion of foreign investors from authoritarian regimes* (H2c).

4.4 Empirical approach

I analyse the determinants of foreign ownership of ISPs across authoritarian African countries between 2000 and 2019. The African continent provides a particularly fruitful setting to study the determinants of FDI in the telecom sector due to the variation in political regimes (Cheeseman, 2015), economic development, and internet connectivity (Aker & Mbiti, 2010), all of which likely inform a government's motivation and ability to attract FDI in the telecom sector. Domestic financial constraints to invest in in telecom infrastructure are comparable to other regions in the Global South, notably Latin America (Wallsten, 2001). In my analysis, I focus on authoritarian African regimes following the Regimes in the World (RIW) operationalisation by Lührmann, Lindberg and Tannenberg (2017), who define authoritarian regimes as those countries without free and fair de-facto multi-party elections ($N_{countries}$ = 44). Table 6 provides descriptive statistics for all variables included in the analysis. I use linear mixed models (LMM) including country random intercepts to account for within-country effects that might occur due to different ethnic or political circumstances, among others (Stegmueller, 2011), as well as time-fixed effects. Variance Inflation Factors

(VIF, Field, 2009) for a linear model excluding the random effect do not suggest substantial collinearity (all VIFs < 3.2).[44]

Table 6. Descriptive statistics

Variable	Min; Max	Mean (SD)	N
Dependent variables			
Share of ISPs (foreign)	0; 1	0.49 (0.34)	683
Share of ISPs (foreign-autocratic)	0; 1	0.20 (0.23)	683
Share of ISPs (foreign-democratic)	0; 1	0.28 (0.28)	683
Independent variables			
Repression	1; 5	3.37 (0.89)	683
Legislative Chambers	0; 2	1.37 (0.61)	683
Control variables			
GDP per capita in USD	111.93; 22'942.58	1'939.27 (2951.46)	650
Growth GDP per capita (%)	-62.38; 121.78	1.69 (8.19)	635
Corruption	0.08; 0.97	0.73 (0.2)	683
Total rents natural resources (% of GDP)	0.26; 84.23	16.21 (14.18)	612
Total Population (in thousands)	606; 200'963	22'684 (29'024)	674
Rural population (% of total population)	10.26; 91.76	58.40 (19.24)	674
Trade (% of GDP)	16.67; 348	70.7 (37.89)	622

4.4.1 Dependent variables

To calculate the proportion of foreign shares, I use the Telecommunications Ownership and Control (TOSCO) dataset covering ISPs and their shareholders in Africa between 2000 and 2019 (Freyburg, Garbe, & Wavre, 2021). TOSCO data includes all African ISPs that started by providing Global System for Mobile Communications (GSM), a second-generation standard, and, hence, provides a near-complete image of those companies providing internet access to individual customers in Africa. For each ISP, TOSCO lists information for all shareholders owning at least 5 per cent stakes, their respective number of stakes, and the location where the shareholder is legally registered.

To test Hypothesis 1a and 1b, I use the *share of ISPs majority-owned by foreign shareholders* per country-year as dependent variable. I focus on majority-ownership as the most straight-forward way to control a company's management and decision-making (Thomsen & Pedersen, 2000; Holderness & Sheehan, 1988). The legal place of registration of the majority shareholder (i.e., shares of 51 per cent or more) determines whether an ISP is coded as domestic or foreign. I then divide the number of foreign-owned ISPs by the total number of ISPs in a given country-year (Appendix D1 provides an example of this aggregation

[44] I estimate confidence intervals with the function bootMer of the package lme4, using 1,000 parametric bootstraps (Bates *et al.*, 2015).

rule). Figure 12 provides an overview of foreign(-autocratic) shares in ISPs per country and year. Appendix D2 provides an additional overview of the most dominant foreign shareholders' origins.

To test Hypothesis 2a, 2b, and 2c, I use the *share of ISPs majority-owned by foreign-autocratic shareholders*. I addition to coding the majority-headquarter as foreign, I determine whether the headquarter is based in a democratic or an authoritarian regime using the RIW operationalisation by Lührmann, Lindberg and Tannenberg (2017). I then divide the number of ISPs majority-owned by foreign-autocratic shareholders by the total number of ISPs in a given country-year (see Appendix D1).[45]

4.4.2 Independent variables

I use data from the Political Terror Scale (PTS) as an indicator of repression. PTS defines political terror as "violations of basic human rights to the physical integrity of the person by agents of the state within the territorial boundaries of the state" (Haschke, 2017: 1) and provides annual ratings that range from low levels (coded with 1) to high levels (coded with 5) of political terror. I rely on the PTS indicator informed by country reports from the US State Department (PTS_S) due to the high number of missing values in the indicators informed by reports from Amnesty International (PTS_A) and Human Rights Watch (PTS_H).

I use data from the Varieties of Democracy project (V-Dem; Coppedge *et al.*, 2020b) as an indicator of formal co-optation. Legislatures can be regarded as forums to monitor and pay off potential rivals (Gandhi, 2008) and provide opposition forces with the opportunity to shape political agendas (Simison, 2020). I use the number of legislative chambers (*v2lgbicam*) ranging from no chamber (coded with 0) to two or more chambers (coded with 2) as an indicator of formal co-optation through legislatures (Bove & Rivera, 2015; Frantz & Kendall-Taylor, 2014)

4.4.3 Controls

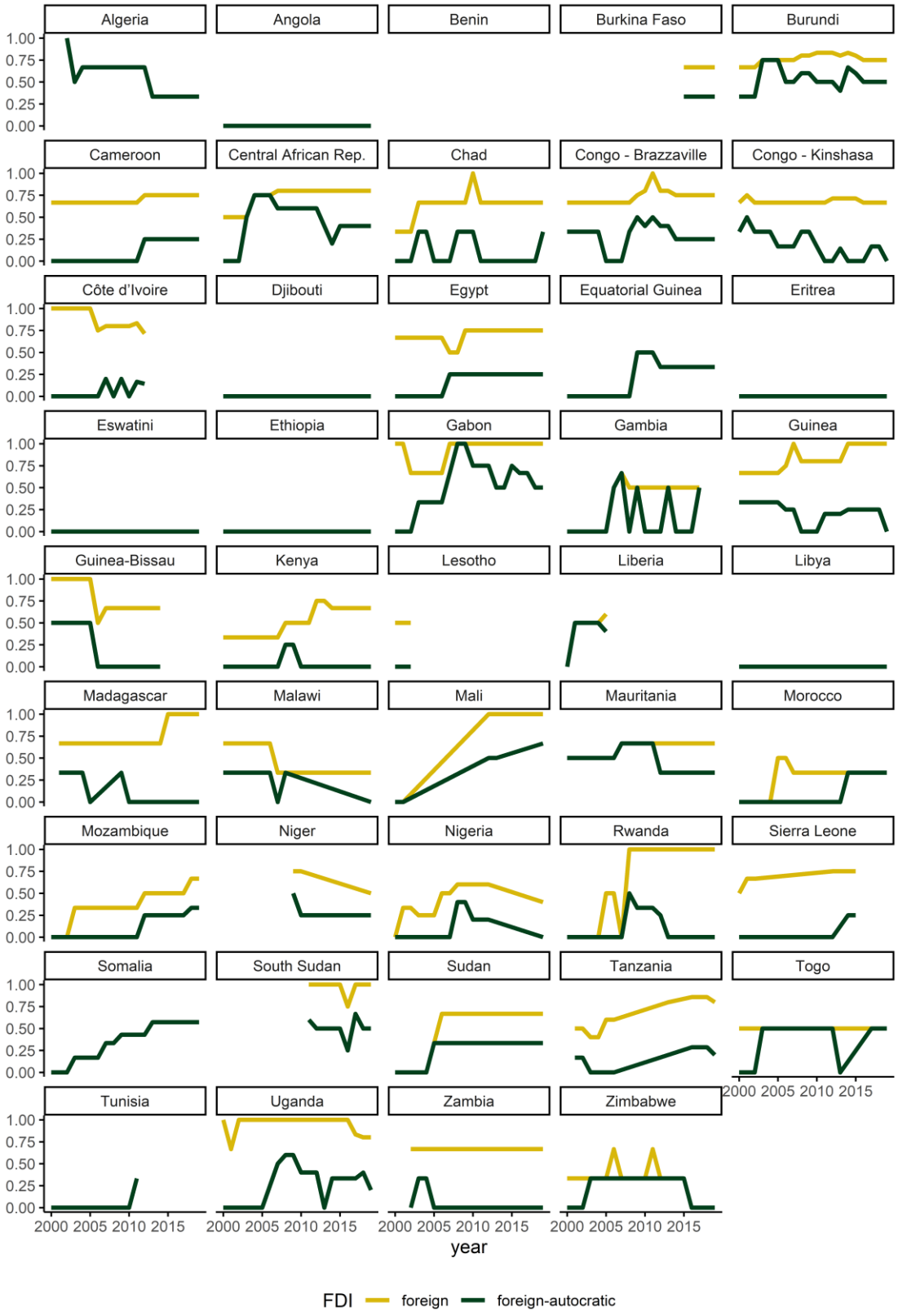
There are likely other factors influencing a government's decision to accept FDI in local internet infrastructure. I account for such confounders by including control variables covering economic, political, and demographic aspects. Economically, those regimes with a low gross domestic product (GDP) can be expected to be more dependent on FDI. Therefore, I include the (log) GDP per capita and the annual change of GDP per capita in per cent using World Bank indicators.[46] Furthermore, regimes with a wealth of natural resources often need the technology and capital of FDI to realise their potential (Bak & Moon, 2016). I

[45] To provide the full picture, I also estimate the effect of repression and co-optation on the share of foreign-democratic investors and include the results in all tables.

[46] All World Bank indicators are available online (World Bank, 2020b).

include a World Bank indicator for the total rents of natural resources as a share of GDP as further control variable.

Figure 12. Aggregated shares of foreign majority-owned ISPs per country



Note: Benin is only coded as autocracy in 2019.

Politically, different regime types vary in their openness to the international economy. Multi-party and single-party regimes are more open to international trade as they provide more stable institutions than personalist regimes, military juntas, and monarchies (Hankla & Kuthy, 2013). I use two indices from the V-Dem project to capture the extent to which the executive depends on the military (*v2x_ex_military*) or a royal council/family (*v2x_ex_hereditary*). Both measures range from 0 (low control) to 1 (high control) and indicate actual control over the executive, even in regimes in which legislatures formally exist, and hence address measurement validity problems of more discrete regime type indicators (Wilson, 2014). In addition, I account for a country's level of corruption that may deter foreign investors from entering the market due to moral beliefs and poor economic prospects in a market lacking competitiveness (Habib & Zurawicki, 2002). Specifically, I use the executive corruption index (*v2x_execorr*) by V-Dem, capturing how often members of the executive engage in corrupt activities with higher values indicating lower levels of corruption.[47] In my analyses, I use an inverted scale to facilitate interpretation (such that higher values indicate more corruption).

Demographically, a larger population requires greater internet coverage and might incentivise a government to accept FDI in internet infrastructure. Thus, I include World Bank indicators for the total (log) population and the percentage of rural population as control variables.

4.5 Results

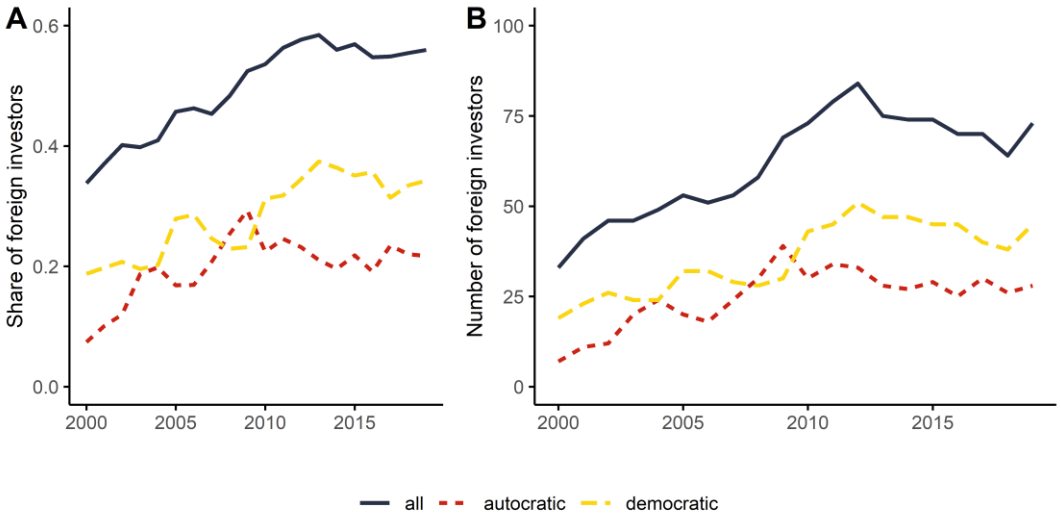
Between 2000 and 2019, the share of foreign investors has substantively increased, regardless of whether they come from autocracies or democracies (see Figure 13). Table 7 provides an overview of the results from the LMMs. As to the share of foreign investors (Models 1 and 2), the results indicate that authoritarian regimes with higher levels of state repression have significantly higher proportions of foreign-owned ISPs (B = 0.03, SE = 0.001, CI [0.01, 0.05]). This finding contradicts Hypothesis 1a that more repressive regimes are less likely to accept foreign companies to invest in local ISPs. Besides, the share of foreign-owned ISPs is significantly higher with increasing numbers of legislative chambers (B = 0.03, SE = 0.01, CI [0.01, 0.05]), supporting Hypothesis 1b that regimes relying on formal co-optation are more likely to accept FDI in the telecom sector.

For the share of foreign-autocratic ISPs as dependent variable (Models 3 and 4), results suggest that the share of ISPs with foreign-autocratic shareholders is significantly higher in those regimes with higher levels of state repression (B = 0.03, SE = 0.01, CI [0.01, 0.05]) supporting Hypothesis 2a. Results further suggest

[47] In contrast to commonly used data by Transparency International, V-Dem indicators rely on the same methodology for the entire time period under scrutiny.

that legislative chambers have no significant influence on the number of shares held by foreign-autocratic investors (B = 0.01, SE = 0.01, CI [−0.01, 0.03]), giving more weight to Hypothesis 2c than 2b, that legislatures discourage FDI from autocracies.

Figure 13. Foreign investment in ISPs 2000-2019



Note. Panel A indicates the overall share of foreign investors in ISPs; Panel B indicates the aboslute number of foreign investors.

For some economic indicators, notably natural resources rents, data is missing for several country-years (see Table 6). When excluding the control variables and estimating the effects of the independent variables only, the detected patterns do not change substantially. I run several robustness checks to account for time lags and the role of state ownership. To account for the potentially lagged effect of the variables, I re-run the models with all independent and control variables lagged by one year (Appendix D3). As indicated by the results, the statistical significance and direction of the effects do not change substantially.

Furthermore, I seek to account for the possibility that authoritarian governments who rely on repression might seek to control internet access through state ownership rather than preventing foreign companies from investing in the telecom sector (Howard, 2011). Domestic state ownership and foreign ownership are highly negatively correlated (see Appendix D4), and while the share of domestic ISPs owned by the state is relatively high (M = 0.37), the share of domestic private firms is extremely low (M = 0.07). I re-run all models but include the share of ISPs majority state-owned as additional control variable (Appendix D5). In these models, all predictors remain fairly stable, suggesting that the results are not driven by the governments' motivation to keep ISPs state-owned rather than dismissing FDI.

Table 7. Results from linear mixed models

	Share of foreign investors		… with headquarter in autocracies		… with headquarter in democracies	
	Model 1	Model 2	Model 3	Model 4	Model 5	Model 6
Repression	0.02 (0.01)*	0.03 (0.01)**	0.02 (0.01)**	0.03 (0.01)**	0.00 (0.01)	0.01 (0.01)
Legislative chambers	0.03 (0.01)**	0.03 (0.01)*	0.01 (0.01)	0.01 (0.01)	0.02 (0.01).	0.02 (0.01).
Corruption		0.05 (0.02)**		0.03 (0.02)*		-0.02 (0.02)
Military control		-0.00 (0.01)		0.01 (0.01)		-0.01 (0.01)
Hereditary control		-0.16 (0.05)*		-0.05 (0.03).		-0.10 (0.04)*
Log GDP per capita		0.13 (0.02)***		0.05 (0.02)*		0.07 (0.02)**
GDP per capita growth		-0.02 (0.01)*		-0.01 (0.01)		-0.01 (0.01)
Rents natural resources (% of GDP)		0.02 (0.02)		0.03 (0.02)*		0.01 (0.02)
Total population		0.06 (0.05)		-0.05 (0.03).		0.07 (0.04)
Rural population (% of total)		0.11 (0.05)*		0.03 (0.03)		0.14 (0.04)***
Trade (% of GDP)		0.04 (0.01)*		-0.01 (0.01)		0.04 (0.01)**
year	0.01 (0.00)***	0.01 (0.00)*	0.00 (0.00)***	0.00 (0.00)	0.01 (0.00)***	0.01 (0.00)***
(Intercept)	-21.03 (2.11)***	-9.90 (4.60)*	-8.46 (2.17)***	-4.29 (3.82)	-19.65 (1.94)***	-20.66 (4.11)***
R^2	0.79	0.86	0.52	0.56	0.76	0.82
No. of observations	683	582	683	582	683	582
No. of countries	44	41	44	41	44	41

Note: ***p <.001; **p < .01; *p < .05; .p < .1; all predictors are z-standardised.

4.6 Discussion

The results provide preliminary insights into the drivers of FDI in the telecom sector in African autocracies. Overall, my findings suggest that the extent to which authoritarian governments rely on repression and co-optation of the opposition shapes their openness to FDI in the telecom sector. In addition, governments appear to make strategic decisions on whether to accept FDI depending on the investor's origin.

More repressive authoritarian regimes seem to be more open to foreign, in particular foreign-autocratic, investors. This finding supports prior studies indicating that authoritarian regimes are keen on expanding internet infrastructure (Rød & Weidmann, 2015; Stier, 2017). My results highlight that, to maintain control over internet access, repressive regimes may be more open to FDI in the telecom sector from companies they consider to be willing to restrict or manipulate internet access (Freyburg & Garbe, 2018). For example, Burundi is marked by high levels of repression and international involvement in the telecom sector. The telecom sector is largely privatised, with five out of the six ISPs active between 2000 and 2019 owned by foreign investors, after the government opened the telecom sector to private investors in the late 1990s (CIPESA, 2020). The two biggest ISPs, in terms of market share, are both owned by foreign-autocratic investors.[48] ISPs in Burundi were highly invested in both censorship of access to internet content deemed critical of the government and surveillance of individuals by providing customer data to the government (ibid.). Both foreign-autocratic ISPs are likely to use Deep Packet Inspection (DPI) to block or censor internet access (Xynou & Filastò, 2020), a technology that requires expensive hardware. This example highlights that ISPs owned by foreign-autocratic investors may be complicit in controlling internet access.

Authoritarian regimes, in which power is shared with opposition forces, seem generally more open to FDI. As indicated by the results, authoritarian legislatures seem to encourage FDI from democratic (rather than authoritarian) investors, supporting the assumption that legislative institutions in autocracies can have the function to put pressure on the government. However, the effects are rather small and call for a more thorough understanding of how legislative institutions shape FDI policies. Recent scholarly work emphasises that whether or not legislative institutions can shape policy outcomes should depend on a number of factors, such as citizen demands for policy reforms (Truex, 2020) or the relative involvement of opposition parties (Simison, 2020). Therefore, whether and how legislatures can put pressure on the

[48] The biggest provider in terms of subscribers Econet Leo, 100 per cent owned by Zimbabwean investor Strive Masiyiwa, entered the Burundian market in the early 2000s. In 2014, Econet took over privately-owned U-Com after the company failed to comply with the government's regulatory charges (Rufyikiri, 2016). In 2014, the military-owned Vietnamese operator Viettel acquired a license to enter the Burundian market (*Viettel wins mobile concession in Burundi*, 2014) under preferential agreements such as tax exemptions (Rufyikiri, 2016).

incumbent to grant access to FDI, and discriminate against specific investors based on their origin, remains an interesting question beyond the telecom sector.

An important caveat of this study is that its research design does not allow for establishing causal relationships. It is unclear whether those regimes relying on repression and co-optation are more (or less) hesitant to accept foreign investors or whether foreign investors are more (or less) hesitant to invest in said countries. Prior research argues that formal institutions, such as legislatures, provide a signal to foreign investors that executive power is constrained and investments are less prone to the risk of expropriation (e.g. Bastiaens, 2016; Moon, 2019). However, these studies commonly neglect the strategic interests of host governments to attract FDI from different types of investors. Ideally, future studies can draw on longer time-series to better account for the lag in the effects of co-optation and repression on FDI (and vice versa).

The results point to potential mechanisms through which domestic institutions shape a government's openness to different foreign investors. To further scrutinise these mechanisms, future studies may pay additional attention to the role of foreign-autocratic state-owned enterprises (SOE), specific policies related to FDI, and the role of market-specific characteristics.

First, as in the case of Burundi, ISPs owned by foreign-autocratic investors are often owned by SOE, including SOE from Libya, Saudi Arabia, or Vietnam, potentially opening the door for more direct diplomatic channels. Uganda, for instance, which is marked by high levels of state repression under the ruling party National Resistance Movement (Tangri & Mwenda, 2008), sold the majority of the incumbent fixed-line provider UTL to the Libyan state-owned company LAP Green in 2006 reflecting "the cordial relations between [Ugandan president] Museveni and Libyan leader Muammar Gaddafi" (Wairagala, 2009: 15) at that time. Future studies examining the link between companies in authoritarian regimes and foreign-autocratic investors should pay particular attention not only to the investor's origin but also to the owner's identity, notably whether the investing entity is a state-owned enterprise (Jones & Zou, 2017) and the degree to which the state is involved in the company's management (Sallai & Schnyder, 2020).

Second, it seems important paying attention to specific policies that prevent or encourage FDI in the telecom sector. In Eritrea, for instance, FDI is generally discouraged. In 2013, the government sold some shares of EriTel, the only and until-then fully state-owned ISP operating in Eritrea, exclusively to Eritrean investors (Reuters, 2013). Other African countries have established indirect barriers to foreign investors, such as high licensing fees. A focus on sector-specific policies appears to be a promising way to better understand how governments encourage or discourage FDI in the telecom sector and may provide an opportunity to study the role that legislative institutions can play in shaping FDI policies.

Third, this study neglects differences across ISPs vis-à-vis their market position and their hierarchy in the infrastructure. Even governments keen on repressing freedom to speech might be willing to accept FDI in small ISPs that do not provide internet services to the vast population. Despite restricting the sample to ISPs that are members of the GSMA, there may be crucial differences across companies in their market dominance. Besides, some ISPs, even if they are not dominant market actors, may run important infrastructure, which allows them to effectively control the traffic routed by other ISPs (Warf, 2012). In Cameroon, for instance, the state-owned provider CamTel runs large parts of the national internet backbone, which allegedly facilitated a politically motivated internet shutdown in 2017 (Dahir, 2017). Future studies may investigate whether the market position of a company influences a government's decision to sell its stakes to foreign investors.

4.7 Conclusion

In this paper, I study the political drivers of foreign investment in the telecom sector in autocracies. My findings suggest that more repressive regimes are more open to FDI in the telecom sector, notably from other authoritarian regimes. At the same time, governments that share power with opposition forces may face pressure to accept FDI from democratic rather than authoritarian regimes. Thus, my findings highlight the potentially conflicting factors that shape FDI policies by authoritarian incumbents. While this study focuses on sector-specific investments in internet infrastructure, the insights may apply to other sectors, in which the ruler cannot afford to lose control over production and distribution.

My study contributes a novel perspective to the discussion about the determinants of FDI in authoritarian regimes. In contrast to most research on FDI in autocracies, I do not focus on the motivations of foreign investors, but on factors that shape a government's decision to attract FDI from abroad. Thereby, I highlight that authoritarian governments make strategic decisions on whether to accept FDI that likely depend on internal factors.

Finally, my study contributes to the growing literature on authoritarian collaboration. To reap the benefits of internet access while avoiding associated risks, authoritarian rulers may strategically encourage investment in internet infrastructure from like-minded regimes. Most of the existing research on authoritarian collaboration has focused on China's economic expansion, its logic, and its consequences (e.g. Taylor, 2006; Fijałkowski, 2011). My results demonstrate that repressive regimes in Africa attract FDI from autocracies all over the world, including Vietnam, Qatar, or Russia, providing insights into modern authoritarian collaboration beyond China.

BLOCKING THE BOTTLENECK: INTERNET SHUTDOWNS AND OWNERSHIP AT ELECTION TIMES IN SUB-SAHARAN AFRICA

Joint work with Tina Freyburg

Published in *International Journal of Communicatio*n, 2018, Vol. 12[49]

Abstract

The Internet is often portrayed as offering new communication and information channels resistant to state control because of its decentralisation. At the same time, the Internet relies on a hierarchical physical infrastructure that, connecting the individual customer to the Internet, provides states with control opportunities. We argue that ownership of the Internet infrastructure, in particular Internet service providers (ISPs), is critical to understanding state Internet control because most direct forms of control require ISPs to comply with government requests. Using qualitative comparative analysis, we systematically link documented Internet shutdowns in sub-Sahara African countries to configurations of ISP state majority ownership, regime type, and election violence. The results support a positive relationship between a temporary halt of Internet provision and ISP majority ownership by authoritarian states when facing election-related violence. Our study underlines the importance of varying ownership structures in explaining political effects of Internet penetration, including its role in challenging authoritarian rule.

[49] Please cite as: Freyburg, T., & Garbe, L. (2018). Authoritarian practices in the digital age| Blocking the bottleneck: Internet shutdowns and ownership at election times in Sub-Saharan Africa. *International Journal of Communication*, 12, 3896–3916. Note that the text is identical to the published version, although the citation style has been adapted and appendices are provided at the end of this dissertation.

5.1 Introduction

"Victory!" the international non-profit digital-rights advocacy group Access Now exclaimed in August 2016. "President of Ghana says no to Internet shutdowns during coming elections" in December (Olukotun, 2016). Such were the times that even Africa's most stable democracies considered intentionally restricting public Internet access during election periods. In 2015–6, in half of the sub-Sahara African (SSA) countries in which presidential or parliamentary national elections were held, the government ordered internet shutdowns as voters headed to polling stations. When in Gambia citizens were called to vote for a president in 2016, access to mobile internet and text messaging was completely cut off on the polling day and had already been hampered during the electoral campaign. News reporting in the media and various digital rights blogs suggest a positive relationship between elections and shutdowns of internet services in electoral authoritarian regimes (Odhiambo, 2017). Here, incumbents are commonly said to justify these politically motivated interruptions by citing national security concerns and fears of the spread of fake election results. Commentators agree, however, that this brute-force method of cutting all access is predominantly meant to prevent opponents from organising protests or reporting election malfeasance.

Although shutting down the internet during polls is a popular tool of African rulers, the temporary interruption of the flow of digital-based information and communication is no default option. Overall, it appears that democratic rulers refrain from interrupting the flow of digital information during election times. When it comes to Africa's autocracies, however, the picture appears mixed. Uganda, Burundi, Ethiopia, Chad, and the Republic of Congo interrupted access to the Internet during election times. In the Central African Republic (CAR), in turn, in which instability and sectarian violence marked the electoral chaos in 2015–6, digital communication and information continued to flow over the whole lengthy electoral period (Agence France-Presse, 2016). The observer might add that the parliamentary and presidential elections as such took place peacefully in CAR; hence, the incumbent might have felt less pressure to block access. The absence of electoral conflict alone, however, appears insufficient to explain cases in which we see no shutdown of internet services in times of authoritarian elections. The 2015 Togolese presidential elections, for instance, took place without major incidents, but the incumbent president Gnassingbé still experimented with disrupting the internet.

In this article, we argue that ownership of the physical internet infrastructure, in particular internet service providers (ISPs), is key when it comes to explaining incidences of internet shutdowns. Governments typically do not directly restrict internet access but order telecom operators and other autonomous systems (ASs) that provide internet to halt their services. Because ISPs provide "last-mile" connection to end users, governments rely on their cooperation if they intend to cut access to particular services or entire (sub-)

networks. Yet existing political science scholarship largely views the internet not only as a technical "black box" but also as a resource that governments have at their free disposal. It hence tends to treat the structure of ISP ownership as a constant rather than a variable.

We, in contrast, view internet services as a good, owned by different private and public actors with potentially diverging interests, and consider the complex physical infrastructure essential for its provision. Few studies have identified varying ownership arrangements as crucial for the economic and political consequences of Internet penetration (on corruption and growth, e.g., Dasgupta, Lall, & Wheeler, 2005; on state repression, e.g., Milner, 2006; Pallin, 2017). Given that most of these studies focus only on specific countries and short time periods, or exclusively rely on descriptive assessments, the findings produced can be seen as limited in their power both to explain and to generalise. Consequently, the relationship between ownership and political outcomes of Internet service provision, including its temporary interruption at times of political contestation, has largely been ignored.

Although a few studies suggest that strategies of political repression such as censorship and (situational) disruption are implemented more effectively if the government is able to control the infrastructure (Weber, 2011), the role of telecom companies, in particular, private intermediaries in enabling or disabling network disruptions, has not yet been systematically explored (Corrales & Westhoff, 2006; Weidmann, 2015). Drawing on insights from studies of the political effects of varying ownership over natural resources (Luong & Weinthal, 2010; Wegenast & Schneider, 2017) and media (Stockmann, 2013), and borrowing the concept of techno-politics from the history of technology tradition (Hecht, 2001; Hughes, 1993), we expect the occurrence of Internet shutdowns to coincide with specific ISP ownership arrangements. Precisely, we contend that the temporal interruption of internet services is facilitated if the state is the majority owner of at least one ISP operating on its territory; by the same token, it should be more challenging for a government to make ISPs comply with its request if the majority of ISPs on its territory is in private hands. This relationship should be even more prominent in times of electoral conflict that may be perceived by the incumbent ruler as threatening re-election and hence political survival.

Empirically, we systematically investigate the link between state majority ownership of ISPs in a country and the politically motivated temporal interruption of access to the internet during contentious events, namely the 33 presidential and parliamentary elections in SSA between 2014 and 2016. To examine whether state majority ownership of ISPs is associated with internet shutdowns, in particular at times of election violence, we use a novel data set of ISP ownership (Freyburg, Garbe, & Wavre, 2021) that we combine with documented internet shutdowns (our outcome), plus a binary measure of (nongovernmental) election violence, as compiled by the global Varieties of Democracy (V-DEM) data set (Coppedge *et al.*,

2017a), and a dichotomous measure of a country's regime type based on Polity IV (Marshall, Gurr, & Jaggers, 2017).

We focus on SSA because this region of the world is especially marked by economic and political transitions that we expect to drive cross-national variation in ISP ownership. Most of them have recognised investment in ICT as crucial driver of economic growth (Albiman & Sulong, 2016). Privatisation has often diversified the market by reducing the traditionally leading role of the state and increasing private-sector involvement. Plus, the third wave of democratisation has been particularly prominent in SSA; still, countries show varying degrees of political liberalisation (Levitsky & Way, 2010). Democracy is the norm today, albeit imperfect, with most governments coming to power through competitive elections, and most rulers following civilian rather than military careers. Yet the struggle for democracy has not been entirely successful; major reversals still appear frequently throughout the region. And, crucially, internet shutdowns have become a particularly popular tool, especially for autocracies during times of elections.

In the following, we first conceptualise internet shutdowns and point to their relevance during election periods. Subsequently, we explain the role of ISPs in disrupting internet services and why their ownership matters for the (non-)occurrence of shutdowns. We then derive propositions regarding the link between ISP state majority ownership and internet shutdowns that we then explore based on a systematic qualitative comparative analysis of all elections in SSA countries in 2014, 2015, and 2016. Our findings suggest that ISP ownership structure varies both within and across countries, and that such patterns of variation can indeed explain the (non-)occurrence of shutdowns. Finally, we discuss the role of ownership of internet infrastructure more broadly and appeal for a shift in the unit of analysis when doing research on internet control.

5.2 Internet shutdowns in election times

Elections are generally regarded as procedural instrument by which political authority and legitimation is periodically and formally granted to elected representative(s). Yet holding elections does not mean that a country is democratic. In liberal democracies, elections serve as viable means of ensuring the orderly process of alternation in power; in authoritarian regimes, however, they are commonly established as a means by which the incumbent rulers hold onto power. Here, "elections are generally about access to state resources, rather than a competition over the rules of the game" (Gandhi & Lust-Okar, 2009: 412). In any case, calling elections is risky, given the uncertainty regarding their outcome; "the succession moment is normally the most dangerous recurring one in all political systems" (Rapoport & Weinberg, 2000: 15; Hafner-Burton, Hyde, & Jablonski, 2014: 155). It requires that an incumbent accepts electoral defeat

and actually steps down from power—a behaviour, that is not a given in nondemocratic or democratising contexts.

In consequence, authoritarian rulers often, but not always, manipulate elections to ensure their prolonged rule. They seek to incarcerate key opposition leaders and their supporters, ban their parties, and repress the media, among others (Gandhi & Lust-Okar, 2009). In their fear of losing power as the result of an election, they willingly risk the outbreak of conflict, if not violence. On the one hand, authoritarian incumbent leaders and ruling party agents often employ or threaten violence against opposition parties and their supporters, before or after elections. On the other hand, electoral malpractice—including voter intimidation, vote buying, and ballot fraud—is known to undermine public confidence in the credibility of elections; hence, opponents may be motivated to resort to conflict, violence, and threat as a means to determine, delay, or otherwise influence the results of the elections (Hafner-Burton, Hyde, & Jablonski, 2014: 154). In short, election violence and fraud often trigger protest against the handling or outcome of the election by opposition forces; such protests can, in turn, provoke the use of more state violence in an effort to dissolve public dissent and stay in power (Tucker, 2007).

Yet opposition forces face a typical collective action problem in authoritarian contexts. Mass protests are often prevented by the inability of opponents to effectively organise and communicate, that is, to locate and contact appropriate participants, to motivate them to make private resources publicly available, to persuade them to remain involved despite short-term setbacks and long-term risks, and to coordinate their efforts productively. Still, it is not simply the likely punishment for dissent given the degree of control and repression that prevents individuals from taking to the streets and challenging the political authority and legitimation of the incumbent ruler. Authoritarian regimes typically restrict traditional broadcast and print media in ways that make it difficult for citizens to coordinate effective collective opposition or to express their dissent in the public sphere (Gandhi & Lust-Okar, 2009; Tucker, 2007).

In the digital age, information and communication technologies (ICT), in particular the internet, are said to help to overcome the coordination problem in at least two ways (Rød & Weidmann, 2015). First, the internet provides opportunities to expose human rights violations and political misbehaviour, such as electoral misconduct, and inform both internal and domestic audiences about what is happening. At the same time, it lowers the costs of acquiring independent information, including about a regime's stability and repressive capacities, the success of protests against related grievances, and how things ought to be done, such as the orderly conduct of elections elsewhere. Second, the internet can facilitate the mobilisation for and organisation of protests under authoritarian rule in that it allows the transmission of information directly to like-minded citizens. It can hence be a powerful tool for opposition elites seeking to spread their political agenda and/or organise antiregime demonstrations. In short, according to these

observers, the internet can undermine authoritarianism by offering new communication channels that are "fundamentally resistant to state regulation, reducing a state's capacity for repression by hindering its ability to control the flow of information and political communication" (Kelly Garrett, 2006: 220).

At the same time, scholars recognise the incumbents' attempts to combat protests using ICT, or enabling its use by protesters (Deibert *et al.*, 2008; Ten Eyck, 2001; Weber, 2011). One of the most extreme forms of rendering control over digital information and communication are internet shutdowns (Howard, Agarwal, & Hussain, 2011), that is, the "intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location" (Access Now, 2016: para. 1). These temporary blackouts have severe consequences for opposition groups' capabilities to effectively use digital communication and information channels. For instance, they prevent ordinary internet users from accessing any websites, including online news portals or social media platforms; protesters can also no longer use coordination tools, such as online mapping services, like Google Earth and Google Maps, which are handy to effectively navigate through militarily occupied zones. They also cripple The Onion Router, known as TOR, an anticensorship tool that technical experts and activists often use to circumvent social media blocks.

How can a state go about shutting down the internet? Despite its decentralisation, the internet relies on some fairly significant hierarchical structures, mostly for the sake of efficiency. It is specifically the physical infrastructure that, connecting the individual customer to the internet, is key to controlling the flow of digital information and communication. Service providers with control over the physical infrastructure can extend that control into applications and content. Eventually, a digital video can only be posted to a website in cyberspace, such as a social media platform like Facebook, as long as the computers remain connected to the internet. Hence, a government's ability to control the internet primarily depends on its control of the ISP that grants internet access to customers on its territory. There are different technical ways that ISPs can comply with a government request to disrupt the internet. For instance, the ISP can simply power down devices, change the routing tables in such a way that packages of data cannot reach their goal, or stop resolving addresses that belong to a certain domain name system, such as that of the concerned country (e.g., .ug for Uganda). In short, while access to the internet and its use depend critically on the permission and support of the domestic government (Milner, 2006), governments cannot directly restrict internet access, but rely on the compliance of ISPs to halt their services.

5.3 State control and ownership of the internet's physical infrastructure

Scholarship on the relationship between technologies, governments, and other political actors that attempt to influence technology adoption established the argument that technology has politics. Challenging the supposed neutrality of technical artefacts, such as the provision of the internet, the concept has been used to "refer to the strategic practice of designing or using technology to constitute, embody, or enact political goals" (Hecht, 2001: 256). Eventually, "arrangements of technical architecture are inherently arrangements of power" (DeNardis, 2012: 721). Our research borrows from this strand of literature by taking into consideration how technology can become an instrument of politics and how technological opportunities can shape political ambitions and actions (Gagliardone, 2016). From this perspective, technical artefacts such as the provision of internet services—or its interruption—can be seen as vehicles for exercising power.

Indeed, the connection of an ISP to the rest of the network presents a bottleneck that is relatively easy to cut off or seize control over. The internet connects thousands of ASs that are tasked with routing; that is, ASs manage unique sets of customers' internet protocol (IP) addresses to and from which they carry traffic. We focus on ASs that are administered by commercial ISPs that operate on the given state territory and provide internet connectivity to the larger population. They can be seen as centralised points of control or "gatekeepers" of the internet as they control the gateway through which data flow in and out (DeNardis, 2014, 2011).

Although we acknowledge that privately owned ISPs may vary in their willingness to follow government orders to shut down the internet, in this article, we focus on the role of state majority ownership as the most immediate, physical form of state control. Eventually, both legal or regulatory control through the threat of revoking the license to operate as well as technical control over the traffic transiting the physical lines become obsolete if (at least considerable parts of) the physical infrastructure is in the hands of the state. We expect a company's commitment to comply with a government's request to shut down its services to be decisively determined by its ownership, notably, facilitated by state majority ownership and hindered otherwise.

Note that the ownership of a company (i.e., shareholders) is different from the management of the company (i.e., the CEO).[50] Some scholars see a company principally as a machine for making profits, where

[50] The border between ownership and management of a company can be blurred, such as in the case of family enterprises (Lemos & Scur 2018).

owners have no incentive to get involved in the management because of the uncertainty of benefits from doing so (Berle & Means, 1933). This strand of literature tends to disregard the role of ownership in management. Others find that control is well exerted by the owners, in particular through their voting rights but also through informal influence, such as during general assemblies or informal meetings with the management teams. According to this position,

> The role of shareholders is to determine all questions that are not routine, that cannot be decided by management because they are relevant to the relationship between the company and the capital market, and these include all fundamental matters affecting it. (Leech, 2013: 476)

We follow the second line of understanding and acknowledge that a company's owner can have substantial influence on its policies by actively engaging with management and voting their shares. We expect ISP majority ownership to be associated with the temporary interruption of access to the internet in autocracies (in contrast to democracies), in particular if election periods are marked by violence.

5.4 Research design and operationalisation of variables

Focusing on SSA, we selected all countries[51] with presidential or parliamentary elections in 2014, 2015, or 2016, according to data provided by the Varieties of Democracy project (V-Dem; Coppedge *et al.*, 2017a). We limit our sample to countries during electoral periods, to hold the chances for mobilisation (and hence shutdowns) constant. Our analysis covers the entire population, that is, all SSA countries where national elections took place (N = 33); any potential bias in case selection is thereby minimised. As Table 8 demonstrates, the occurrence of internet shutdowns at election times varies, with elections being accompanied by shutdowns in 10 of these 33 cases, as does the presence of ISP state majority ownership, the occurrence of electoral violence, and the regime type (for raw data, see Appendix E1).

To probe the plausibility of our argument, we use crisp-set qualitative comparative analysis (csQCA), which is an analytical technique to uncover empirical patterns in data by examining set-theoretic relationships between causally relevant conditions following a deterministic logic of causation (Schneider & Wagemann, 2010). This research method is adequate because we are interested in the effect of a dichotomous condition (state majority ownership vs. no state majority ownership) on a dichotomous outcome (occurrence vs. non-occurrence of an internet shutdown). CsQCA links binary-coded conditions and outcomes through set-theoretical relations by classifying their presence (= 1) and absence (= 0) for each case. Based on Boolean methods of logical comparison (i.e., the algebra of logic and set-theoretical

[51] Except for São Tomé and Mauritius, because no data on ISP ownership are available for the African islands, but Madagascar.

relationships), csQCA is therefore appropriate not only to check the necessity and sufficiency of conditions but also to identify more than one path leading to the same outcome.

Table 8. Calibrated data

Case	ISP State Ownership	Autocracy	Electoral Violence	Internet Shutdown
Benin 2015	1	0	0	0
Benin 2016	1	0	0	0
Botswana 2014	1	0	0	0
Burkina Faso 2015	0	0	0	0
Burundi 2015	1	1	1	1
CAR 2015	0	1	0	0
CAR 2016	0	0	0	0
Chad 2016	1	1	1	1
Djibouti 2016	0	1	1	1
Equatorial Guinea 2016	1	0	0	0
Ethiopia 2015	1	1	0	1
Gabon 2016	1	1	0	1
Gambia 2016	0	0	1	1
Ghana 2016	1	1	0	1
Guinea 2015	0	0	0	0
Guinea-Bissau 2014	1	0	0	0
Ivory Coast 2015	0	0	0	0
Ivory Coast 2016	0	0	0	0
Lesotho 2015	1	0	0	0
Malawi 2014	0	0	0	0
Mauritania 2014	0	0	0	0
Mozambique 2014	0	1	0	0
Namibia 2014	1	0	1	0
Niger 2016	1	0	0	0
Nigeria 2015	1	0	0	0
Republic of Congo 2016	1	0	0	0
South Africa	1	0	0	0
Sudan, North 2015	0	1	1	1
Tanzania 2015	1	0	1	0
Togo 2015	1	1	0	1
Uganda 2016	0	1	1	1
Zambia 2015	1	0	0	0
Zambia 2016	1	0	1	0

Our outcome is the occurrence or non-occurrence of an internet shutdown during election periods (i.e., shortly before, during, or shortly after polling day). Defined as "intentional disconnections of digital communications by government authorities" (Wagner, 2018: 3918; Access Now, 2016), shutdowns can be considered as an extreme form of censorship. Looking specifically at politically motivated internet shutdowns during election times enables us to differentiate simple technical failures from "the intent of a governmental actor to disconnect networks" (Wagner, 2018: 3919). Because governments now have the ability to apply shutdowns and other restrictions in a more targeted manner, and authorities commonly cut off specific regions in response to local instability, dissent, or insecurity, we apply a more comprehensive understanding of internet shutdowns than Ben Wagner's. Specifically, we count as a shutdown any considerably disrupted access to the internet in a country, including the targeted blocking of particularly

prominent global platforms commonly used for mobilisation and campaigning purposes (e.g. WhatsApp, YouTube, Facebook, Twitter), and the intentional slowing down of connections or of a specific protocol or resource (i.e. "throttling"; Aceto & Pescapé, 2015). Note that full internet shutdowns are often employed at a sub country level (e.g. state, city, province, neighbourhood) and may not involve all ISPs providing internet services within a state's territory. Data come predominantly from the Access Now platform in the context of its #KeepItOn initiative and is complemented with information from the global news database Factiva. Restricting the time period of interest to the year of the election, we used the following search strings for each country: *country AND elections AND [internet OR access] AND [shutdown OR blocked]*.

In two of the cases, 2015 Ethiopia and 2016 Equatorial Guinea, the occurrence of an internet shutdown was not as clear as in the rest. Both countries feature in several lists as among the most censored countries in the world; internet and mobile phone networks are repeatedly disrupted, and social media, circumvention tool websites, and communications platforms are temporarily blocked time and again (Freedom House, 2015; U.S. Department of State, 2017b, 2017a). Because both countries constantly face a high level of internet filtering and manipulation, it is difficult to assess whether the blocking of access to the internet in the run-up to the general elections is directly linked to the elections. As the given sources support a temporary halt of services, we code an internet shutdown as present for both.

Our main condition of interest is state control of ISPs by means of majority ownership. We draw on the definition of owners as pivotal actors based on the size of owned shares (Leech, 2013). By virtue of controlling more than half of the voting interests in the company, the majority shareholder has decisive influence in the business operations and strategic direction of the company. Setting the full control threshold conservatively, we avoid any potential inconsistencies emerging from the competition for control. We distinguish between ISPs for which the state holds the majority of outstanding shares (i.e., 51% or more), and those for which it holds fewer or no shares. States tend to be the majority shareholder of those ISPs that provide the national internet backbone and may operate key infrastructure within a country that is used by other ISPs as well (Warf, 2012). In Cameroon, for instance, the state-owned ISP CamTel runs crucial parts of the national fibre backbone on which other providers rely to service their subscribers. Even if the state is the majority shareholder of only one small ISP out of many operating on its territory, then by having direct access to key parts of the internet infrastructure, it can paralyze the provision of internet access in a country. Against this, we code this condition with 1 if there is at least one ISP of which the state is the majority shareholder, and with 0 otherwise.

We draw on an original data set covering all telecommunications companies that hold official state licenses to operate cables and provide internet services (Freyburg, Garbe, & Wavre, 2021). Data come from financial-analysis tools (e.g., Eikon [http://eikon.thomsonreuters.com] and Orbis

[https://orbis.bvdinfo.com]), specialised blogs (e.g., Research ICT Africa [https://www.researchictafrica.net]), news websites such as All Africa (http://allafrica.com) and Quartz Africa (https://qz.com/Africa), and Bloomberg Snapshot repositories (https://www.bloomberg.com). This information is triangulated with the annual reports provided by the telecommunications companies and data from market research and analysis companies, in particular, African Telecommunications News (AMETW; https://www.africantelecomsnews.com) and TeleGeography (https://www.telegeography.com).

We further include a country's regime type. Existing studies claim the manipulation of internet access to be more prevailing in autocracies (Deibert *et al.*, 2008; Howard, Agarwal, & Hussain, 2011). To determine categorically whether a regime is an autocracy or a democracy, we use Ulfelder (2007) two-component measure that corresponds to common understanding of an electoral democracy. It has not only been shown to be particularly useful for Africa (Bogaards, 2012) but also avoids conceptual overlaps with our third condition, election violence. The selected Polity IV component variables are executive recruitment (EXREC) and the competitiveness of political participation (PARCOMP; Marshall, Gurr, & Jaggers, 2017). In line with Ulfelder (2007: 1001), we identify a regime as democracy (= 0) if it provides "some contestation in the selection of the chief executive (EXREC > 5) and do[es] not substantially restrict political participation (PARCOMP >2 or = 0)"; when a regime falls short on one or both dimensions, we categorise it as autocracy instead (= 1). By determining the democratic minimum for each of the Polity component variables, we avoid not only the problem of concept-measure inconsistency but the logic behind the minimum as aggregation rule also matches the general configurational nature of our study.[52]

Our third and last condition is election violence. Elections in SSA are particularly delicate, with many countries still in a difficult process of transition where elements of democratic participation are intertwined with authoritarian rule and political repression. According to Lindberg (2004), 80% of African elections were accompanied by some kind of election-related violence in the late 1990s and early 2000s. To account for the role of violent protest, we use the V-Dem (v2elpeace) variable that captures whether "the campaign period, election day, and postelection process [were] free from violence related to the conduct of the election and the campaigns (but not conducted by the government and its agents)" (Coppedge *et al.*, 2017b: 92). We use the ordinal variable variant and code "widespread violence," "significant levels of violence," as well as "some outbursts of limited violence" with 1, and the remaining two categories ("only a few instances of isolated violent acts," "no election-related violence") with 0.

[52] ISPs are not more likely to be majority-owned by the state if the country is ruled autocratically, $r(31) = -.24$, $p = .81$.

5.5 Results

5.5.1 ISP state ownership and internet shutdowns in Africa

We use crisp-set QCA to establish whether particular configurations of conditions, namely national similarities and differences in internet ownership structure, election violence, and regime type, can be linked to the (non-)occurrence of internet shutdowns. Table 9 and Table 10 show the parsimonious solution based on our dichotomised data. All the conditions in the parsimonious solution generally show the expected direction. For each outcome, the occurrence (= positive) and the non-occurrence (= negative) of an internet shutdown, there are two sufficient conjunctions, each covering part of the empirically observed configurations. They are displayed with a logical OR relation, either one being sufficient for some of the configurations, but both are necessary to cover all of them.

The results of the csQCA support our general expectations. As to the negative outcome (*N* = 23), if the state holds no majority of shares from at least one ISP, then we also observe no internet shutdown in the absence of election violence. That is, the absence of election violence and the absence of ISP state majority ownership are together sufficient for the absence of internet shutdowns, independent of the regime type (39%). Plus, if the state is majority owner but democratically constituted, then we also observe no internet shutdowns during election times, regardless of how violent they are. We therefore observe several democracies, 14 to be exact (61%), in which ISPs are majority-owned by the state but no internet shutdowns occurred during election times (see Appendix E2).

Table 9. csQCA output—parsimonious solution for internet shutdowns (negative outcome)

Cases	Conditions			Coverage	Consistency
	ISP State Ownership	*Autocracy*	*Electoral Violence*	*Raw/Unique*	
Burkina Faso_2015, CAR_2016, Ghana_2016, Guinea_2015, Ivory Coast_2015, Lesotho_2015, Malawi_2014; CAR_2015, Mauritania_2014	○		○	.39	1.0
Benin_2015, Benin_2016, Botswana_2014, Djibouti_2016, Guinea-Bissau_2014, Ivory Coast_2016, Namibia_2014, Niger_2016, Nigeria_2015, Zambia_2015; Mozambique_2014, South Africa 2014, Tanzania_2015, Zambia_2016	●	○		.61	1.0
Solution	isp * violence + ISP * autocracy <=> shutdown			1.0	1.0

Note: Empty circles depict the absence of the condition, shaded circles its presence. In line with Boolean operators, uppercase letters indicate the presence of an outcome or a condition, and lowercase letters indicate their absence; * designates logical AND, while + designates logical OR, and the logical (set-theoretical) relation <=> signals both necessity and sufficiency; solution coverage and consistency (inclusion) for both paths is 1.000; all cases are uniquely covered.

If we turn to the positive outcome ($N = 10$), again, one solution with two conjunctions is suggested. If the state is the majority owner of at least one ISP and an autocracy, then we observe an internet shutdown, regardless of election-related violence (60%). However, if the state is no majority shareholder but elections are marked by violence, then we can observe shutdowns, too. The latter conjunction refers to four cases, namely Gabon in 2016, the Republic of Congo in 2016, North Sudan in 2015, and Uganda in 2016—that is, three autocracies but one democracy: Gabon. In other words, and unexpectedly, a democracy in which the state is no majority shareholder of any ISP company shows a positive outcome. Global democracy measures, notably Freedom House's Freedom in the World and Polity's Institutionalised Autocracy, rate 2016 Gabon as autocracy (i.e., with "not free" and at −0.5, respectively), however. We therefore re-run our analysis with Gabon recoded as autocracy; the dominant tendency remains unchanged (Appendix E3).

Still, the remaining cases—Sudan (North) 2015, the Republic of Congo 2016, and Uganda 2016—work against our expectation that state majority ownership of at least one ISP is necessary to explain the occurrence of internet shutdowns. We therefore zoom in to the ISP ownership structure of two of these cases, Uganda and the Republic of Congo, to better understand the relationship between the state and the ISP on its territory.[53] What features might have facilitated ISP compliance with the government's request to interrupt the provision of internet services?

Table 10. csQCA output—parsimonious solution for internet shutdowns (positive outcome)

Cases	Conditions			Coverage	Consistency
	ISP State Ownership	*Autocracy*	*Electoral Violence*	*Raw/Unique*	
Equatorial Guinea_2016, Ethiopia_2015, Gambia_2016, Togo_2015; Burundi_2015, Chad_2016	●	●		.60	1.0
Gabon_2016; Republic of Congo_2016, Sudan-North_2015, Uganda_2016	○		●	.40	1.0
Solution	ISP * AUTOCRACY + isp * VIOLENCE <=> SHUTDOWN			1.0	1.0

Note: Empty circles depict the absence of the condition, shaded circles its presence. In line with Boolean operators, uppercase letters indicate the presence of an outcome or a condition, and lowercase letters indicate their absence; * designates logical AND, while + designates logical OR, and the logical (set-theoretical) relation <=> signals both necessity and sufficiency; solution coverage and consistency (inclusion) for both paths is 1.000; all cases are uniquely covered.

[53] The ownership structure in North Sudan resembles the Congolese one, with four licensed ISPs owned by private investors from emerging or oil-rich Middle East economies, namely Canartel, MTN Sudan, Sudatel, and Zain Sudan.

5.5.2 The Republic of Congo and Uganda: The role of private ownership

Both the Republic of Congo's 2016 presidential election and Uganda's 2016 general elections were marked by internet shutdowns in the context of election violence, but no major state involvement in ISP. According to the French news agency Agence France-Presse, Congo's interior minister Raymond Mboulou urged the ISP on the country's territory to shut down their services for "reasons of security and national safety" (*Congo holds elections under telecom blackout*, 2016). The country experienced an outbreak of election violence after president Denis Sassou-Nguesso secured a third term in the presidential elections, thereby extending his 32-year rule "over the oil-rich, but poor nation" (*Congo in media blackout for presidential elections*, 2016). Likewise, in February 2016, the Ugandan government ordered a shutdown of major social media platforms like Facebook, Twitter, and WhatsApp on polling day, officially pronounced as a "security measure to avert lies" (Duggan, 2016: para. 4). The electoral period had been tense, with rampant voter intimidation and harassment, and protesters and opposition supporters having frequently been met with armed security forces.

In the Republic of Congo (Brazzaville), only three licensed ISPs operate on Congolese territory, namely Airtel Congo, Equateur Telecom Congo (formerly Azur Congo), and MTN Congo. This clearly highlights the lack of diversity in the Congolese ISP landscape, making it more susceptible to government manipulation. Moreover, all of the ISPs are in the hands of private investors from emerging economies. Airtel Congo and MTN Congo belong to the major multinational corporations and leading emerging market telecom operators Bharti Airtel in India and MTN in South Africa, respectively. Both internationally operating companies have chosen to invest in emerging economies on the African continent with its billion-plus population, attracted by the growth of the sector (Schoentgen & Gille, 2017). The third ISP—Equateur Telecom Congo—is owned by Congolese private investor Jean Bruno Obambi. Even though little is known about Obambi, he belongs to a family of businessmen that is said to have close ties to the ruling elite of Sassou-Nguesso (Africa Intelligence, 2016).

In Uganda, in turn, the ISP landscape is more diverse, with no less than eight different licensed ISPs. Seven of them belong to non-Western shareholders, whereas the eighth ISP—Vodafone Uganda—primarily belongs to companies based in the United Kingdom and the Netherlands. While all major ISPs, including MTN, Airtel, Smile, and UTL shut down their services, it was precisely Vodafone Uganda whose connectivity remained functional (*Govt blocks facebook, twitter*, 2016). This suggests that the cooperation of ISPs to shut down their services on request may depend on company-specific characteristics, such as their ownership. While similarly to Congo Brazzaville, Bharti Airtel and MTN have major shares in two of the ISPs (Africell and MTN Uganda, respectively), the other affected ISPs belong to different private and nonprivate shareholders. Smile, an ISP mainly servicing bigger urban regions in Uganda, is owned by a

shareholder based in Mauritius, with several traces going back to investors in Saudi Arabia, Nigeria, and South Africa. The main share (69%) of UTL, on the other hand, belongs to the Libyan company LAP Green that is run by the Libyan government, whereas the minor share (31%) belongs to the Ugandan government. UTL is one of the biggest ISPs servicing large parts of the Ugandan population. This suggests that UTL alone has already a major impact in terms of providing and hence cutting access to the internet. This finding is strengthened by recent developments taking place in Uganda. After the Libyan shareholder faced major difficulties in injecting capital in the ailing company, the Ugandan state has announced to take over UTL (*Uganda government takes over troubled telecom*, 2017). This may suggest that the Ugandan government tries to regain control over the telecommunications infrastructure as UTL operates important parts of the national communication backbone. Even though the state government holds no majority of shares in any of the ISPs involved in the internet shutdowns, the ownership patterns in the Republic of Congo and Uganda seem to have facilitated their occurrence.

A closer look at the ownership patterns in 2016 Congo (Brazzaville) and in 2016 Uganda hence reveals that private ISPs may have varying motivations for cooperating with the government, and that some ISPs face higher stakes for participating in a shutdown than do others. Eventually, private ISPs can be domestic or foreign, and the latter can be dominated by investors with headquarters in countries that vary in terms of their level of democraticness or the expansion strategies of their economies, among others. The two case studies further suggest that there is no need for direct state control through majority ownership if the majority of ISPs operating on state territory are owned by foreign companies from fast-growing developing countries with ambitious expansion strategies, such as India or South Africa; by private companies with investors from authoritarian regimes, like Saudi-Arabia and Libya; or by private domestic companies with close ties to the ruling elite. Overall, it appears worth exploring further the different types of private ownership and their effects on a state's capacity to use ICT for repressive purposes.

5.6 Discussion and outlook

Although state involvement in ISPs can be used straightforwardly by governments to render control over internet access, the situation becomes multidimensional once private ISPs are involved. Setting up telecom infrastructure is costly (Andoh-Baidoo, Osatuyi, & Kunene, 2014); states often need to rely on foreign investment to foster internet-based economic growth. If a digitally repressive state decides to not only keep the communication borders open but also accept foreign investment, the most direct way of controlling the internet infrastructure through state ownership is no longer available. Rather, the incumbent government depends on (foreign) private telecom companies in its efforts to control internet-based information and communication. In an attempt to solve the alleged "dictator's dilemma," state governments often require—by law or voluntary agreement—that ISPs assist upon request in interrupting

internet services, restricting specific internet content, and providing user-identifying information, among others. As part of their license agreement, ISPs hence often agree on potentially being willing to temporarily shut down their services on government request.

In consequence, a company can become subject to two potentially conflicting laws: the local law requiring compliance with government requests, and a national law. Compliance with a government request to interrupt services should depend on where a company's shareholders are mainly based. If the majority shareholders have headquarters in established democracies, national laws may comprise (international) human rights standards. In May 2015, United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, together with experts from relevant other organisations, issued a declaration that internet kill switches are impermissible under international human rights law, even in times of conflict (Article 19, 2015). According to this declaration, governments can no longer justify ordering telecommunications companies to shut off internet services in the face of social unrest or protest. Telecom companies hence face a choice between strained ties with the host government or public condemnation, if not persecution at home (Lecraw, 1984: 27). We would hence expect companies with roots in established democracies to be less willing to comply with an authoritarian state's order to interrupt or manipulate their services to repress political opposition or prevent protests.

Recent events support this expectation. The Telecommunications Industry Dialog, for instance, is a group of eight multinational companies with headquarters in European democracies and the United States who jointly address freedom of expression and privacy in the sector.[54] All European dialogue members also joined the expanded Global Network Initiative (GNI) in 2017. These companies have committed to the GNI Principles on freedom of expression and privacy and agreed to collaborate with academics, civil society organisations, and investors to further their efforts to advance privacy and freedom of expression in the ICT sector. Prominent examples of such efforts to minimise complicity in government censorship and other abuses include (Vodafone, 2014) transparency reports detailing the type and number of requests it receives from government bodies. These company reports are meant to not only compensate for gaps in the national governance of governmental surveillance activities but also to regain trust from customers.

Results from Ranking Digital Rights (2017) support that ISPs from emerging markets are less sensitive when it comes to public commitments and disclosed policies protecting users' freedom of expression and privacy. While the big Western multinationals (AT&T, Vodafone, Orange and Telefonica) place first, ISPs from emerging markets, notably the Indian Bharti Airtel or South Africa-based MTN perform hardly

[54] These companies are AT&T (United States); Millicom, Nokia, Telia, and Telenor Group (all Scandinavia); Telefonica (Spain); Orange (France); and Vodafone (UK).

any better than Malaysian Axiata and only slightly better than Etisalat from the United Arab Emirates. The Indian and South African governments also joined the group of countries, including Russia, China, and Saudi Arabia, that opposed the 2016 resolution of the United Nations Human Rights Council condemning "unequivocally measures to intentionally prevent or disrupt access to or dissemination of information online" (2016). The point of contention for these countries was the line condemning any intentional disruption to internet access or infringement on the ability to share information online, which they asked to be deleted. Eventually, the UN resolution, though nonbinding, stands in direct opposition to recent government actions to intentionally prevent access to the internet. Overall, it appears that foreign companies from emerging markets are willing to accept restrictions on their service provisions because of competitive necessity, in particular if the new market abroad is crucial in terms of size and geographical location.

As this discussion demonstrates, instances of internet shutdowns raise concerns about various values, including freedom of expression, commerce, public safety, and law enforcement. They raise questions about the conditions under which government-requested interruption of internet services is (perceived as) legitimate. Universal internet outages in a country such as Egypt might be rejected as technological repression violating basic human rights by the same citizen who accepts it in other circumstances, despite the collateral damage to free expression, commerce and possibly public safety. An example for a scenario potentially perceived as appropriate would be government authorities in a country such as the United Kingdom cutting off internet services in a location allegedly targeted by a planned terrorist attack that is said to be coordinated by social media. "More than anything, these instances are a reminder that infrastructure is not a given and can be severed by governmental action" (DeNardis, 2012: 731).

5.7 Conclusion

Despite its allegedly decentralised nature, the internet relies on a hierarchical physical infrastructure that provides for opportunities to control and manipulate the flow of digital information and communication. The arguably most brute force method of internet control is a temporary shutdown. Between 2014 and 2016, access to the internet was restricted during about one third of the elections in SSA countries. Typically, these intentional disruptions were ordered by the incumbent rulers to prevent opponents from organising protests or reporting election malfeasance. Yet the government usually cannot directly interrupt internet access but relies on the willingness of ASs, in particular ISPs, to halt their services. ASs can be seen as bottlenecks of the internet, as they form central points through which data flow in and out for a larger population. Especially in Africa, cutting last-mile access can be efficient as there are only few ASs that control all IP addresses within a country. Most ASs belong to ISPs owned by the state and/or private investors. In this article, we argued that ISP ownership is critical to understanding authoritarian practices violating citizens' freedom of expression in the digital sphere.

Specifically, we studied the link between internet shutdowns and state majority ownership of ISPs at the time of general elections in any SSA country between 2014 and 2016. Our csQCA of original data on ISP ownership structures and documented internet shutdowns revealed a positive relationship between companies majority-owned by an authoritarian state and a temporary halt of internet provision during electoral periods. On the one hand, our findings demonstrate that election violence alone is insufficient to explain internet shutdowns ordered by the government. On the other hand, it turns out that neither is state majority ownership of ISPs sufficient to explain why some autocracies interrupt access to the internet and others did not. Case studies of Uganda and the Republic of Congo's 2016 elections highlighted that shutdowns can also occur in the absence of state majority ownership when private ISPs are willing to comply with a government request to halt their services. In particular, our analysis suggests that internet shutdowns may be facilitated if ISPs are owned by private companies with investors from authoritarian regimes like Saudi Arabia and Libya, with their headquarters in fast-growing developing countries, such as India or South Africa, or private companies whose owners are close to the ruling elite. While the mechanism of state-owned ISPs and internet disruptions appears to be straightforward, further research needs to determine the circumstances under which ISPs owned by private investors comply with government requests to restrict their services.

The structure of private ownership is arguably complex and may serve various goals, including optimising taxation or "blurring" accountability. Although the configurational analysis is useful to get a better understanding of the relevance of the ownership variable, it does not allow capturing the multidimensionality of the real-world situation. That is, by aggregating our company-level data at the macro level of countries, we lose much information about the ownership structure of different companies within the same country, including whether the mother shareholder of a foreign company is based in a democratically constituted country, or not. To adequately account for the effects of different ownership structures on the likelihood of ICT use for repressive purposes, however, it appears to matter whether a mother company (e.g., Vodafone with its headquarter in the United Kingdom) can be held accountable for the action of those companies in which it holds shares. Also, the size of the market, in which a shareholder invests, and potential future profits seem to play a role when it comes to a company's willingness to cooperate with governments. In addition, upcoming large-N studies should also systematically account for temporally and spatially varying levels of internet penetration, in terms of political relevance for protest mobilisation, but also economic damage in consequence of a shutdown. Overall, the structure of shareholders is more complex than the presented analysis at the country level suggests; longitudinal comparative studies at the level of companies are needed. These considerations call for further research on the role of private ownership of ISPs in authoritarian contexts.

GENERAL CONCLUSION

6.1 Main contributions

This thesis shows both theoretically and empirically that authoritarian governments vary in their motivation and capacity to exert control over internet access. My investigation focuses on the highly relevant but understudied African region by combining evidence from qualitative interviews, qualitative comparative analyses, and large-*N* statistical analyses. The presented studies build upon existing theories and complement the literature on authoritarian survival with insights from political communication, internet governance, and state-business relations.

Primarily, my research contributes to a more nuanced understanding of the conditions under which authoritarian rulers exert control over internet access. On one hand, I address the potential of internet access to challenge authoritarian rule due to its decentralised and low-cost features that help citizens and opposition supporters overcome traditional collective action problems. On the other, I emphasise the importance of basic internet infrastructure and its ownership to understand a regime's capacity to control and manipulate internet access. Internet infrastructure is subject to potentially conflicting interests depending on the identity of its owners and their relations to the government.

The thesis consists of four studies which are theoretically and empirically bridged by focusing on different aspects of internet access and use in African autocracies. The first study investigates how opposition supporters use ICT to challenge electoral malpractice. The remaining studies analyse how state-business relations shape authoritarian rulers' capacity to control internet access and examine both their political determinants and effects.

Study one focuses on internet use by opposition supporters and its potential to undermine traditional forms of electoral malpractice, in particular electoral violence. Theoretically, I propose that the internet facilitates mobilisation efforts by opposition supporters in authoritarian regimes. At the same time, it also provides governments with additional information to commit targeted acts of repression. The results indicate that opposition supporters are more likely to use ICT to challenge electoral malpractice than government supporters or non-partisan citizens. However, they also face a higher risk of state repression, as

evidenced by a greater likelihood of electoral violence in opposition strongholds with higher levels of internet connectivity. Accordingly, by manipulating internet access during elections, authoritarian rulers aim to undermine the challenges arising from oppositional use of ICT and obscure activities of state repression. These insights contribute to the literature on political communication by specifying how ICT shape mobilisation efforts in authoritarian-developing contexts at election times, for which both theoretical and empirical accounts remain scarce (Emmer & Kunst, 2018).

Study two complements the literature on authoritarian survival with insights from international business studies. By theorising state-business relations based on company owners' identity and origin, the study provides testable expectations as to which ISPs support or challenge the implementation of information controls. Empirically, it introduces original data on the ownership of internet infrastructure across the African continent and replicates a study by Rød & Weidmann (2015), in which a variable on ISP state ownership per country and year is added. The results indicate that, rather than internet penetration, state ownership of internet-providing companies has a negative effect on democratic change. Crucially, this finding highlights the shortcomings of research on the political determinants and effects of internet penetration, which tend to neglect the importance of those actors providing internet services.

Study three contributes to the literature on authoritarian collaboration. Theoretically, it proposes that authoritarian rulers face different constraints on their attempts to maintain control over the telecom sector and pressure to grant access to foreign investors. The results indicate that authoritarian governments relying on repression are more open to foreign-autocratic investors. This suggests that authoritarian African rulers make strategic decisions on whether to accept foreign investment in the telecom sector and selectively grant access to investors from like-minded regimes. These findings contribute to the growing debate on authoritarian collaboration through economic ties by generating new empirical insights that go beyond the focus on FDI from China.

The final study empirically assesses a government's capacity to manipulate internet access. The results from a qualitative comparative analysis of all African elections between 2014 and 2016 suggest that ISP majority state ownership facilitates internet disruptions during authoritarian elections. However, state-ownership of internet infrastructure is not a necessary condition for implementing internet disruptions. As shown by case-specific evidence from Congo-Brazzaville and Uganda, governments develop other strategies to ensure the compliance of ISPs with their requests to manipulate internet access.

In sum, this thesis contributes to the debate about how increasing digitalisation affects authoritarian rule. Its findings underline that both the motivation and capacity of autocrats to exert control over internet access vary across authoritarian regimes and likely explain differences in the extent to which

authoritarian regimes filter, block, or manipulate internet access: first, by investigating how ICT use by opposition supporters can threaten regime survival, it points to authoritarian governments' motives to establish information controls; and second, the analysis of ISP ownership reveals the role of state-business relations in shaping a government's capacity to control digital information flows.

6.2 Avenues for future research

This thesis lays the ground for further research on the control over internet infrastructure and its implications for authoritarian survival. The studies also highlight current gaps in the field and point to several avenues for further research about the determinants, mechanisms, and effects of control over internet access.

6.2.1 Mechanisms: Exerting control over internet access

The theory and evidence presented in Study two, three, and four acknowledge the importance of internet infrastructure and its ownership to understand the determinants and effects of internet access and use. These insights challenge the dominant narrative of political science studies that treat the internet as a "black box". Further research should investigate (1) how regulatory strategies enable authoritarian governments to control ISPs beyond ownership and (2) the role of internet infrastructure not operated by ISPs to control internet access.

First, in this thesis, I focus exclusively on ISP ownership as a means to control internet access. However, as highlighted throughout this thesis, governments also use other channels to make companies comply with their request to disrupt or manipulate internet access (cf. Howard, 2011). A prominent way to constrain the agency of ISPs is through license agreements. Many ISPs, when following government orders to disrupt internet access, refer to their license agreements to justify their actions. For example, during Uganda's 2021 elections MTN, one of the major ISPs, informed its customers via Twitter that it implemented the government directive "in compliance with its National Telecommunications Operator License" (MTN Uganda [@mtnug], 2021). Indeed, case studies suggest that authoritarian governments often establish restrictive licensing terms for ISPs who, in turn, face a revocation of their license if they fail to comply (e.g. Rodan, 1998; MacKinnon, 2011).[55] In consequence, to understand the role of license agreements in shaping censorship behaviour, it would be interesting to investigate whether ISPs subjected to similar license agreements react in similar ways to government requests to manipulate internet access and whether there is a self-selection into entering license agreements depending on the ISP's ownership.

[55] Theoretically, a large body of literature deals with the regulation of business and its social and political implications (see Clarke, 1999 for an overview). These insights could be useful to reflect on the ways in which governments regulate ISPs how they shape political outcomes such as information controls.

Second, this thesis focuses on infrastructure owned and operated by ISPs. This focus seems useful since ISPs operate last-mile infrastructure needed to provide (and manipulate) internet access for individual consumers. Yet, the backbone infrastructure underlying last-mile networks—such as fibre optics, copper cables, towers—is often owned by companies other than ISPs and subject to increasing commercialisation. For example, Chinese companies have built large networks of fibre optics in Africa, on which many local ISPs rely (Gagliardone & Geall, 2014). Also, Western content providers like Google, Facebook, or Amazon increasingly invest in backbone infrastructure across Africa (Nothias, 2020). How the ownership and management of such higher-level internet infrastructure determine internet access and use, thus, appears to be an important question for further research on more recent developments.

6.2.2 Determinants: ICT access and use in the context of authoritarian elections

Evidence from Study one highlights the ways in which internet use can threaten authoritarian survival, whereas Study three investigates how different political institutions determine the regime's ability and motivation to maintain control over the telecom sector. Future research may investigate (1) how internet use by opposition supporters triggers digitally repressive responses, notably at elections times, and (2) which corporate actors support authoritarian governments in establishing control over internet access and use.

First, results from Study one underline the shortcomings of cross-country comparisons using internet penetration as independent variable to estimate the effect of internet access and use on political outcomes such as democratisation. As highlighted by the Ugandan case, even in countries with low internet penetration, internet access can play a significant role for mobilisation depending on its distribution and use (cf. Nisbet, Stoycheff, & Pearce, 2012). Focusing on China, King, Pan and Roberts (2013) examined how government authorities discriminate between internet use deemed important to learn about public opinion and internet use perceived as regime-threatening requiring digitally repressive responses. Future studies may further look into the actual use of internet by citizens and opposition supporters in authoritarian contexts, notably at election times, and the conditions under which internet use trigger digitally repressive responses. In light of the increasing trend to shut down internet access in African autocracies (Garbe, 2020), it would be interesting to learn whether and how internet restrictions affect opposition supporters' mobilisation efforts.

Second, Study three highlights institutional aspects of domestic governments that likely constrain an authoritarian ruler in attracting investment in the telecom sector. In this study, I focus on how government characteristics influence the share and composition of FDI in the telecom sector while neglecting the agency of ISPs. However, FDI is based on deals between two independent partners and companies

actively decide to invest in a country based on their own interests. A tremendous amount of scholarship has looked into the determinants of company investment in authoritarian-developing contexts (e.g. Schneider & Frey, 1985; Blanton & Blanton, 2007; Büthe & Milner, 2008). As indicated by evidence from ISP ownership in Africa, several major foreign investors are state entities, such as Etisalat (United Arab Emirates) or Viettel (Vietnam). Given the sovereigntist agenda towards internet governance by many authoritarian governments' (Flonk, Jachtenfuchs, & Obendiek, 2020), future research may examine whether and how political motives shape FDI strategies of multinational (state-owned) internet companies.

6.2.3 Effects: Control over internet access across ISPs

Results from study four suggest that ISPs, depending on their owner identity and origin, differ in their willingness to implement information controls. Study one points to potential effects of internet disruptions on the conduct of authoritarian elections. To provide more robust evidence, future studies should (1) use more disaggregated approaches to study information controls across ISPs and (2) examine internet disruptions and electoral malpractice using quasi-experimental approaches.

Due to the highly (country-) aggregated nature of the data on internet shutdowns, the results from Study four do not directly demonstrate the effects of ISP ownership on internet control. To systematically investigate this link, more fine-grained data of manipulation to internet access across ISPs is needed. Despite much progress in computer science in measuring internet activity and its disruption (e.g. Dainotti *et al.*, 2014; Niaki *et al.*, 2020; Filasto & Appelbaum, 2012; Wright, Darer, & Farnan, 2018), information at the level of individual ISPs, especially in the African context, is limited. In our on-going research, we use a hitherto neglected source of internet traffic data, namely VPN usage data. VPN usage data provides information on how much traffic is routed through a VPN. This data indirectly indicates when an ISP bans access to specific websites (indicated by increases in VPN use) or cuts access to its entire network (indicated by drops in VPN use). Against limitations in large-scale internet traffic data, the use of VPN data is an innovative way to analyse ISP behaviour in the African context.

Second, as highlighted by the interviews from Uganda in Study one, internet disruptions can have severe consequences for the conduct of authoritarian elections. To the best of my knowledge, existing research exclusively focuses on the effects of internet disruptions on protest behaviour and state repression. However, systematic knowledge on the impact of internet disruptions on electoral malpractice is still missing. Future studies might investigate the ways in which internet disruptions hinder opposition supporters in reporting and countering electoral malpractice. To isolate the effect of internet disruptions, ideally, such studies would use quasi-experimental approaches in which electoral conduct in areas facing a disruption is compared to areas not facing a disruption.

6.3 Concluding remarks

Comparative scholars have moved beyond the question of whether internet access fosters or challenges democratisation, and started investigating the conditions under which it supports authoritarian survival. To date, there remains a dearth of research on the political determinants and effects of internet access in developing, especially African, countries. Therefore, this thesis makes an important contribution to the understanding of digitalisation in a hitherto neglected region. It highlights the potential of internet use by opposition actors to challenge authoritarian rule. It further emphasises that the internet is not a resource that governments can simply control and manipulate as they choose. Rather, the internet is owned by a variety of public and private actors that shape governments' capacity to exert control over internet access. Given the involvement of Western companies, donors, and international organisations in Africa's ICT landscape, insights from this thesis not only contribute to a better understanding of ICT use and control in Africa, but also point to the responsibility of other global actors in shaping this landscape.

REFERENCES

Access Now. (2016). *#KeepItOn*. Retrieved 08.01.2019 from https://www.accessnow.org/keepiton/

Access Now. (2018). *Venezuela blocks access to the TOR network*. Retrieved 04.03.2021 from https://www.accessnow.org/venezuela-blocks-tor/

ACE. (2020). *Voting Operations*. Retrieved 20.04.2020 from https://aceproject.org/ace-en/topics/vo/onePage

Acemoglu, D., & Robinson, J. A. (2000). Political losers as a barrier to economic development. *American Economic Review, 90*(2), 126-130.

Aceto, G., & Pescapé, A. (2015). Internet censorship detection: A survey. *Computer Networks, 83*, 381-421.

Acharya, H. B., Chakravarty, S., & Gosain, D. (2017). Few throats to choke: On the current structure of the internet. *Proceedings of the IEEE 42nd Conference on Local Computer Networks (LCN)* (339-346), IEEE.

Adeola, S. (2017). *Benin Parliament rejects bill to reduce presidential term limit*. Retrieved 26.01.2021 from https://www.theafricancourier.de/news/africa/benin-parliament-rejects-bill-to-reduce-presidential-term-limit/

Africa Intelligence. (2016). *Paul Obambi, The man at the top of Congo-B's private sector tree*. Retrieved 10.11.2017 from https://www.africaintelligence.com/aia/insiders/congo-b/2016/01/19/paul-obambi-the-man-at-the-top-of-congo-b-s-private-sector-tree/108125864-be1

Afrobarometer. (2016). *Uganda Round 6*. Retrieved 01.03.2021 from http://www.afrobarometer.org

Agence France-Presse. (2016). *Central African Republic candidates call for halt to 'tainted' election*. Retrieved 28.12.2020 from https://www.theguardian.com/world/2016/jan/04/central-african-republic-candidates-call-for-halt-to-tainted-election

Ajayi, S. I., & Ndikumana, L. (2014). *Capital flight from Africa: Causes, effects, and policy issues*. Oxford University Press.

Aker, J. C., & Mbiti, M. I. (2010). Mobile phones and economic development in Africa. *The Journal of Economic Perspectives, 24*(3), 207-232.

Albiman, M. M., & Sulong, Z. (2016). The role of ICT use to the economic growth in Sub Saharan African region (SSA). *Journal of Science and Technology Policy Management, 7*(3), 306-329.

Alemu, R. (2018). *The liberalisation of the telecommunications sector in sub-Saharan Africa and fostering competition in telecommunications services markets: An analysis of the regulatory framework in Uganda*. Springer.

Alozie, N. O., Akpan-Obong, P., & Foster, W. A. (2011). Sizing up information and communication technologies as agents of political development in sub-Saharan Africa. *Telecommunications Policy, 35*(8), 752-763.

Andoh-Baidoo, F. K., Osatuyi, B., & Kunene, K. N. (2014). ICT capacity as the investment and use of ICT: Exploring its antecedents in Africa. *Information Technology for Development, 20*(1), 44-59.

Anthonio, F. (2019). *Internet shutdowns, fatal clampdowns; a continuing threat to freedom of expression and assembly rights in Africa*. Retrieved 23.01.2019 from http://www.africafex.org/digital-rights/internet-shutdowns-fatal-clampdowns-a-continuing-threat-to-freedom-of-expression-and-assembly-rights-in-africa

Anyanwu, J. C. (2006). Promoting of investment in Africa. *African Development Review, 18*(1), 42-71.

Arayssi, M., & Jizi, M. I. (2019). Does corporate governance spillover firm performance? A study of valuation of MENA companies. *Social Responsibility Journal, 15*(5), 597-620.

Armstrong, C. S., Guay, W. R., & Weber, J. P. (2010). The role of information and financial reporting in corporate governance and debt contracting. *Journal of accounting and economics, 50*(2-3), 179-234.

Arregle, J. L., Hitt, M. A., Sirmon, D. G., & Very, P. (2007). The development of organizational social capital: Attributes of family firms. *Journal of Management studies, 44*(1), 73-95.

Arriola, L., & Johnson, C. (2012). *Electoral violence in democratizing states*. Unpublished Manuscript. University of California, Berkeley.

Asunka, J., Brierley, S., Golden, M., Kramon, E., & Ofosu, G. (2017). Electoral fraud or violence: The effect of observers on party manipulation strategies. *British Journal of Political Science, 49*(1), 1-23.

Avgerou, C., Hayes, N., & La Rovere, R. L. (2016). Growth in ICT uptake in developing countries: New users, new uses, new challenges. *Journal of Information Technology, 31*(4), 329-333.

Ayalew, Y. E. (2019). The Internet shutdown muzzle(s) freedom of expression in Ethiopia: Competing narratives. *Information & Communications Technology Law, 28*(2), 208-224.

Ayittey, G. B. N. (2011). *Defeating Dictators: Fighting Tyranny in Africa and Around the World*. St. Martin's Publishing Group.

Bachrach, P., & Baratz, M. S. (1970). *Power and poverty: Theory and practice*. Oxford University Press.

Bader, J., Grävingholt, J., & Kästner, A. (2010). Would autocracies promote autocracy? A political economy perspective on regime-type export in regional neighbourhoods. *Contemporary Politics, 16*(1), 81-100.

Baguma, R., & Eilu, E. (2015). Using mobile phones in elections in developing countries: Opportunities and challenges. In A. Gamatié (Ed.), *Computing in research and development in Africa. Benefits, trends, challenges and solutions*. Springer International Publishing.

Bahia, K., & Suardi, S. (2019). *The state of mobile internet connectivity 2019*. GSMA. Retrieved 24.02.2020 from https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/07/GSMA-State-of-Mobile-Internet-Connectivity-Report-2019.pdf

Bailard, C. S. (2015). Ethnic conflict goes mobile: Mobile technology's effect on the opportunities and motivations for violent collective action. *Journal of Peace Research, 52*(3), 323-337.

Bailard, C. S. (2016). Corporate ownership and news bias revisited: Newspaper coverage of the Supreme Court's citizens united ruling. *Political Communication, 33*(4), 583-604.

Bak, D., & Moon, C. (2016). Foreign direct investment and authoritarian stability. *Comparative Political Studies, 49*(14), 1998-2037.

Barkan, J. D. (2008). Progress and retreat in Africa: Legislatures on the rise? *Journal of Democracy, 19*(2), 124-137.

Bartlett, J., Krasodomksi-Jones, A., Daniel, N., Fisher, A., & Jesperson, S. (2015). *Social media for election communication and monitoring in Nigeria*. Demos. Retrieved 23.02.2021 from https://www.demos.co.uk/wp-content/uploads/2015/11/Social-Media-in-Nigerian-Election.pdf

Bastiaens, I. (2016). The politics of foreign direct investment in authoritarian regimes. *International Interactions, 42*(1), 140-171.

Bates, D., Mächler, M., Bolker, B., & Walker, S. (2015). Fitting linear mixed-effects models using lme4. *Journal of Statistical Software, 1*(1).

Beardsworth, N. (2016). Challenging dominance: The opposition, the coalition and the 2016 election in Uganda. *Journal of Eastern African Studies, 10*(4), 749-768.

Bennedsen, M., & Wolfenzon, D. (2000). The balance of power in closely held corporations. *Journal of Financial Economics, 58*(1-2), 113-139.

Bennett, W. L., & Segerberg, A. (2013). *The logic of connective action: Digital media and the personalization of contentious politics.* Cambridge University Press.

Berle, A. A., & Means, G. C. (1933). *The modern corporation and private property*. Macmillan.

Bhasin, T., & Gandhi, J. (2013). Timing and targeting of state repression in authoritarian elections. *Electoral Studies, 32*(4), 620-631.

Bimber, B. (2017). Three prompts for collective action in the context of digital media. *Political Communication, 34*(1), 6-20.

Birkinshaw, J., Braunerhjelm, P., Holm, U., & Terjesen, S. (2006). Why do some multinational corporations relocate their headquarters overseas? *Strategic Management Journal, 27*(7), 681-700.

Biryabarema, E. (2016). *Uganda police buy anti-riot gear ahead of Museveni's re-election bid*. Reuters. Retrieved 23.02.2021 from https://www.reuters.com/article/us-uganda-security-idUSKCN0VH1I7

Biryaberema, E. (2011). *Uganda bans SMS texting of key words during poll*. Reuters. Retrieved 23.02.2021 from https://www.reuters.com/article/ozatp-uganda-election-telecoms-idAFJOE71G0M520110217

Blanton, S. L., & Blanton, R. G. (2007). What attracts foreign investors? An examination of human rights and foreign direct investment. *The Journal of Politics, 69*(1), 143-155.

Boas, T. C. (2006). Weaving the authoritarian web: the control of internet use in nondemocratic regimes. In J. Zysman & A. Newman (Eds.), *How revolutionary was the digital revolution? National responses, market transitions, and global technology*. Stanford University Press.

Bogaards, M. (2012). Where to draw the line? From degree to dichotomy in measures of democracy. *Democratization, 19*(4), 690-712.

Boix, C., & Svolik, M. W. (2013). The foundations of limited authoritarian government: Institutions, commitment, and power-sharing in dictatorships. *The Journal of Politics, 75*(2), 300-316.

Bonvecchi, A., & Simison, E. (2017). Legislative institutions and performance in authoritarian regimes. *Comparative Politics, 49*(4), 521-544.

Bosch, T. (2013). Youth, facebook and politics in South Africa. *Journal of African Media Studies, 5*(2), 119-130.

Boss, D., Connelly, B., Hoskisson, R., & Tihanyi, L. (2013). Corporate governance: Ownership interests, incentives and conflicts. In D. Wright, D. Siegel, K. Keasey, & L. Filatotchev (Eds.), *The Oxford handbook of corporate governance*. Oxford University Press.

Bove, V., & Rivera, M. (2015). Elite co-optation, repression, and coups in autocracies. *International Interactions, 41*(3), 453-479.

Bratton, M. (2008). Vote buying and violence in Nigerian election campaigns. *Electoral Studies, 27*(4), 621-632.

Bueno De Mesquita, B., Morrow, J. D., Siverson, R. M., & Smith, A. (1999). Policy Failure and Political Survival: The Contribution of Political Institutions. *Journal of Conflict Resolution, 43*(2), 147-161.

Bueno De Mesquita, B., Smith, A., Siverson, R. M., & Morrow, J. D. (2003). *The logic of political survival*. MIT press.

Bunz, M. (2014). *The silent revolution: How digitalization transforms knowledge, work, journalism and politics without making too much noise*. Palgrave Macmillan.

Burrell, J. (2010). Evaluating shared access: social equality and the circulation of mobile phones in rural Uganda. *Journal of computer-mediated communication, 15*(2), 230-250.

Büthe, T., & Milner, H. V. (2008). The politics of foreign direct investment into developing countries: Increasing FDI through international trade agreements? *American Journal of Political Science, 52*(4), 741-762.

Calderon, C., Kambou, G., Korman, V., Kubota, M., & Cantu Canales, C. (2019). *An analysis of issues shaping Africa's economic future* (Africa's Pulse). World Bank.

Cannizzaro, A. P., & Weiner, R. J. (2018). State ownership and transparency in foreign direct investment. *Journal of International Business Studies, 49*(2), 172-195.

Carey, S. C. (2006). The Dynamic Relationship Between Protest and Repression. *Political Research Quarterly, 59*(1), 1-11.

Carey, S. C. (2010). The use of repression as a response to domestic dissent. *Political Studies, 58*(1), 167-186.

Castells, M. (2015). *Networks of outrage and hope: Social movements in the internet age* (2nd ed.). Polity Press.

Chaturvedi, A. (2005). Rigging elections with violence. *Public Choice, 125*(1/2), 189-202.

Cheeseman, N. (2008). The Kenyan elections of 2007: An introduction. *Journal of Eastern African Studies, 2*(2), 166-184.

Cheeseman, N. (2015). *Democracy in Africa: Successes, failures, and the struggle for political reform (New approaches to African history book 9)*. Cambridge University Press.

Cheeseman, N., & Klaas, B. (2018). *How to rig an election*. Yale University Press.

Chen, X., Li, G., Hu, Y., & Li, Y. (2016). How anonymity influence self-disclosure tendency on Sina Weibo: An empirical study. *The Anthropologist, 26*(3), 217-226.

Chibita, M. B. (2016). Digital activism in Uganda. In B. Mutsvairo (Ed.), *Digital activism in the social media era* (pp. 69-93). Springer.

Christensen, D., & Garfias, F. (2018). Can you hear me now? How communication technology affects protest and repression. *Quarterly journal of political science, 13*(1), 89.

CIPESA. (2016). *Ugandans turn to proxies, VPN in face of social media shutdown*. CIPESA. Retrieved 24.02.2021 from https://cipesa.org/2016/02/ugandans-turn-to-proxies-vpn-in-face-of-social-media-shutdown/

CIPESA. (2019). *Despots and disruptions: Five dimensions of internet shutdowns in Africa*. CIPESA. Retrieved 24.02.2021 from https://cipesa.org/?wpfb_dl=283

CIPESA. (2020). *State of internet freedom in Burundi 2019. Mapping trends in government internet controls, 1999-2019*. Retrieved 23.01.2021 from https://cipesa.org/?wpfb_dl=335

Clarke, M. (1999). *Regulation: The social control of business between law and politics*. Palgrave Macmillan UK.

Collier, P., & Vicente, P. C. (2012). Violence, bribery, and fraud: the political economy of elections in Sub-Saharan Africa. *Public Choice, 153*(1-2), 117-147.

Colombo, A., D'Aoust, O., & Sterck, O. (2018). From rebellion to electoral violence: Evidence from Burundi. *Economic Development and Cultural Change, 67*(2), 333-368.

Commander, S., Harrison, R., & Menezes-Filho, N. (2011). ICT and productivity in developing countries: New firm-level evidence from Brazil and India. *Review of Economics and Statistics, 93*(2), 528-541.

Congo holds elections under telecom blackout. (2016). France 24. Retrieved 28.12.2020 from https://www.france24.com/en/20160320-congo-brazzaville-holds-elections-under-telecom-blackout-nguesso

Congo in media blackout for presidential elections. (2016). Al Jazeera. Retrieved 28.12.2020 from http://www.aljazeera.com/news/2016/03/congo-media-blackout-presidential-elections-160320044041238.html

Connelly, B. L., Hoskisson, R. E., Tihanyi, L., & Certo, S. T. (2010). Ownership as a form of corporate governance. *Journal of Management studies, 47*(8), 1561-1589.

Cooley, A. (2015). Authoritarianism goes global: Countering democratic norms. *Journal of Democracy, 26*(3), 49-63.

Coppedge, M., Gerring, J., Knutsen, C. H., Lindberg, S. I., Teorell, J., Altman, D., Bernhard, M., Fish, M. S., Glynn, A., & Hicken, A. (2020a). V-Dem Codebook v10.

Coppedge, M., Gerring, J., Knutsen, C. H., Lindberg, S. I., Teorell, J., Altman, D., Bernhard, M., Fish, M. S., Glynn, A., & Hicken, A. (2020b). *V-Dem Dataset v10 [Country-Year/Country-Date]*

Coppedge, M., Gerring, J., Lindberg, S. I., Skaaning, S.-E., Teorell, J., Altman, D., Bernhard, M., Fish, M. S., Glynn, A., Hicken, A., Knutsen, C. H., Marquardt, K. L., McMann, K., Mechkova, V., Paxton, P., Pemstein, D., Saxer, L., Seim, B., Sigman, R., & Staton, J. (2017b). V-Dem Codebook v7.1.

Coppedge, M., Gerring, J., Lindberg, S. I., Skaaning, S.-E., Teorell, J., Altman, D., Bernhard, M., Fish, S. M., Glynn, A., Hicken, A., Knutsen, C. H., Krusell, J., Lührmann, A., Marquardt, K. L., McMann, K., Mechkova, V., Olin, M., Paxton, P., Pemstein, D., Pernes, J., Sanhueza Petrarca, C., von Römer, J., Saxer, L., Seim, B., Sigman, R., Staton, J., Stepanova, N., & Wilson, C. (2017a). *V-Dem [Country-Year/Country-Date] Dataset v7.1*.

Corrales, J., & Westhoff, F. (2006). Information technology adoption and political regimes. *International Studies Quarterly, 50*(4), 911-933.

Cuervo-Cazurra, A., Inkpen, A., Musacchio, A., & Ramaswamy, K. (2014). Governments as owners: State-owned multinational companies. *Journal of International Business Studies, 45*(8), 919-942.

Culpepper, P. D. (2010). *Quiet politics and business power: Corporate control in Europe and Japan*. Cambridge University Press.

Dada, T., & Sayadi, E. (2017). *Egypt is blocking more websites: Why it matters, and what you can do*. Retrieved 29.01.2021 from https://www.accessnow.org/egypt-blocking-websites-matters-can/

Dahir, A. L. (2017). *How Cameroon pressured mobile operators to shut down the internet and stifle dissent*. Retrieved 10.10.2018 from https://qz.com/africa/893401/cameroon-pressured-mtn-and-other-operators-to-shut-down-internet-in-bamenda-buea-regions/

Dahir, A. L. (2019). *Mauritania blocked the internet over protests though just one in five people are online*. Retrieved 26.02.2020 from https://qz.com/africa/1655017/mauritania-shuts-down-internet-after-disputed-elections/

Dahl, R. (1959). Business and politics: A critical appraisal of political science. In R. Dahl, M. Haire, & P. Lazarsfeld (Eds.), *Social Science Research on Business Product and Potential*. Columbia University Press.

Dainotti, A., Squarcella, C., Aben, E., Claffy, K., Chiesa, M., Russo, M., & Pescapè, A. (2014). Analysis of country-wide internet outages caused by censorship. *IEEE/ACM Transactions on Networking, 22*(6), 1964-1977.

Dam, L., & Scholtens, B. (2012). Does ownership type matter for corporate social responsibility? *Corporate Governance: An International Review, 20*(3), 233-252.

Dasgupta, S., Lall, S., & Wheeler, D. (2005). Policy reform, economic growth and the digital divide. *Oxford Development Studies, 33*(2), 229-243.

Davenport, C. (2007). State repression and political order. *Annual Review of Political Science, 10*(1), 1-23.

Deibert, R. (2013). *Black Code : Surveillance, privacy, and the dark side of the internet*. Signal.

Deibert, R., Palfrey, J. G., Rohozinski, R., & Zittrain, J. (2008). *Access denied: The practice and policy of global internet filtering*. The MIT Press.

Deibert, R. J., Palfrey, J. G., Rohozinski, R., & Zittrain, J. (2010). *Access controlled: The shaping of power, rights, and rule in cyberspace*. The MIT Press.

Deibert, R. J., & Rohozinski, R. (2010). Liberation vs. control: The future of cyberspace. *Journal of Democracy, 21*(4), 43-57.

DeNardis, L. (2012). Hidden layers of internet control. *Information, Communication & Society, 15*(5), 720-738.

DeNardis, L. (2014). *The global war for internet governance*. Yale University Press.

DeNardis, L., & Musiani, F. (2016). Governance by infrastructure. In F. Musiani, D. L. Cogburn, L. DeNardis, & N. S. Levinson (Eds.), *The turn to internet infrastructure in internet governance* (pp. 155-167). Palgrave Macmillan.

Desbordes, R., & Vauday, J. (2007). The political influence of foreign firms in developing countries [https://doi.org/10.1111/j.1468-0343.2007.00317.x]. *Economics & Politics, 19*(3), 421-451.

Diamond, L. (2010). Liberation technology. *Journal of Democracy, 21*(3), 69-83.

Djankov, S., Caralee McLiesh, Tatiana Nenova, & Andrei Shleifer. (2003). Who owns the media? *The Journal of Law and Economics, 46*(2), 341-382.

Doh, J. P., Teegen, H., & Mudambi, R. (2004). Balancing private and state ownership in emerging markets' telecommunications infrastructure: Country, industry, and firm influences. *Journal of International Business Studies, 35*(3), 233-250.

Douma, S., George, R., & Kabir, R. (2006). Foreign and domestic ownership, business groups, and firm performance: Evidence from a large emerging market. *Strategic Management Journal, 27*(7), 637-657.

Duggan, B. (2016). *Uganda shuts down social media. Candidates arrested on election day*. Retrieved 10.02.2017 from http://edition.cnn.com/2016/02/18/world/uganda-election-social-media-shutdown/

Dunaway, J., & Lawrence, R. G. (2015). What predicts the game frame? Media ownership, electoral context, and campaign news. *Political Communication, 32*(1), 43-60.

Durant, R. F., Legge, J. S., & Moussios, A. (1998). People, profits, and service delivery: Lessons from the privatization of British Telecom. *American Journal of Political Science, 42*(1), 117-140.

Dyer, W. G., & Whetten, D. A. (2006). Family firms and social responsibility: Preliminary evidence from the S&P 500. *Entrepreneurship Theory and Practice, 30*(6), 785-802.

Edwards, B., & McCarthy, J. D. (2004). Resources and social movement mobilization. In D. A. Snow, S. A. Soule, & H. Kriesi (Eds.), *The Blackwell companion to social movements* (pp. 116-152). Blackwell Publishing.

El-Nawawy, M., Khamis, S., & Khamis, C. S. (2012). Political activism 2.0: Comparing the role of social media in Egypt's "Facebook revolution" and Iran's "Twitter uprising". *Cyber Orient, 6*(1), 8-33.

Eltantawy, N., & Wiest, J. B. (2011). The Arab Spring| Social media in the Egyptian revolution: Reconsidering resource mobilization theory. *International Journal of Communication, 5*, 1207–1224.

Emmer, M., & Kunst, M. (2018). "Digital Citizenship" revisited: The impact of ICTs on citizens' political communication beyond the Western state. *International Journal of Communication, 12*, 2191–2211.

Enenu, M. (2016). *The games incumbents play to stay in power*. The Observer. Retrieved 23.02.2021 from https://www.observer.ug/viewpoint/42440-the-games-incumbents-play-to-stay-in-power

Erdmann, G., Bank, A., Hoffmann, B., & Richter, T. (2013). *International cooperation of authoritarian regimes: Toward a conceptual framework* (GIGA Working Paper, Vol. 229). GIGA.

Eriksson, J., & Giacomello, G. (2009). Who controls the internet? Beyond the obstinacy or obsolescence of the state. *International Studies Review, 11*(1), 205-230.

Esteban, M. (2009). The Chinese amigo: Implications for the development of Equatorial Guinea. *The China Quarterly* (199), 667-685.

Estrin, S., Meyer, K. E., Nielsen, B. B., & Nielsen, S. (2016). Home country institutions and the internationalization of state owned enterprises: A cross-country analysis. *Journal of World Business, 51*(2), 294-307.

Farrell, H. (2012). The consequences of the internet for politics. *Annual Review of Political Science, 15*(1), 35-52.

FDC disregards EC on anti-vote-rigging team. (2016). Uganda Radio Network. Retrieved 28.12.2020 from https://ugandaradionetwork.com/story/fdc-recruiting-power10-anti-vote-rigging-team

FDC to crack regime arrogance & impunity - Mugisha Muntu. (2016). The Observer. Retrieved 23.02.2021 from https://observer.ug/news-headlines/42910-fdc-to-crack-regime-arrogance-impunity-mugisha-muntu

Field, A. (2009). *Discovering statistics using SPSS: And sex drugs and Rock 'n' Roll* (2nd ed.). Sage.

Fijałkowski, Ł. (2011). China's 'soft power' in Africa? *Journal of Contemporary African Studies, 29*(2), 223-232.

Filasto, A., & Appelbaum, J. (2012). *OONI: Open observatory of network interference*. Paper presented at the 2nd USENIX workshop on free and open communications on the internet (FOCI), Bellevue, WA.

Flanagan, J. (2014). *Online leaker exposes Mugabe's secrets*. Retrieved 10.01.2019 from https://www.smh.com.au/world/online-leaker-exposes-mugabes-secrets-20130715-2pyxt.html

Flonk, D., Jachtenfuchs, M., & Obendiek, A. S. (2020). Authority conflicts in internet governance: Liberals vs. sovereigntists? *Global Constitutionalism, 9*(2), 364-386.

Follow, D. F. (2020). *Burundi goes to the polls as authorities clampdown on social media*. Retrieved 28.12.2020 from https://allafrica.com/stories/202005210005.html

Frantz, E., & Kendall-Taylor, A. (2014). A dictator's toolkit. *Journal of Peace Research, 51*(3), 332-346.

Freedom House. (2015). *Ethiopia. Freedom on the Net 2015*. Retrieved 20.11.2017 from https://freedomhouse.org/report/freedom-net/2015/ethiopia

Freund, C., & Weinhold, D. (2002). The internet and international trade in services. *American Economic Review, 92*(2), 236-240.

Freyburg, T., & Garbe, L. (2018). Authoritarian practices in the digital age| Blocking the bottleneck: Internet shutdowns and ownership at election times in Sub-Saharan Africa. *International Journal of Communication, 12*, 3896–3916.

Freyburg, T., Garbe, L., & Wavre, V. (2021). *Who owns the internet, and why does it matter? A new dataset on Internet infrastructure and ownership of Internet service providers in sub-Sahara and North Africa, 2000–2016* [Unpublished Manuscript]. University of St.Gallen.

Freyburg, T., & Richter, S. (2015). Local actors in the driver's seat: Transatlantic democracy promotion under regime competition in the Arab world. *Democratization, 22*(3), 496-518.

Friedrich, C. J., & Brzezinski, Z. K. (1963). *Totalitarian dictatorship and autocracy* (revised ed.). Frederick A. Praeger.

Fuchs, D. (2005). Commanding heights? The strength and fragility of business power in global politics. *Millennium, 33*(3), 771-801.

Fuerrutter, M. (2021). *The (non-)sanctioning of human rights violations: News media coverage and European Union sanctions* [Unpublished Manuscript]. University of St.Gallen.

Gagliardone, I. (2016). *The politics of technology in Africa*. Cambridge University Press.

Gagliardone, I. (2019). *Social media and elections in Africa*. Oxford Research Encyclopedia of Politics. Retrieved 24.02.2021 from https://doi.org/10.1093/acrefore/9780190228637.013.1380

Gagliardone, I., & Geall, S. (2014). *China in Africa's media and telecommunications: cooperation, connectivity and control*. NOREF. Retrieved 23.02.2021 from https://www.academia.edu/download/33550771/7880fd6b12b93bdd18eddcbd4f4e207f.pdf

Gandhi, J. (2008). *Political institutions under dictatorship*. Cambridge University Press.

Gandhi, J., & Lust-Okar, E. (2009). Elections under authoritarianism. *Annual Review of Political Science, 12*(1), 403-422.

Gandhi, J., Noble, B., & Svolik, M. (2020). Legislatures and legislative politics without democracy. *Comparative Political Studies, 53*(9), 1359-1379.

Gandhi, J., & Przeworski, A. (2006). Cooperation, cooptation and rebellion under dictatorships. *Economics & Politics, 18*(1), 1-26.

Garbe, L. (2020). *What we do (not) know about internet shutdowns in Africa*. Retrieved 24.02.2021 from http://democracyinafrica.org/internet_shutdowns_in_africa/

Garrity, J. (2017). Getting connected: The internet and its role as a global public good forum: The global commons. *Georgetown Journal of International Affairs, 18*(1), 6-8. (8)

Gasmi, F., Maingard, A., Noumba, P., & Recuero Virto, L. (2013). The privatization of the fixed-line telecommunications operator in OECD, Latin America, Asia, and Africa: One size does not fit all. *World Development, 45*, 189-208.

Geddes, B. (2006). *Why Parties and Elections in Authoritarian Regimes?* American Political Science Association, Washington D.C. .

Geddes, B., Wright, J., & Frantz, E. (2014). Autocratic breakdown and regime transitions: A new data set. *Perspectives on Politics, 12*(2), 313-331.

Geddes, B., Wright, J., & Frantz, E. (2016). Autocratic regimes code book v1.2.

Gerschewski, J. (2013). The three pillars of stability: Legitimation, repression, and co-optation in autocratic regimes. *Democratization, 20*(1), 13-38.

Giles, C., & Mwai, P. (2020). *Africa internet: Where and how are governments blocking it?* Retrieved 31.01.2021 from https://www.bbc.com/news/world-africa-47734843

Gillwald, A., Mothobi, O., Ndiwalana, A., & Tusubira, F. F. (2019). *The state of ICT in Uganda*. Retrieved 28.12.2020 from https://www.africaportal.org/publications/state-ict-uganda/

Global Voices. (2018). *Netizen report: Elections in Mali marred by militant violence — and internet shutdowns*. Global Voices. Retrieved 28.12.2020 from https://globalvoices.org/2018/08/16/netizen-report-elections-in-mali-marred-by-militant-violence-and-internet-shutdowns/

Gohdes, A. (2015a). *Digital disruptions: A global analysis of internet outages and state violence, 1995-2010*. paper presented at APSA annual meeting 2015, San Francisco.

Gohdes, A. (2015b). Pulling the plug: Network disruptions and violence in civil conflict. *Journal of Peace Research, 52*(3), 352-367.

Gohdes, A. (2016). *Internet shutdowns during political unrest are becoming normal – and it should worry us*. Retrieved 04.02.2020 from https://politicalviolenceataglance.org/2016/09/16/internet-shutdowns-during-political-unrest-are-becoming-normal-and-it-should-worry-us/

Gohdes, A. (2020). Repression technology: Internet accessibility and state violence. *American Journal of Political Science, 64*(3), 488-503.

Göhler, G. (2009). Power to and power over. In S. R. Clegg & M. Haugaard (Eds.), *The Sage handbook of power* (pp. 27-39). SAGE Publications Ltd.

Goldsmith, J., & Wu, T. (2006). *Who controls the internet?: Illusions of a borderless world*. Oxford University Press.

Gonzalez-Ocantos, E., de Jonge, C. K., Meléndez, C., Nickerson, D., & Osorio, J. (2019). Carrots and sticks: Experimental evidence of vote-buying and voter intimidation in Guatemala. *Journal of Peace Research, 57*(1), 46-61.

Gourevitch, P. A., & Shinn, J. (2005). *Political power and corporate control: the new global politics of corporate Governance*. Princeton University Press.

Govt blocks facebook, twitter. (2016). The Observer. Retrieved 28.12.2020 from https://www.observer.ug/news-headlines/42668-govt-blocks-facebook-twitter-2

Greenstein, S. (2020). The basic economics of internet infrastructure. *Journal of Economic Perspectives, 34*(2), 192-214.

Grøgaard, B., Rygh, A., & Benito, G. R. (2019). Bringing corporate governance into internalization theory: State ownership and foreign entry strategies. *Journal of International Business Studies, 50*(8), 1310-1337.

Grönlund, Å., & Wakabi, W. (2015). Citizens' use of new media in authoritarian regimes: A case study of Uganda. *The Electronic Journal of Information Systems in Developing Countries, 67*(1), 1-23.

Grossman, G. U. Y., Humphreys, M., & Sacramone-Lutz, G. (2014). "I wld like u WMP to extend electricity 2 our village": On information technology and interest articulation. *The American Political Science Review, 108*(3), 688-705.

Grossman, G. U. Y., & Lewis, J. I. (2014). Administrative unit proliferation. *The American Political Science Review, 108*(1), 196-217.

GSMA Intelligence. (2019). *Mobile coverage maps*. Retrieved 04.02.2020 from https://www.mobilecoveragemaps.com/

Gurr, T. R. (2015). *Why Men Rebel* (40th Anniversary ed.). Routledge.

Habib, M., & Zurawicki, L. (2002). Corruption and foreign direct investment. *Journal of International Business Studies, 33*(2), 291-307.

Hadenius, A., & Teorell, J. (2007). Pathways from authoritanianism. *Journal of Democracy, 18*(1), 143-157.

Hafner-Burton, E. M., Hyde, S. D., & Jablonski, R. S. (2014). When do governments resort to election violence? *British Journal of Political Science, 44*, 149-179.

Hankla, C. R., & Kuthy, D. (2013). Economic liberalism in illiberal regimes: Authoritarian variation and the political economy of trade. *International Studies Quarterly, 57*(3), 492-504.

Hansmann, H. (2013). Ownership and organizational form. In R. Gibbons & J. Roberts (Eds.), *The handbook of organizational economics* (pp. 891-917). Princeton University Press.

Hanson, J. K. (2013). *Loyalty and acquiescence: Authoritarian regimes and inequality outcomes*. Paper presented at the 2010 APSA Annual Meeting, Washington, DC.

Harlow, S. (2013). It was a Facebook revolution": Exploring the meme-like spread of narratives during the Egyptian protest. *Revista de comunicación,* (12), 59-82.

Hart, O., Shleifer, A., & Vishny, R. W. (1997). The proper scope of government: theory and an application to prisons. *The quarterly journal of economics, 112*(4), 1127-1161.

Haschke, P. (2017). The political terror scale (PTS) codebook.

Hawthorne, R., & Grzybowski, L. (2019). *Mobile access won't fix the digital divide. Fixed-line is needed too*. Retrieved 28.01.2021 from https://theconversation.com/mobile-access-wont-fix-the-digital-divide-fixed-line-is-needed-too-126801

Hecht, G. (2001). Technology, politics, and national identity in France. In M. Allen & G. Hecht (Eds.), *Technologies of power* (pp. 253-294). MIT Press.

Hellmeier, S. (2016). The dictator's digital toolkit: Explaining variation in internet filtering in authoritarian regimes. *Politics & Policy, 44(6)*, 1158-1191.

Höglund, K. (2009). Electoral violence in conflict-ridden societies: Concepts, causes, and consequences. *Terrorism and Political Violence, 21*(3), 412-427.

Holderness, C. G. (2009). The myth of diffuse ownership in the United States. *Review of Financial Studies, 22*(4), 1377–1408.

Holderness, C. G., & Sheehan, D. P. (1988). The role of majority shareholders in publicly held corporations: An exploratory analysis. *Journal of Financial Economics, 20*, 317-346.

Howard, M. M., & Roessler, P. G. (2006). Liberalizing electoral outcomes in competitive authoritarian regimes. *American Journal of Political Science, 50*(2), 365-381.

Howard, P. (2011). *The digital origins of dictatorship and democracy: Information technology and political Islam*. Oxford University Press.

Howard, P., Agarwal, S. D., & Hussain, M. M. (2011). When do states disconnect their digital networks? Regime responses to the political uses of social media. *The Communication Review, 14*(3), 216-232.

Howard, P. N., & Hussain, M. M. (2011). The upheavals in Egypt and Tunisia: The role of digital media. *Journal of Democracy, 22*(3), 35-48.

Howard, P. N., & Mazaheri, N. (2009). Telecommunications reform, internet use and mobile phone adoption in the developing world. *World Development, 37*(7), 1159-1169.

Hughes, S., & Lawson, C. (2005). The barriers to media opening in Latin America. *Political Communication, 22*(1), 9-25.

Hughes, T. P. (1993). *Networks of power: electrification in Western society, 1880-1930*. JHU Press.

Human Rights Watch. (2016). *Guinea: Protect phone user's privacy. Mass data collection could expose personal information*. Retrieved 22.01.2019 from https://www.hrw.org/news/2016/02/05/guinea-protect-phone-users-privacy

Human Rights Watch. (2020). *Ethiopia: Communications shutdown takes heavy toll*. Retrieved 27.04.2020 from https://www.hrw.org/news/2020/03/09/ethiopia-communications-shutdown-takes-heavy-toll

Humanitarian Data Exchange. (2018). *Uganda - admin level 3 boundaries*. Retrieved 26.02.2020 from https://data.humdata.org/dataset/uganda-admin-level-4-boundaries

Iazzolino, G. (2015). *Following mobile money in Somaliland* (Rift Valley Institute Research Paper. Rift Valley Institute. http://riftvalley.net/download/file/fid/3870

Internet Sans Frontières. (2018). *Chad: Revelations on the extent of social media censorship*. Retrieved 12.10.2018 from https://internetwithoutborders.org/chad-revelations-on-the-extent-of-the-social-media-censorship/

ITU. (2021). *ICT statistics home page*. Retrieved 31.01.2021 from http://www.itu.int/en/ITU-D/Statistics/Pages/default.aspx

Jackson, P. T. (2016). *The conduct of inquiry in international relations* (2nd ed.). Routledge.

Jamali, D., Safieddine, A. M., & Rabbath, M. (2008). Corporate governance and corporate social responsibility synergies and interrelationships. *Corporate Governance: An International Review, 16*(5), 443-459.

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics, 3*(4), 305-360.

Jho, W. (2007). Global political economy of technology standardization: A case of the Korean mobile telecommunications market. *Telecommunications Policy, 31*(2), 124-138.

Jin, S., & Cho, C. M. (2015). Is ICT a new essential for national economic growth in an information society? *Government Information Quarterly, 32*(3), 253-260.

Johnson, R. A., & Greening, D. W. (1999). The effects of corporate governance and institutional ownership types on corporate social performance. *Academy of Management Journal, 42*(5), 564-576.

Jones, L., & Zou, Y. (2017). Rethinking the role of state-owned enterprises in China's rise. *New Political Economy, 22*(6), 743-760.

Josua, M., & Edel, M. (2015). To repress or not to repress—regime survival strategies in the Arab Spring. *Terrorism and Political Violence, 27*(2), 289-309.

Kaaya, S. K. (2016). *Amama Mbabazi to EC: What are you hiding?* The Observer. Retrieved 23.02.2021 from https://observer.ug/news-headlines/42646-amama-mbabazi-to-ec-what-are-you-hiding

Kakaire, S. (2016). *Vote rigging: How it happens*. The Observer. Retrieved 21.02.2021 from https://observer.ug/news-headlines/42522-vote-rigging-how-it-happens

Kamau, S. C. (2017). Democratic engagement in the digital age: youth, social media and participatory politics in Kenya. *Communicatio, 43*(2), 128-146.

Karekwaivanane, G. H. (2019). 'Tapanduka Zvamuchese': Facebook, 'unruly publics', and Zimbabwean politics. *Journal of Eastern African Studies, 13*(1), 54-71.

Karugaba, M. (2016, February 12). EC bans use of mobile phones at polling stations. *New Vision*.

Kasm, S. (2018). Redefining publics: Mosireen, state crime and the rise of a digital public sphere. *State Crime Journal, 7*(1), 100-140.

Kedzie, C. (1997). *Communication and democracy: Coincident revolutions and the emergent dictator's dilemma*, [Doctoral Thesis, RAND Graduate School]. Santa Monica, CA. https://www.rand.org/pubs/rgs_dissertations/RGSD127.html

Kelly Garrett, R. (2006). Protest in an information society: A review of literature on social movements and new ICTs. *Information, Communication & Society, 9*(2), 202-224.

Kembabazi, G. (2016). *An open internet versus social media shutdown*. Association for Progressive Communications. Retrieved 20.08.2020 from https://www.apc.org/en/blog/open-internet-versus-social-media-shutdown

Keremoğlu, E., & Weidmann, N. B. (2020). How dictators control the internet: A review essay. *Comparative Political Studies, 53*(10-11), 1690-1703.

King, G., Pan, J., & Roberts, M. E. (2013). How censorship in China allows government criticism but silences collective expression. *American Political Science Review, 107*(2), 326-343.

Knutsen, C. H., Nygård, H. M., & Wig, T. (2017). Autocratic Elections: Stabilizing Tool or Force for Change? *World Politics, 69*(1), 98-143.

Kuenzi, M., & Lambright, G. M. (2011). Who votes in Africa? An examination of electoral participation in 10 African countries. *Party Politics, 17*(6), 767-799.

Kuran, T. (1989). Sparks and prairie fires: A theory of unanticipated political revolution. *Public Choice, 61*(1), 41-74.

Kurbalija, J. (2014). *An introduction to internet governance* (6th ed.). Diplo Foundation.

La Porta, R., Lopez-De-Silanes, F., & Shleifer, A. (1999). Corporate ownership around the world. *The Journal of Finance, 54*(2), 471-517.

Laffont, J. J., & Tirole, J. (2000). *Competition in telecommunications*. MIT Press.

Lam, P.-L., & Shiu, A. (2010). Economic growth, telecommunications development and productivity growth of the telecommunications sector: Evidence around the world. *Telecommunications Policy, 34*(4), 185-199.

Lambsdorff, J. G., & Cornelius, P. (2000). Corruption, foreign investment and growth. In K. Schwab, L. Cook, P. Cornelius, J.D. Sachs, S. Sievers, & A. Warner (Eds.), *The Africa competitiveness report* (Vol. 2001, pp. 70-78). Oxford University Press.

Lecraw, D. (1977). Direct investment by firms from less developed countries. *Oxford Economic Papers, 29*(3), 442-457.

Lecraw, D. J. (1984). Bargaining power, ownership, and profitability of transnational corporations in developing countries. *Journal of International Business Studies, 15*(1), 27-43.

Ledyaeva, S., Karhunen, P., & Kosonen, R. (2013). Birds of a feather: Evidence on commonality of corruption and democracy in the origin and location of foreign investment in Russian regions. *European Journal of Political Economy, 32*, 1-25.

Leech, D. (2013). Shareholder voting power and ownership control of companies. In M. J. Holler & H. Nurmi (Eds.), *Power, voting, and voting power: 30 years after* (pp. 475-498). Springer.

Leiponen, A. (2006). National styles in the setting of global standards. The relationship between firms' standardization strategies and national origins. In J. Zysman & A. L. Newman (Eds.), *How revolutionary was the digital revolution? National responses, market transitions, and global technology* (pp. 338-358). Stanford Business Books.

Lemos, R., & Scur, D. (2018). *All in the family? CEO choice and firm organization*. CEP Discussion Papers No 1528, LSE Centre for Economic Performance, London.

Lessig, L. (2006). *Code 2.0* (2nd ed.). Basic Books.

Letsa, N. W. (2019). The political geography of electoral autocracies: The influence of party strongholds on political beliefs in Africa. *Electoral Studies, 60*, 102047.

Levitsky, S., & Way, L. A. (2002). The rise of competitive authoritarianism. *Journal of Democracy, 13*(2), 51-65.

Levitsky, S., & Way, L. A. (2010). *Competitive authoritarianism: Hybrid regimes after the Cold War*. Cambridge University Press.

Lichtman, D., & Posner, E. (2006). Holding Internet Service Providers Accountable. *Supreme Court Economic Review, 14*, 221-259.

Lindberg, S. I. (2004). The democratic qualities of competitive elections: Participation, competition and legitimacy in Africa. *Commonwealth & Comparative Politics, 42*(1), 61-105.

Lührmann, A., Lindberg, S., & Tannenberg, M. (2017). *Regimes in the World (RIW): A Robust Regime Type Measure Based on V-Dem*. Retrieved 24.02.2021 from https://ssrn.com/abstract=2971869

Lührmann, A., Tannenberg, M., & Lindberg, S. I. (2018). Regimes of the world (RoW): Opening new avenues for the comparative study of political regimes. *Politics and Governance, 6*(1), 60–77.

Luong, P. J., & Weinthal, E. (2006). Rethinking the resource curse: Ownership structure, institutional capacity, and domestic constraints. *Annual Review of Political Science, 9*, 241-263.

Luong, P. J., & Weinthal, E. (2010). *Oil is not a curse. Ownership structure and institutions in Soviet successor states*. Cambridge University Press.

Lutscher, P. M., Weidmann, N. B., Roberts, M. E., Jonker, M., King, A., & Dainotti, A. (2020). At home and abroad: The use of denial-of-service attacks during elections in nondemocratic regimes. *Journal of Conflict Resolution, 64*(2-3), 373-401.

MacKinnon, R. (2011). Liberation technology: China's networked authoritarianism. *Journal of Democracy, 22*(2), 32-46.

Maerz, S. F., Lührmann, A., Hellmeier, S., Grahn, S., & Lindberg, S. I. (2020). State of the world 2019: autocratization surges – resistance grows. *Democratization, 27*(6), 909-927.

Magaloni, B. (2008). Credible power-sharing and the longevity of authoritarian rule. *Comparative Political Studies, 41*(4-5), 715-741.

Magaloni, B., & Kricheli, R. (2010). Political order and one-party rule. *Annual Review of Political Science, 13*, 123-143.

Main, L. (2001). The global information infrastructure: Empowerment or imperialism? *Third World Quarterly, 22*(1), 83-97.

Marchant, E., & Stremlau, N. (2020). Internet shutdowns in Africa| The changing landscape of internet shutdowns in Africa—Introduction. *International Journal of Communication, 14*, 8.

Mare, A. (2016). Baba Jukwa and the digital repertoires of connective action in a 'competitive authoritarian regime': The case of Zimbabwe. In B. Mutsvairo (Ed.), *Digital activism in the social media era* (pp. 45-68). Springer.

Mariotti, S., Mutinelli, M., Nicolini, M., & Piscitello, L. (2015). Productivity spillovers from foreign multinational enterprises to domestic manufacturing firms: To what extent does spatial proximity matter? *Regional Studies, 49*(10), 1639-1653.

Markus, S., & Charnysh, V. (2017). The flexible few: Oligarchs and wealth defense in developing democracies. *Comparative Political Studies, 50*(12), 1632-1665.

Marshall, M. G., Gurr, T. R., & Jaggers, K. (2014). *Political regime characteristics and transitions, 1800-2013*. Center for Systemic Peace.

Marshall, M. G., Gurr, T. R., & Jaggers, K. (2017). *Political regime characteristics and transitions, 1800-2013*. Center for Systemic Peace.

Martin, J. A. (2014). Mobile media and political participation: Defining and developing an emerging field. *Mobile Media & Communication, 2*(2), 173-195.

McCarthy, J. D., & Zald, M. N. (1977). Resource mobilization and social movements: A partial theory. *American Journal of Sociology, 82*(6), 1212-1241.

Mesquita, B. B. d., & Smith, A. (2009). Political survival and endogenous institutional change. *Comparative Political Studies, 42*(2), 167-197.

Micek, P., & Kenyanito, E. P. (2016). *Telcos find backbone, deny Guinea's request for users' data*. Retrieved 22.01.2019 from https://www.accessnow.org/telcos-find-backbone-deny-guineas-request-for-users-data/

Michaelsen, M. (2016). Exit and voice in a digital age: Iran's exiled activists and the authoritarian state. *Globalizations, 15*(2), 248-264.

Miller, D. (1987). The genesis of configuration. *The Academy of Management Review, 12*(4), 686-701.

Miller, D., Le Breton-Miller, I., & Lester, R. H. (2010). Family ownership and acquisition behavior in publicly-traded companies. *Strategic Management Journal, 31*(2), 201-223.

Milner, H. V. (2006). The digital divide. *Comparative Political Studies, 39*(2), 176-199.

Moon, C. (2019). Political institutions and FDI inflows in autocratic countries. *Democratization, 26*(7), 1256-1277.

MTN Uganda [@mtnug]. (2021). *MTN Uganda has*. Retrieved 13.02.2021 from https://twitter.com/mtnug/status/1349298148489924608

Mudambi, R. (2003). *Privatization and globalization: The changing role of the state in business*. Edward Elgar Publishing.

Musisi, F. (2016, February 14). Queries as Electoral Commission bans phones at polling stations. *Daily Monitor*.

Mutahi, P., & Kimari, B. (2017). *The impact of social media and digital technology on electoral violence in Kenya*. IDS. Retrieved 01.03.2021 from https://opendocs.ids.ac.uk/opendocs/bitstream/handle/20.500.12413/13159/Wp493_Online.pdf?sequence=287

Mutsvairo, B. (2016). Dovetailing desires for democracy with new ICTs' potentiality as platform for activism. In B. Mutsvairo (Ed.), *Digital activism in the social media era* (pp. 3-23). Springer.

Myovella, G., Karacuka, M., & Haucap, J. (2020). Digitalization and economic growth: A comparative analysis of sub-Saharan Africa and OECD economies. *Telecommunications Policy, 44*(2), 101856.

Newman, L. H. (2019). *How the Iranian government shut off the internet*. Retrieved 26.02.2020 from https://www.wired.com/story/iran-internet-shutoff/

Niaki, A. A., Cho, S., Weinberg, Z., Hoang, N. P., Razaghpanah, A., Christin, N., & Gill, P. (2020). IClab: a global, longitudinal internet censorship measurement platform. *Proceedings of the 2020 IEEE Symposium on Security and Privacy (SP)* (135-151), IEEE.

Nielsen, R. A. (2014). Rewarding Human Rights? Selective Aid Sanctions against Repressive States. *International Studies Quarterly, 57*(4), 791-803.

Nieuwenhuis, R., Te Grotenhuis, M., & Pelzer, B. (2012). Influence.ME: tools for detecting influential data in mixed effects models. *R Journal, 4*(2), 38–47.

Nisbet, E. C., Stoycheff, E., & Pearce, K. E. (2012). Internet use and democratic demands: A multinational, multilevel model of internet use and citizen attitudes about democracy. *Journal of Communication, 62*(2), 249-265.

Nofsinger, J. R., & Sias, R. W. (1999). Herding and feedback trading by institutional and individual investors. *The Journal of Finance, 54*(6), 2263-2295.

Nothias, T. (2020). Access granted: Facebook's free basics in Africa. *Media, Culture & Society, 42*(3), 329-348.

Nyirenda-Jere, T., & Biru, T. (2015). *Internet development and internet governance in Africa*. Retrieved 31.10.2017 from https://www.internetsociety.org/wp-content/uploads/2017/08/InternetInAfrica-2015070820Final.pdf

Nyokabi, D. M., Diallo, N., Ntesang, N. W., White, T. K., & Ilori, T. (2019). The right to development and internet shutdowns: Assessing the role of information and communications technology in democratic development in Africa.

Odhiambo, S. A. (2017). *Internet shutdowns during elections*. Retrieved 28.12.2020 from https://africaupclose.wilsoncenter.org/internet-shutdowns-during-elections/

Okolloh, O. (2009). Ushahidi, or 'testimony': Web 2.0 tools for crowdsourcing crisis information. *Participatory learning and action, 59*(1), 65-70.

Oluka, B. H. (2016). *Cash squeeze, intimidation rock FDC vote-guarding plans*. The Observer. Retrieved 23.02.2021 from https://www.observer.ug/news-headlines/42524-cash-squeeze-intimidation-rock-fdc-vote-guarding-plans-2

Olukotun, D. B. (2016). *Internet shutdowns - an explainer*. Retrieved 25.01.2017 from http://www.dw.com/en/internet-shutdowns-an-explainer/a-36731481

Omanga, D. (2019). WhatsApp as 'digital publics': the Nakuru Analysts and the evolution of participation in county governance in Kenya. *Journal of Eastern African Studies, 13*(1), 175-191.

Oyedemi, T. (2015). Participation, citizenship and internet use among South African youth. *Telematics and Informatics, 32*(1), 11-22.

Pallin, C. (2017). Internet control through ownership: the case of Russia. *Post-Soviet Affairs, 33*(1), 16-33.

Pemstein, D., Meserve, S. A., & Melton, J. (2010). Democratic compromise: A latent variable analysis of ten measures of regime type. *Political Analysis, 18*(4), 426-449.

Pierskalla, J. H. (2009). Protest, Deterrence, and Escalation: The Strategic Calculus of Government Repression. *Journal of Conflict Resolution, 54*(1), 117-145.

Pierskalla, J. H., & Hollenbach, F. M. (2013). Technology and collective action: The effect of cell phone coverage on political violence in Africa. *American Political Science Review, 107*(2), 207-224.

Pitkin, H. F. (1972). *Wittgenstein and justice*. University of California Press.

Presidential, parliamentary elections in embarrassing mess. (2016). The Observer. Retrieved 23.02.2021 from https://observer.ug/news-headlines/42678-presidential-parliamentary-elections-in-embarrassing-mess

Privacy International. (2015). *For God and my president: State surveillance in Uganda*. Privacy International. https://www.privacyinternational.org/sites/default/files/Uganda_Report_1.pdf

Przeworski, A., Alvarez, R. M., Alvarez, M. E., Cheibub, J. A., Limongi, F., & Neto, F. P. L. (2000). *Democracy and development: Political institutions and well-being in the world, 1950-1990* (Vol. 3). Cambridge University Press.

Qin, B., Strömberg, D., & Wu, Y. (2017). Why does China allow freer social media? Protests versus surveillance and propaganda. *Journal of Economic Perspectives, 31*(1), 117-140.

Ranking Digital Rights. (2017). *Ranking Digital Rights corporate accountability index*. Retrieved 28.12.2020 from https://rankingdigitalrights.org/index2017

Rapoport, D. C., & Weinberg, L. (2000). Elections and violence. *Terrorism and Political Violence, 12*(3-4), 15-50.

Rasmussen, T. (2014). Internet and the political public sphere. *Sociology Compass, 8*(12), 1315-1329.

Rauchfleisch, A., & Kovic, M. (2016). The internet and generalized functions of the public sphere: Transformative potentials from a comparative perspective. *Social Media + Society, 2*(2).

Rauschenbach, M., & Paula, K. (2019). Intimidating voters with violence and mobilizing them with clientelism. *Journal of Peace Research*, 1-15.

Resnick, D., & Van de Walle, N. (2013). *Democratic trajectories in Africa: Unravelling the impact of foreign aid*. Oxford University Press.

Reuber, G. L., Crookell, H., Emerson, M., & Gallais-Hamonno, G. (1973). *Private foreign investment in development*. Clarendon Press.

Reuter, O. J., & Szakonyi, D. (2013). Online social media and political awareness in authoritarian regimes. *British Journal of Political Science, 45*(1), 29-51.

Reuters. (2013). *Eritrea offers stake in state telco, but not to foreigners*. Retrieved 25.01.2021 from https://www.tesfanews.net/eritrea-offers-stake-in-state-telco-but-not-to-foreigners/

Ritzen, Y. (2018). *Cameroon internet shutdowns cost Anglophones millions*. Retrieved 10.01.2020 from https://www.aljazeera.com/news/2018/01/cameroon-internet-shutdowns-cost-anglophones-millions-180123202824701.html

Rød, E. G., & Weidmann, N. B. (2015). Empowering activists or autocrats? The internet in authoritarian regimes. *Journal of Peace Research, 52*(3), 338-351.

Rodan, G. (1998). The internet and political control in Singapore. *Political Science Quarterly, 113*(1), 63-89.

Rodine-Hardy, K. (2013). *Global markets and government regulation in telecommunications*. Cambridge University Press.

Rommel, T. (2018). *Foreign direct investment and the politics of autocratic survival*, [Doctoral Thesis, University of Zurich]. Switzerland.

Rudbeck, J., Mukherjee, E., & Nelson, K. (2016). When autocratic regimes are cheap and play dirty: The transaction costs of repression in South Africa, Kenya, and Egypt. *Comparative Politics, 48*(2), 147-166.

Rufyikiri, G. (2016). *Grand corruption in Burundi: a collective action problem which poses major challenges for governance reforms*. Retrieved 23.01.2021 from https://medialibrary.uantwerpen.be/oldcontent/container2673/files/Publications/WP/2016/08-Rufiyikiri.pdf

Ruijgrok, K. (2017). From the web to the streets: Internet and protests under authoritarian regimes. *Democratization, 24*(3), 498-520.

Ruijgrok, K. (2020). Illusion of control: How internet use generates anti-regime sentiment in authoritarian regimes. *Contemporary Politics*, 1-24.

Rydzak, J. (2018). *Disconnected. A human rights-based approach to network disruptions*. Global Network Initiative. https://globalnetworkinitiative.org/gin_tnetnoc/uploads/2018/06/Disconnected-Report-Network-Disruptions.pdf

Rydzak, J., Karanja, M., & Opiyo, N. (2020). Internet shutdowns in Africa| Dissent does not die in darkness: Network shutdowns and collective action in African countries. *International Journal of Communication, 14*, 4265-4286.

Sallai, D., & Schnyder, G. (2020). What is "authoritarian" about authoritarian capitalism? The dual erosion of the private–public divide in state-dominated business systems. *Business & Society*, 0007650319898475.

Schedler, A. (2006). *Electoral authoritarianism. The dynamics of unfree competition*. Lynne Rienner Publishers.

Scherer, A. G., & Palazzo, G. (2011). The new political role of business in a globalized world – A review of a new perspective on CSR and its implications for the firm, governance, and democracy *Journal of Management studies, 48*(4), 899-931.

Schmotz, A., & Tansey, O. (2018). Regional autocratic linkage and regime survival. *European Journal of Political Research, 57*(3), 662-686.

Schneider, C. Q., & Maerz, S. F. (2017). Legitimation, cooptation, and repression and the survival of electoral autocracies. *Zeitschrift für Vergleichende Politikwissenschaft, 11*(2), 213-235.

Schneider, C. Q., & Wagemann, C. (2010). Standards of good practice in qualitative comparative analysis (QCA) and fuzzy-sets. *Comparative Sociology, 9*(3), 397-418.

Schneider, F., & Frey, B. S. (1985). Economic and political determinants of foreign direct investment. *World Development, 13*(2), 161-175.

Schneider, V., Fink, S., & Tenbücken, M. (2005). Buying out the state: a comparative perspective on the privatization of infrastructures. *Comparative Political Studies, 38*(6), 704-727.

Schoentgen, A., & Gille, L. (2017). Valuation of telecom investments in sub-Saharan Africa. *Telecommunications Policy, 41*(7), 537-554.

Seawright, J., & Gerring, J. (2008). Case selection techniques in case study research: A menu of qualitative and quantitative Options. *Political Research Quarterly, 61*(2), 294-308.

Shleifer, A., & Vishny, R. W. (1997). A survey of corporate governance. *The Journal of Finance, 52*(2), 737-783.

Simison, E. (2020). Supporters and opposition in authoritarian legislatures. *The Journal of Legislative Studies*, 1-20.

Simmons, E. (2014). Grievances do matter in mobilization. *Theory and Society, 43*(5), 513-546.

Sjögren, A. (2018). Wielding the stick again: the rise and fall and rise of state violence during presidential elections in Uganda. In M. Söderberg Kovacs & J. Bjarnesen (Eds.), *Violence in African elections: between democracy and Big Man politics* (pp. 47-66). Zed Books.

Ssekika, E. (2016). *Kiggundu: only EC to announce results*. Retrieved 23.02.2021 from https://observer.ug/news-headlines/42407-kiggundu-only-ec-to-announce-results

Stegmueller, D. (2011). Apples and oranges? The problem of equivalence in comparative research. *Political Analysis, 19*(4), 471-487.

Stier, S. (2017). Internet diffusion and regime type: Temporal patterns in technology adoption. *Telecommunications Policy, 41*(1), 25-34.

Stockmann, D. (2013). *Media commercialization and authoritarian rule in China*. Cambridge University Press.

Stone, A., Shiffman, S., Atienza, A., & Nebeling, L. (2007). *The science of real-time data capture: Self-reports in health research*. Oxford University Press.

Stoycheff, E., Burgess, G. S., & Martucci, M. C. (2020). Online censorship and digital surveillance: The relationship between suppression technologies and democratization across countries. *Information, Communication & Society, 23*(4), 474-490.

Strange, R. (2018). Corporate ownership and the theory of the multinational enterprise. *International Business Review, 27*(6), 1229-1237.

Sur, S., Gassmann, H., & Zhang, J. (2019). Defining Ownership: An empirical assessment of the ownership measures. *Canadian Journal of Administrative Sciences, 36*(1), 5-19.

Sur, S., Lvina, E., & Magnan, M. (2013). Why do boards differ? Because owners do: Assessing ownership impact on board composition. *Corporate Governance: An International Review, 21*(4), 373-389.

Sutherland, E. (2019). *Law and order in Africa–policing social networks*. Paper presented at European Conference on African Studies (ECAS) 2019, Edinburgh.

Tangri, R., & Mwenda, A. M. (2008). Elite corruption and politics in Uganda. *Commonwealth & Comparative Politics, 46*(2), 177-194.

Taye, B. (2019). *Targeted, cut off, and left in the dark. The #KeepItOn report on internet shutdowns in 2019*. Access Now. https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf

Taylor, I. (2006). China's oil diplomacy in Africa. *International Affairs, 82*(5), 937-959.

Ten Eyck, T. A. (2001). Does information matter? A research note on information technologies and political protest. *The Social Science Journal, 38*(1), 147-160.

Teo, T. K. (2019). Inequality under authoritarian rule [online publication]. *Government and Opposition*, https://www.cambridge.org/core/article/inequality-under-authoritarian-rule/72EB75A875F846DABE870C879A857BB0776367D.

Thomsen, S., & Pedersen, T. (2000). Ownership structure and economic performance in the largest european companies. *Strategic Management Journal, 21*(6), 689-705.

Tortora, B. (2014). *Africa continues going mobile*. Retrieved 30.10.2017 from http://www.gallup.com/poll/168797/africa-continues-going-mobile.aspx

Toshkov, D. (2016). *Research Design in Political Science*. Palgrave.

Truex, R. (2020). Authoritarian gridlock? Understanding delay in the Chinese legislative system. *Comparative Political Studies, 53*(9), 1455-1492.

Tucker, J. A. (2007). Enough! Electoral fraud, collective action problems, and post-Communist Colored Revolutions. *Perspectives on Politics, 5*(3), 535-551.

Tucker, J. A., Theocharis, Y., Roberts, M. E., & Barberá, P. (2017). From liberation to turmoil: Social media and democracy. *Journal of Democracy, 28*(4), 46-59.

Tufekci, Z., & Wilson, C. (2012). Social media and the decision to participate in political protest: Observations from Tahrir Square. *Journal of Communication, 62*(2), 363-379.

Turner, R. H., & Killian, L. M. (1957). *Collective behavior* (Vol. 3). Prentice-Hall Englewood Cliffs.

Tusiime, I., Nkundabanyanga, S. K., & Nkote, I. N. (2011). Corporate governance: Ownership structure, board structure and performance of public sector entities. *Journal of Public Administration and Policy Research, 9*(3), 250-260.

U.S. Department of State. (2017a). *Country reports on human rights practices for 2017. Equatorial Guinea*. Retrieved 28.12.2020 from https://2009-2017.state.gov/j/drl/rls/hrrpt/humanrightsreport//index.htm#wrapper

U.S. Department of State. (2017b). *Country reports on human rights practices for 2017. Ethiopia*. Retrieved 28.12.2020 from https://2009-2017.state.gov/j/drl/rls/hrrpt/humanrightsreport//index.htm#wrapper

Uganda government takes over troubled telecom. (2017). The East African. Retrieved 28.12.2020 from http://www.theeastafrican.co.ke/business/Uganda-government-takes-over-troubled-telecom/2560-3833146-8ojxtqz/index.html

Ulfelder, J. (2007). Natural-resource wealth and the survival of autocracy. *Comparative Political Studies, 40*(8), 995-1018.

UNDP. (2014). *Data*. Retrieved Oct 28 from http://hdr.undp.org/en/data

United Nations. (2016). *Oral revisions of 30 June*. Retrieved 28.12.2020 from https://www.article19.org/data/files/Internet_Statement_Adopted.pdf

Van Dam, C., Gregor, F., Brachotte, S., & Morrow, P. (2017). Corporate responsibility to respect human rights vis-à-vis legal duty of care. In A. Rubio, J. José, & K. Yiannibas (Eds.), *Human rights in business. Removal of barriers to access to justice in the European Union* (pp. 119–138). Routledge.

van Ham, C., & Lindberg, S. I. (2015). From sticks to carrots. Electoral manipulation in Africa, 1986–2012. *Government and Opposition, 50*(3), 521-548.

Vargas-Leon, P. (2016). Tracking internet shutdown practices: Democracies and hybrid regimes. In F. Musiani, D. L. Cogburn, L. DeNardis, & N. S. Levinson (Eds.), *The turn to internet infrastructure in internet governance* (pp. 167-189). Palgrave Macmillan.

Verba, S., Brady, S. V., Schlozman, K. L., & Brady, H. E. (1995). *Voice and equality: Civic voluntarism in American politics*. Harvard University Press.

Viettel wins mobile concession in Burundi. (2014). Retrieved 23.01.2021 from https://www.commsupdate.com/articles/2014/02/17/viettel-wins-mobile-concession-in-burundi/

Villalonga, B. (2000). Privatization and efficiency: differentiating ownership effects from political, organizational, and dynamic effects. *Journal of Economic Behavior & Organization, 42*(1), 43-74.

Vimalkumar, M., Singh, J. B., & Sharma, S. K. (2020). Exploring the multi-level digital divide in mobile phone adoption: A comparison of developing nations [Online Article]. *Information Systems Frontiers*, https://doi.org/10.1007/s10796-10020-10032-10795.

Vodafone. (2014). *Country-by-country disclosure of law enforcement assistance demands*. Retrieved 28.12.2020 from http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement/country_by_country.html

von Borzyskowski, I., & Kuhn, P. M. (2020). Dangerously informed: Voter information and pre-electoral violence in Africa. *Journal of Peace Research, 57*(1), 15-29.

Von Soest, C. (2015). Democracy prevention: The international collaboration of authoritarian regimes. *European Journal of Political Research, 54*(4), 623-638.

Vu, K. M. (2011). ICT as a source of economic growth in the information age: Empirical evidence from the 1996-2005 period. *Telecommunications Policy, 35*(4), 357-372.

Wagner, B. (2018). Authoritarian practices in the digital age| Understanding internet shutdowns: A case study from Pakistan. *International Journal of Communication, 12*, 3917-3938.

Wairagala, W. (2009). Bringing affordable telecommunications services to Uganda. A policy narrative and analysis. Association for Progressive Communications (APC), South Africa.

Wallsten, S. J. (2001). An econometric analysis of telecom competition, privatization, and regulation in Africa and Latin America. *The Journal of Industrial Economics, 49*(1), 1-19.

Walsh, J. P., & Seward, J. K. (1990). On the efficiency of internal and external corporate control mechanisms. *Academy of Management Review, 15*(3), 421-458.

Warf, B. (2012). *Global Geographies of the Internet*. Springer

Waterbury, J. (1999). Fortuitous byproducts. In L. Anderson (Ed.), *Transitions to democracy* (pp. 261-283). Columbia University Press.

Wavre, V. (2018). *Policy diffusion and telecommunications regulation*. Springer.

Wavre, V. (2020). The rise of the policy-takers: Universal service policy adoption in Jordan and Morocco. *Journal of Digital Media & Policy, 15*(6).

Weber, R. H. (2011). Politics through social networks and politics by government blocking: Do we need new rules? *International Journal of Communication, 5*, 1186-1194.

Wegenast, T., & Schneider, G. (2017). Ownership matters: Natural resources property rights and social conflict in Sub-Saharan Africa. *Political Geography, 61*, 110-122.

Weidmann, N. B. (2015). Communication networks and the transnational spread of ethnic conflict. *Journal of Peace Research, 52*(3), 285-296.

Weidmann, N. B. (2016). A closer look at reporting bias in conflict event data. *American Journal of Political Science, 60*(1), 206-218.

Weidmann, N. B., & Rød, E. G. (2019). *The internet and political protest in autocracies*. Oxford University Press.

Weyland, K. (2017). Autocratic diffusion and cooperation: The impact of interests vs. ideology. *Democratization, 24*(7), 1235-1252.

Williams, M. D. J., Mayer, R., & Minges, M. (2011). *Africa's ICT infrastructure: Building on the mobile revolution*. World Bank Publications.

Wilson, M. C. (2014). A discreet critique of discrete regime type data. *Comparative Political Studies, 47*(5), 689-714.

Wilson, S. L. (2015). How to control the internet: Comparative political implications of the internet's engineering. *First Monday [Online], 20*(2).

Workneh, T. W. (2020). Social media, protest, & outrage communication in Ethiopia: toward fractured publics or pluralistic polity? *Information, Communication & Society*, 1-20.

World Bank. (2020a). *National panel survey 2015-2016*. Retrieved 02.03.2021 from https://microdata.worldbank.org/index.php/catalog/3460

World Bank. (2020b). *The World Bank open data*. Retrieved 28.01.2021 from https://data.worldbank.org/

Wright, J., Darer, A., & Farnan, O. (2018). *On identifying anomalies in Tor usage with applications in detecting internet censorship*. Proceedings of the 10th ACM Conference on Web Science, Amsterdam, Netherlands. https://doi.org/10.1145/3201064.3201093

Xu, X. (2020). To repress or to co-opt? Authoritarian control in the age of digital surveillance [online publication]. *American Journal of Political Science*, https://doi.org/10.1111/ajps.12514.

Xynou, M., Basso, S., Padmanabhan, R., & Filastò, A. (2021). *Uganda: Data on internet blocks and nationwide internet outage amid 2021 general election*. Retrieved 29.01.2021 from https://ooni.org/post/2021-uganda-general-election-blocks-and-outage/

Xynou, M., & Filastò, A. (2020). *Burundi blocks social media amid 2020 general election*. Retrieved 23.01.2021 from https://ooni.org/post/2020-burundi-blocks-social-media-amid-election/

Xynou, M., Filastò, A., Alimardani, M., Kouhi, S., Bowen, K., Vmon, & Media, A. S. S. (2017). *Internet censorship in Iran: Network measurement findings from 2014-2017*. Retrieved 20.12.2020 from https://ooni.org/post/iran-internet-censorship/

Yan, X., & Zhang, Z. (2009). Institutional investors and equity returns: Are short-term institutions better informed? *The Review of Financial Studies, 22*(2), 893-924.

Young, L. E. (2020). Who dissents? Self-efficacy and opposition action after state-sponsored election violence. *Journal of Peace Research, 57*(1), 62-76.

Zeitzoff, T. (2017). How social media is changing conflict. *Journal of Conflict Resolution, 61*(9), 1970-1991.

APPENDICES

Appendix A 115

Appendix A1. Frequency of social media filtering, 2019 115

Appendix A2. Frequency of internet and social media blocking in Africa, 2019 115

Appendix A3. Key variables: Conceptualisation and operationalisation 116

Appendix A4. Fixed and mobile broadband penetration in worldwide, 2000-2019 118

Appendix B 119

Appendix B1. Electoral violence during African elections, 2015-2018 119

Appendix B2. Use of ICT during elections 120

Appendix B3. Electoral violence during African elections 2015-2018 121

Appendix B4. Distribution of best linear unbiased predictors (BLUPs) 122

Appendix B5. List of interview partners 123

Appendix B6. Questions included in survey from Research World International Ltd. 124

Appendix B7. Reliability checks 125

Appendix B8. Likelihood of electoral violence 126

Appendix B9. Likelihood of electoral violence (excluding Kampala) 126

Appendix C 127

Appendix C1. Estimated effect of the share of SOE on democratisation (Geddes et al.) 127

Appendix D 128

Appendix D1. Aggregation rule for Burundi, 2019 128

Appendix D2. Headquarters of foreign shareholders and number of subsidiaries (2000-2019) 129

Appendix D3. Results from linear mixed models (t-1) 130

Appendix D4. Means, standard deviations, and correlations 131

Appendix D5. Linear mixed models including the share of public-domestic ISPs 132

Appendix E 133

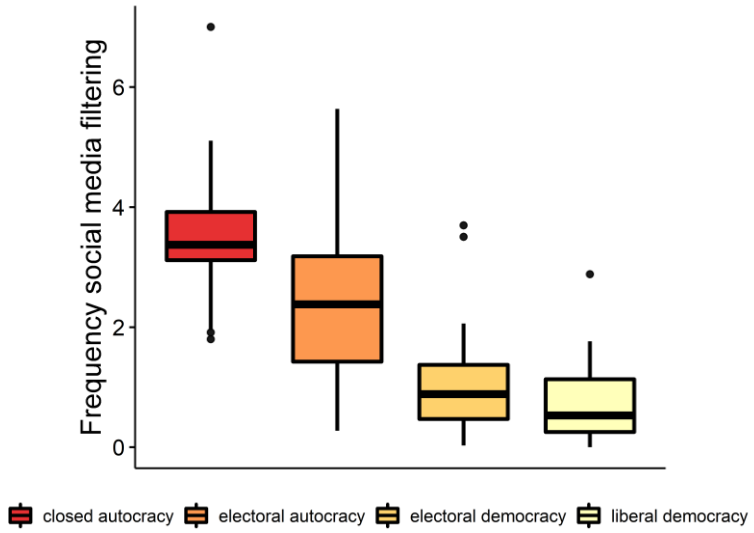
Appendix E1. Raw data 133

Appendix E2. Truth table 134

Appendix E3. csQCA output with Gabon recoded as autocracy 135

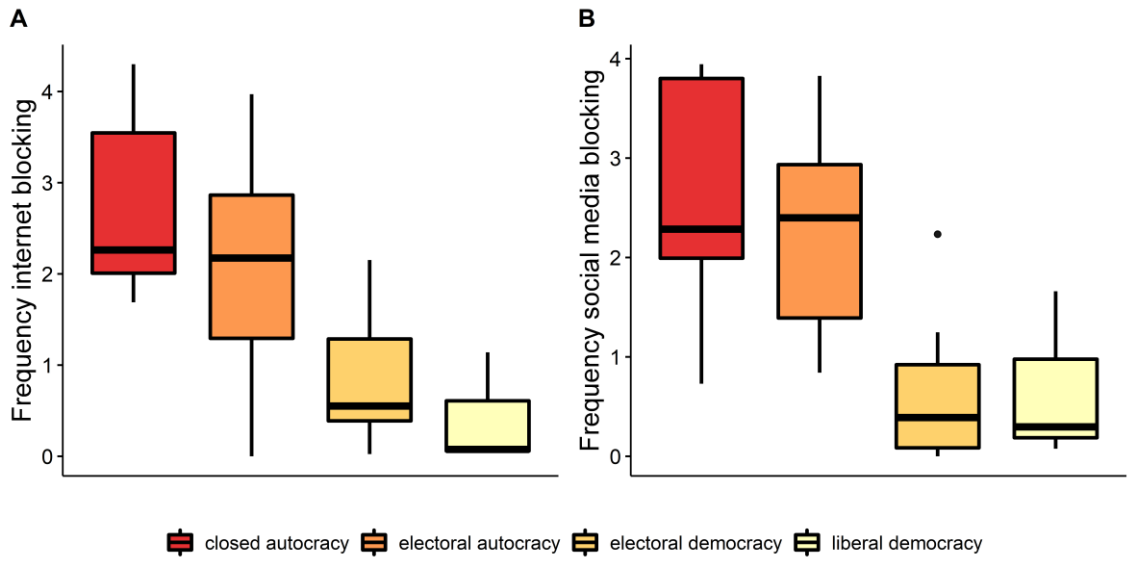
Appendix A

Appendix A1. Frequency of social media filtering, 2019



Note: The frequency of social media filtering (v2smgovsmcenprc) comes from the Varieties of Democracy project (V-Dem; Coppedge *et al.*, 2020b). Higher values indicate higher frequencies of filtering.

Appendix A2. Frequency of internet and social media blocking in Africa, 2019



Note: Variables for frequency of internet shutdowns (*v2govshut*) and social media shutdowns (*v2smgovsm*) come from the Varieties of Democracy project (V-Dem; Coppedge *et al.*, 2020b). Higher values indicate higher frequencies of blocking.

Appendix A3. Key variables: Conceptualisation and operationalisation

Internet Service Providers

Internet Service Providers (ISP) are the companies that grant internet access to individual customers, the so-called 'last-mile', by managing the infrastructure that is underlying the internet (Kurbalija, 2014; DeNardis, 2012). These companies effectively control different physical and virtual layers of the internet (Vargas-Leon, 2016). The infrastructure which is used to provide internet access varies considerably across countries, most notably between the developed and developing countries. While in Western countries, most people connect to the internet via fixed-line broadband access, the vast majority of internet users in developing countries, and notably in Africa, relies on mobile networks (Hawthorne & Grzybowski, 2019).

In this thesis, I analyse all ISPs that have official state licenses to operate infrastructure and that started by providing Global System for Mobile Communications (GSM) services, also known as second generation (2G) services. All ISPs included in the Telecommunications Ownership and Control (TOSCO) dataset are listed as members of the GSM Association (GSMA) plus a few incumbent fixed-line providers and hence, due to the importance of mobile internet in Africa, provide a near-complete image of those companies providing internet access to individuals. This focus excludes all Mobile Virtual Network Providers (MVNOs) that only play a marginal role in the provision of internet services to private individual customers.

Internet Shutdowns

I follow Rydzak (2018: 6) in defining an internet disruption as any "intentional, significant disruption of electronic communication within a given area and/or affecting a predetermined group of citizens". This can range from full blocking of internet access, such as during Uganda's 2021 presidential elections (Xynou et al., 2021), to the blocking of access to specific websites only, such as during Burundi's 2020 presidential elections (Follow, 2020). The ways in which shutdowns are implemented technically vary, but mostly encompass either routing or packet forwarding mechanisms (Dainotti et al., 2014).[56] Official justifications for internet disruptions are manifold including the prevention of cheating during national exams, preventing the spread of fake news and hate speech, or safeguarding national security (Taye, 2019: 13). Yet, as empirical research demonstrates, such disruptions may actually pursue different goals such as muzzling activists or facilitating state repression (Gohdes, 2020; Ayalew, 2019).

[56] Routing on the internet is coordinated at the AS-level using Border Gateway Protocol (BGP) as the interdomain routing protocol. If an ISP withdraws its BGP routes from the internet, the destination addresses it advertises as prefixes—the block(s) of IP addresses that have been allocated to it by the regional internet registry—disappear from the internet and cannot be reached anymore. As for packet filtering, using information about the source and the destination of a packet, such as the IP address, an ISP can manipulate access control lists so to deny traffic to or from a specific IP address, such as social media websites.

I rely on data from the non-governmental organisation Access Now that crowdsources data on internet shutdowns based on individuals' reports (Access Now, 2016) and triangulate them with media reports. While media reporting may be unreliable, precisely in the context of authoritarian regimes (Weidmann, 2016), this does not seem to a be major issue for this thesis' purpose, which focuses on a small number of shutdown incidences for which cases were cross-checked.

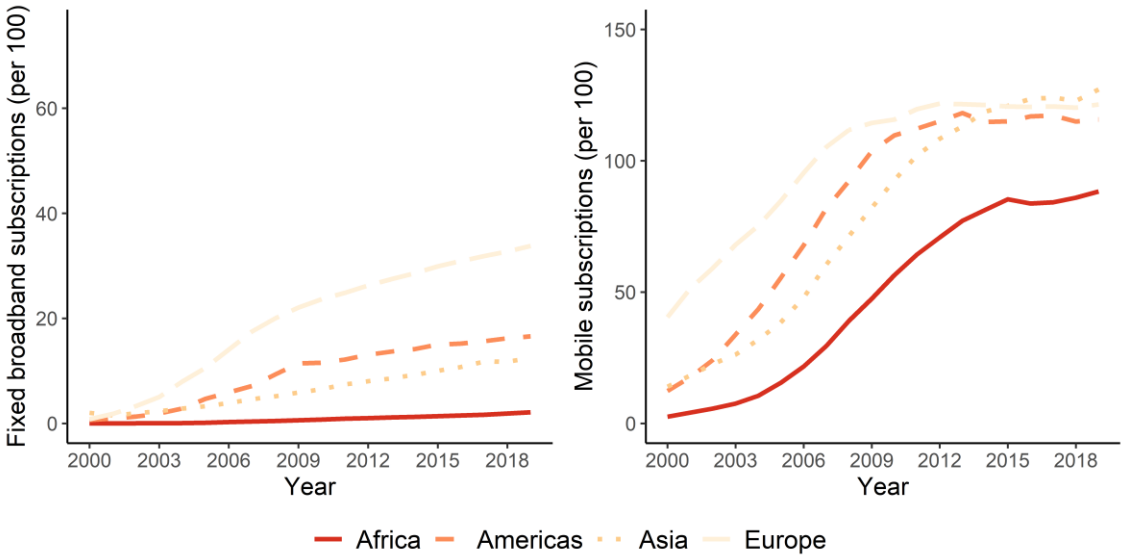
Ownership

Political economists define owners as the entity/-ies (i.e. a state, private actors, family, banks) holding the shares of a company. Following Shleifer and Vishny (1997), owners have an important role in company management exerted in particular through their voting rights but also through informal influence, such as during general assemblies or informal meetings with the management teams. According to this position, "[t]he role of shareholders is to determine all questions that are not routine, that cannot be decided by management because they are relevant to the relationship between the company and the capital market, and these include all fundamental matters affecting it" (Leech, 2013: 476). Owners can be classified along several dimensions, most notably based on their owner identity and origin (Thomsen & Pedersen, 2000; Strange, 2018).

I use data on ISP ownership for African countries between 2000 and 2019 based on a variety of sources. financial analysis software (e.g. Thomson and Reuters' Eikon [eikon.thomsonreuters.com] and Orbis [orbis.bvdinfo.com]), specialised blogs (e.g. Research ICT Africa [www.researchictafrica.net]), news websites like All Africa [AllAfrica.com] and Quartz Africa [https://qz.com/Africa], and Bloomberg Snapshot repositories [www.bloomberg.com]. This information is triangulated with the annual reports provided by the telecommunications companies and data from market research and analysis companies, in particular TeleGeography [www.telegeography.com].

The ownership data is aggregated in different ways throughout this thesis. To better understand the consequences of state ownership for authoritarian survival (Study 2), we rely on the proportion of ISPs that are majority-state owned as well as the overall proportion held by the state per country-year. In order to examine the role of foreign ownership in African autocracies, I use the aggregated proportion of ISPs majority-owned by foreign companies and majority-owned by foreign companies from autocracies (Study 3).

Appendix A4. Fixed and mobile broadband penetration in worldwide, 2000-2019



Note: Data comes from the International Telecommunications Union (ITU, 2021).

Appendix B

Appendix B1. Electoral violence during African elections, 2015-2018

	Model 1	Model 2
shutdown	-1.12 (0.26)***	-0.68 (0.26)*
polyarchy		3.00 (0.77)***
conflict intensity		0.32 (0.22)
GDP per capita		-0.04 (0.08)
internet penetration		0.00 (0.00)
political terror		-0.23 (0.18)
(Intercept)	-0.33 (0.13)*	-0.52 (1.85)
Adj. R^2	0.24	0.47
N	58	54

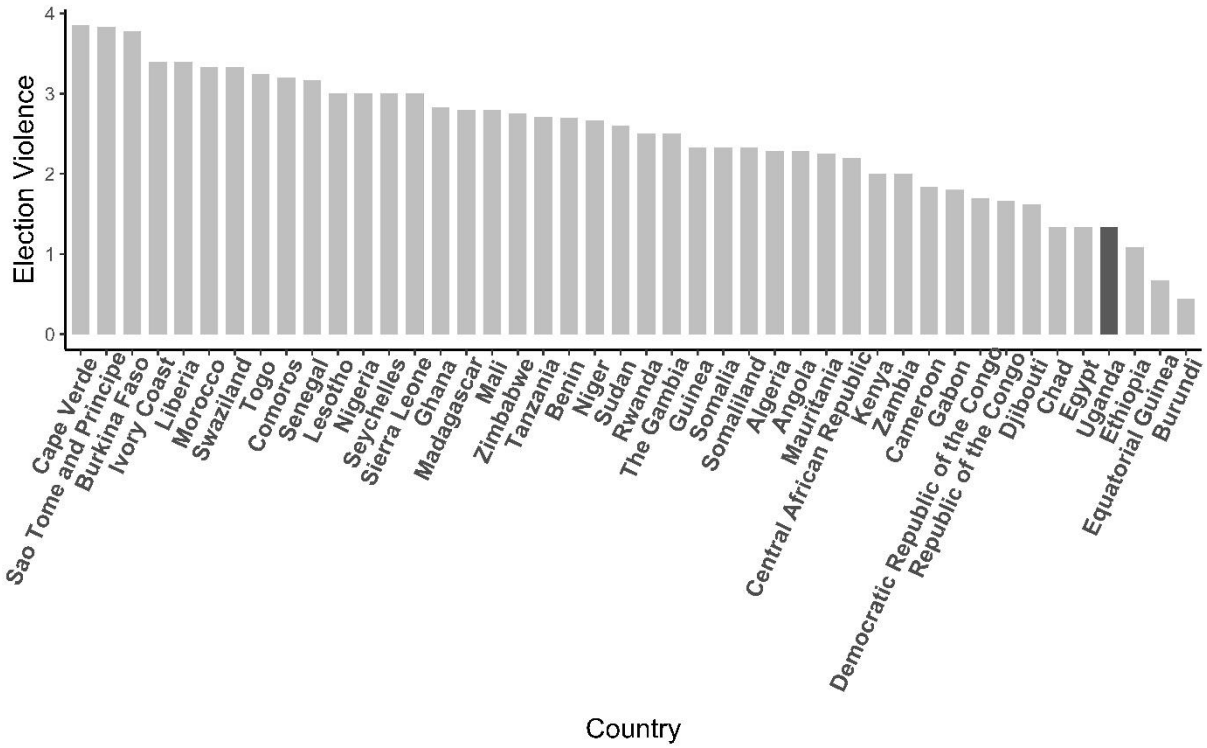
Note: $^{***}p < .001$, $^{**}p < .01$, $^{*}p < .05$*;* lower values indicate higher levels of electoral violence; the indicator for election violence committed by state authorities (*v2elintim*) comes from the Varieties of Democracy project (Coppedge *et al.*, 2020a); data for internet shutdowns from #KeepItOn campaign of the civil society organisation Access Now (2016). N = 58.

Appendix B2. Use of ICT during elections

	Model 1 (report)	Model 2 (report)	Model 3 (communicate)	Model 4 (communicate)
opposition	1.46 (0.27)***	1.40 (0.28)***	0.74 (0.24)**	0.56 (0.26)*
gender (male)		0.64 (0.30)*		0.52 (0.25)*
age (ref: 20-29)				
30 – 39		0.74 (0.32)*		0.45 (0.27)·
40-49		0.59 (0.43)		0.23 (0.37)
50-59		0.45 (0.54)		-0.37 (0.54)
60+		0.67 (0.71)		0.05 (0.68)
education		0.15 (0.09)		0.21 (0.08)*
economic status		0.05 (0.28)		0.34 (0.24)
urban setting		0.36 (0.31)		0.37 (0.27)
(Intercept)	-3.06 (0.23)***	-4.43 (0.48)***	-2.29 (0.18)***	-3.71 (0.42)***
AIC	486.69	453.28	655.11	594.08
N	847	790	847	790
N group (county)	82	82	82	82

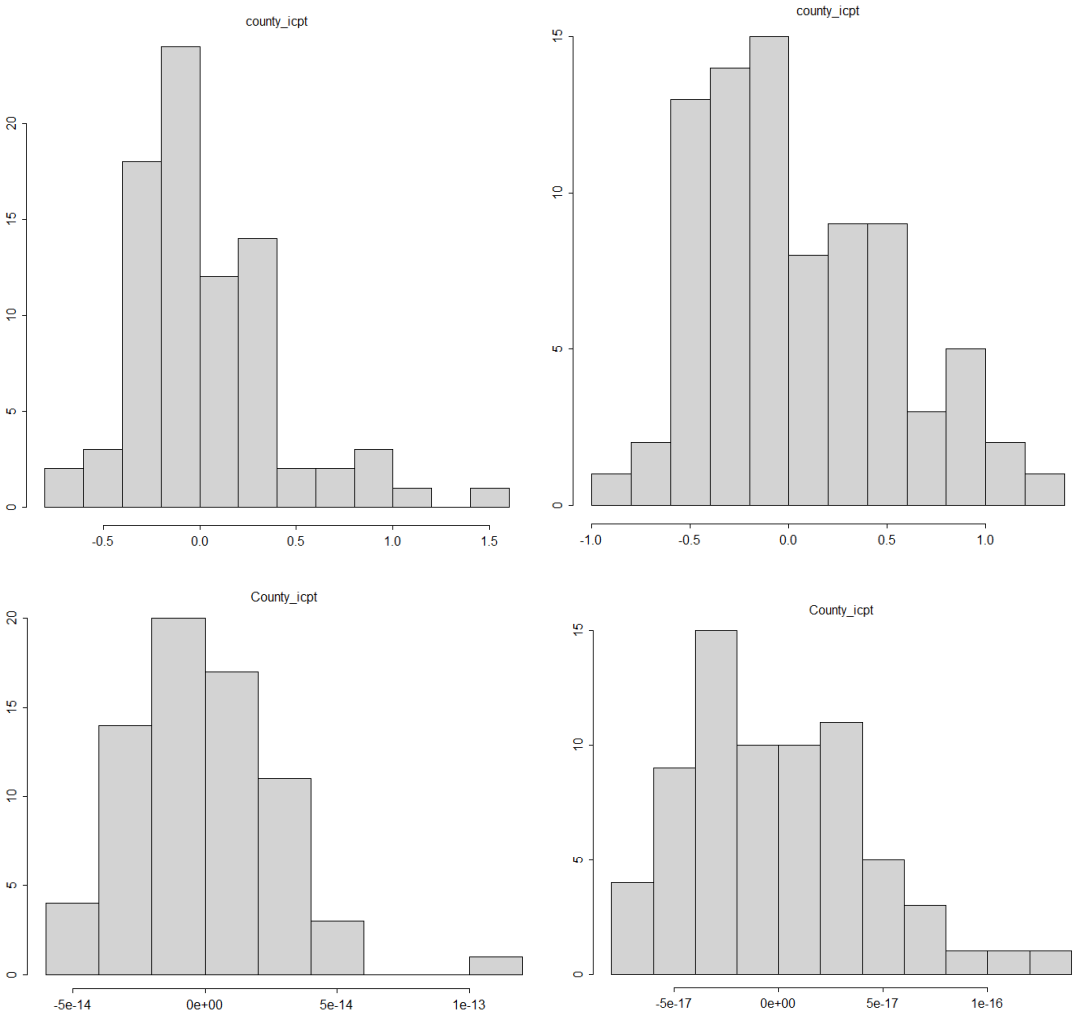
Note: $^{***}p < .001$, $^{**}p < .01$, $^{*}p < .05$, $^{+}p < .1$; models 1 and 2 use citizens' intention to use of social media to report about the conduct of elections and models 3 and 4 citizens' intention to use social media to communicate participation in elections as dependent variable (see question 3, Appendix B6).

Appendix B3. Electoral violence during African elections 2015-2018



Note: Lower scores indicate higher levels of election violence. The indicator for election violence (v2elintim) comes from the Varieties of Democracy project (Coppedge et al., 2020). *N* = 44.

Appendix B4. Distribution of best linear unbiased predictors (BLUPs)



Note: Plots indicate the distribution of BLUPs for the models with ICT to report (upper left), ICT use to communicate (upper right), violence udring polling (lower left) and violence during vote counting (lower right) as dependent variable.

Appendix B5. List of interview partners

Code	Position	Location	Date
UG1	Civil Society Organisation	Kampala	23.10.2018
UG2	Journalist	Kampala	24.10.2018
UG3	Journalist	Kampala	24.10.2018
UG4	Politician (independent)	Kampala	29.10.2018
UG5	Politician (FDC)	Kampala	29.10.2018
UG6	Politician (independent)	Gulu	31.10.2018
UG7	Politician (FDC)	Gulu	31.10.2018
UG8	Journalist	Gulu	31.10.2018
UG9	Politician (FDC)	Gulu	31.10.2018
UG10	Civil Society Organisation	Gulu	1.11.2018
UG11	Civil Society Organisation	Gulu	1.11.2018
UG12	Politician (FDC)	Gulu	1.11.2018
UG13	Electoral Commission	Gulu	1.11.2018
UG14	Politician (DP)	Kitgum	2.11.2018
UG15	Politician (FDC)	Kitgum	2.11.2018
UG16	Politician (NRM)	Kitgum	2.11.2018
UG17	Politician (DP)	Kitgum	2.11.2018
UG18	Electoral Commission	Kitgum	3.11.2018
UG19	Politician (NRM)	Kitgum	3.11.2018
UG20	Politician (FDC)	Kitgum	3.11.2018
UG21	Politician (DP)	Kitgum	3.11.2018
UG22	Politician (FDC)	Gulu	5.11.2018
UG23	Civil Society Organisation	Kampala	6.11.2018
UG24	Politician (FDC)	Kampala	6.11.2018

Appendix B6. Questions included in survey from Research World International Ltd.

1) At the time of the 2016 presidential elections, was there a political party that you supported more than the others- and, if yes, which of the following?

Political Party	Code
None	0
National Resistance Movement (NRM)	1
Forum for Democratic Change (FDC)	2
Democratic Party (DP)	3
Uganda's People's Congress (UPC)	4
Other, please specify: _____	5

2) Did you have access to internet services (including Facebook, Whatsapp, Twitter, etc.) in the beginning of 2016? And, if so, how did you usually access internet services?

a) I did not have access to the internet.
b) I had access through mobile data using my own smart phone.
b) I had access through mobile data using the smart phone of a family member/friends.
c) I had access through fixed line internet at home.
d) I had access through wifi or fixed line internet at public internet cafés.
e) I did not use internet services, including Facebook, WhatsApp, Twitter etc.

3) On the day of presidential elections in 2016, how did you intend to use internet services, in particular social media (e.g. Facebook, WhatsApp, Twitter) and mobile money?

a) I planned to use mobile money to pay for transport to get to my polling station
b) I planned to use mobile money to cover polling related expenses (e.g. pay staff at polling stations)
c) I planned to use social media to communicate to others that I participated in the elections
d) I planned to use social media to report about different incidences that I observed at polling stations (e.g. violence, ballot stuffing)
e) I did not intend to use internet services on polling day

Appendix B7. Reliability checks

To assess the reliability of information from the survey data, I use two indicators from the Afrobarometer round 6 from 2015 (Afrobarometer, 2016) and from World Bank survey data gathered in Uganda in 2015 (World Bank, 2020a).

Internet Access

In the Afrobarometer survey, one question assesses how often people use the internet to obtain news (q12d: "How often do you get news from the following sources? (Internet), range 0 to 4) and one question assesses how often people use the internet in general (q92b: "How often do you use: (the Internet)?", range from 0 to 4). While both questions do not directly assess whether an individual has internet access, they can be seen as an indirect indicator of people's access to the internet. I calculate the share of people with internet access for the survey data and the share of people who use the internet a few times a month or more at the district level. I find that both, general internet use ($r = .56$, $p < .001$) and internet use for news consumption ($r = .62$, $p < .001$) are significantly correlated with the share of people with internet access in the survey data.

Opposition Support

In the Afrobarometer survey, one question assesses whether people see the opposition as an alternative to the incumbent government (q64: "Please tell me whether you agree or disagree with the following statement: The political opposition in Uganda presents a viable alternative vision and plan for the country.", range 0 to 5). I calculate the share of people who strongly or moderately agree with the statement at the district level which is significantly correlated with the share of opposition supporters from the survey ($r = .42$, $p < .001$).

Education

I use panel data from the World Bank survey in Uganda 2015-2016 to assess the reliability of education levels. For both data sets, I correlate completed secondary education (= 1) with a respondent's sex (male = 1, female = 2). I then use Fisher's z to test the difference between the two correlation coefficients from both samples. The test statistic indicates that the coefficients do not significantly differ from each other ($z = 0.8814$, $p = .3781$).

Appendix B8. Likelihood of electoral violence

	M1: Violence (t1)	M2: Violence (t1)	M3: Violence (t2)	M4: Violence (t2)
internet*opposition		19.18 (7.84)*		15.26 (7.35)*
internet	-2.20 (1.21)·	-6.64 (2.27)**	-0.89 (1.10)	-4.09 (1.84)*
opposition	3.28 (1.43)*	-3.00 (2.85)	1.28 (1.38)	-3.90 (2.82)
education	0.20 (0.36)	0.22 (0.36)	-0.07 (0.35)	-0.10 (0.35)
economic status	-3.26 (1.40)*	-3.96 (1.40)**	-3.15 (1.48)*	-3.52 (1.44)*
opposition share 2011	0.30 (0.89)	0.36 (0.88)	0.92 (0.87)	1.01 (0.86)
urban	1.20 (0.48)*	1.19 (0.49)*	0.83 (0.46)·	0.76 (0.45)·
(Intercept)	-1.37 (0.84)	-0.01 (0.98)	-0.68 (0.82)	0.48 (0.98)
N	195	195	195	195
N group (county)	70	70	70	70

Note: $^{***}p < .001$, $^{**}p < .01$, $^{*}p < .05$, $^{+}p < .1$

Appendix B9. Likelihood of electoral violence (excluding Kampala)

	M1: Violence (t1)	M2: Violence (t1)	M3: Violence (t2)	M4: Violence (t2)
internet*opposition		19.53 (9.03)*		20.49 (9.01)*
internet	-2.65 (1.30)*	-6.51 (2.30)**	-0.99 (1.20)	-4.65 (1.96)*
opposition	2.73 (1.54)·	-3.11 (3.06)	1.52 (1.53)	-4.80 (3.13)
education	0.22 (0.39)	0.05 (0.41)	-0.16 (0.39)	-0.40 (0.41)
economic status	-3.40 (1.46)*	-4.02 (1.47)**	-3.42 (1.59)*	-3.88 (1.52)*
opposition share 2011	0.32 (0.96)	0.35 (0.98)	0.60 (0.95)	0.69 (0.96)
urban	0.83 (0.51)	0.89 (0.53)·	0.72 (0.51)	0.77 (0.52)
(Intercept)	-1.15 (0.85)	0.40 (1.11)	-0.35 (0.85)	1.35 (1.13)
N	165	165	165	165
N group (county)	62	62	62	62

Note: $^{***}p < .001$, $^{**}p < .01$, $^{*}p < .05$, $^{+}p < .1$

Appendix C

Appendix C1. Estimated effect of the share of SOE on democratisation (Geddes et al.)

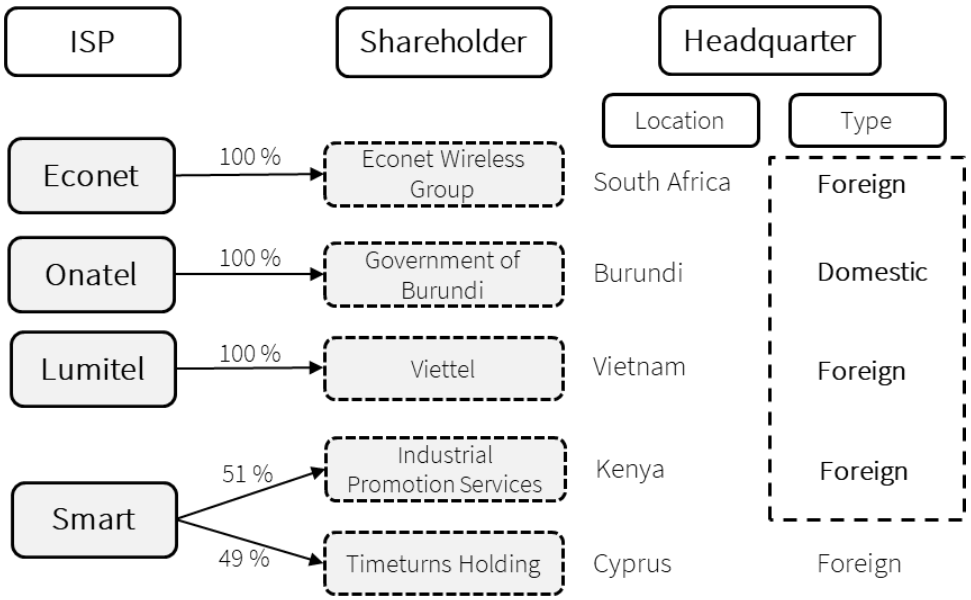
	Model 1	Model 2	Model 3	Model 4
% Internet penetration$_{t-1}$	-2.48 (2.24)			-2.80 (2.99)
Δ Internet penetration			-2.30 (3.75)	
share of SOE			-0.72 (3.21)	-3.18(3.35)
ln(GDP pc)$_{t-1}$	1.38 (1.71)	0.45 (1.28)	1.22 (1.80)	0.30 (1.42)
GDP pc growth$_{t-1}$	14.21 (16.87)	11.80 (14.12)	15.28 (16.95)	13.18 (14.81)
ln(Trade openness)$_{t-1}$	-0.42 (2.19)	-0.38 (1.68)	-0.32 (2.22)	-0.35 (1.78)
ln(Oil/gas income)$_{t-1}$	0.06 (0.09)	0.08 (0.08)	0.06 (0.09)	0.07 (0.09)
Ongoing civil war	-3.87 (3.07)	-1.87 (1.69)	-3.29 (2.81)	-1.92 (1.83)
Military regime	3.16 (2.88)	2.09 (2.02)	2.47 (3.23)	1.32 (2.20)
Personalist regime	1.38 (1.71)	-0.86 (1.53)	-1.34 (2.01)	-1.71 (1.73)
ln(Total population)$_{t-1}$	0.81 (1.14)	0.53 (0.91)	0.87 (1.17)	0.56 (0.99)
Rural population$_{t-1}$	5.24 (11.57)	4.18 (8.35)	4.45 (11.61)	4.05 (8.65)
(Intercept)	-25.74 (33.04)	-15.94 (23.51)	-24.69 (34.23)	-13.99 (24.90)
AIC	57.22	61.04	58.53	61.95
BIC	118.49	122.30	123.53	126.94
Log likelihood	-12.61	-14.52	-12.27	-13.98
No. of observations	340	340	338	338
No. of countries	37	37	37	37

Note: Standard errors in parentheses. Time since transition (as well as its squared and cubed transformation) not displayed. Monarchies are also not displayed due to their low occurrence (N = 2) and large standard errors. In the models including the *share of SOE* (i.e. state-owned ownership), two observations are excluded as there were no ISPs operating in Algeria in 2000 and 2001. *p < .05, **p < .01, ***p < .001.

Appendix D

Appendix D1. Aggregation rule for Burundi, 2019

In Burundi, four ISPs, namely Econet, Onatel, Lumitel, and Smart, provided internet services to individual customers in 2019. The first three are owned by a single shareholder, which is counted as majority-owner. Smart is owned by two shareholders, one of which holds the majority of shares, Industrial Promotion Services, and is hence counted as majority-owner. The information about the shareholders' headquarters reveals that three out of for majority-shareholders are based in foreign countries. Therefore, 75 percent of the telecom sector in Burundi are coded as foreign-owned (i.e., a proportion of 0.75). Vietnam and Kenya are counted as foreign-autocratic shareholders, resulting in 50 percent of the Burundian telecom sector coded as foreign-autocratic (i.e. a proportion of 0.5) and 25 percent coded as foreign-democratic (i.e. a proportion of 0.25).



Appendix D2. Headquarters of foreign shareholders and number of subsidiaries (2000-2019)

	Headquarter	*Number of subsidiaries*
Shareholders with HQ in Democracy	*South Africa*	21
	India	15
	France	16
	Netherlands	14
	France	14
	UK	13
	British Virgin Islands	8
	USA	7
	Luxembourg	5
	Cyprus	4
	Mauritius	4
	TOTAL	122
Shareholders with HQ in Autocracy	*Kuwait*	17
	Lebanon	10
	United Arab Emirates	13
	Morocco	9
	Egypt	9
	Kenya	6
	Libya	6
	Bahrain	5
	Ivory Coast	5
	Vietnam	4
	Congo Kinshasa	4
	TOTAL	88

Note: Table lists the number of subsidiaries in autocracies owned by foreign companies (with at least four subsidiaries) according to their headquarter. The table only provides information for first-level shareholders. For example, companies based in South Africa hold majority-shares in 21 subsidiaries in different authoritarian countries in Africa between 2000 and 2019. The regime type of the headquarter is coded using the Regimes in the World operationalisation by Lührmann et al. (2017).

Appendix D3. Results from linear mixed models (t-1)

	Share of foreign investors		… with headquarter in autocracies		… with headquarter in democracies	
	Model 1	Model 2	Model 3	Model 4	Model 5	Model 6
Repression	0.01 (0.01)	0.02 (0.01)*	0.02 (0.01)·	0.02 (0.01)	-0.00 (0.01)	0.01 (0.01)
Legislative chambers	0.03 (0.01)**	0.02 (0.01)*	0.01 (0.01)	0.01 (0.01)	0.02 (0.01)·	0.02 (0.01)·
Corruption		0.04 (0.02)*		0.03 (0.02)·		-0.02 (0.02)
Military control		-0.00 (0.01)		0.02 (0.01)*		-0.02 (0.01)·
Hereditary control		-0.15 (0.05)**		-0.04 (0.03)		-0.10 (0.04)*
Log GDP per capita		0.11 (0.02)***		0.04 (0.02)		0.06 (0.02)**
GDP per capita growth		-0.00 (0.00)·		-0.00 (0.00)		-0.00 (0.00)
Rents natural resources (% of GDP)		0.02 (0.02)		0.03 (0.02)*		-0.00 (0.02)
Total population		0.05 (0.04)		-0.04 (0.02)·		0.05 (0.03)·
Rural population (% of total)		0.01 (0.00)*		0.00 (0.00)		0.01 (0.00)***
Trade (% of GDP)		0.00 (0.00)***		-0.00 (0.00)		0.00 (0.00)***
Year	0.01 (0.00)***	0.00 (0.00)·	0.00 (0.00)**	0.00 (0.00)	0.01 (0.00)***	0.01 (0.00)***
(Intercept)	-20.51 (2.21)***	-9.76 (4.24)*	-7.10 (2.33)**	-1.58 (3.59)	-19.03 (2.12)***	-20.73 (3.89)***
R^2	0.80	0.86	0.54	0.55	0.77	0.82
No of obs.	639	576	639	576	639	576
No of obs. (country)	43	41	43	41	43	41

Note: ***p <.001; **p < .01; *p < .05; ·p < .1; all predictors are z-standardised.

Appendix D4. Means, standard deviations, and correlations

Variable	*M*	*SD*	1	2	3	4	5	6	7	8	9	10	11	12	13
1. Share (foreign)	0.49	0.34													
2. Share (foreign-autocratic)	0.20	0.23	.52**												
3. Share (foreign-democratic)	0.28	0.28	.74**	-.14**											
4. Share (public)	0.38	0.35	-.79**	-.44**	-.58**										
5. Repression	3.37	0.89	.09*	.07	.06	-.12**									
6. Legislatures	1.37	0.61	.11**	.18**	.01	-.14**	-.06								
7. Opposition parties	0.18	1.02	.31**	.15**	.24**	-.42**	-.05	.05							
8. Military control	0.28	0.16	.27**	.24**	.12**	-.16**	.05	-.12**	.01						
9. Hereditary control	0.05	0.17	-.28**	-.16**	-.19**	.16**	-.21**	.26**	-.23**	-.31**					
10. GDP growth (in %)	1.71	8.20	-.13**	-.14**	-.02	.12**	-.00	.03	-.02	-.07	.02				
11. (log) GDP	6.92	1.08	-.18**	.01	-.19**	.13**	-.24**	.19**	-.22**	.04	.26**	.06			
12. (log) population	16.18	1.34	.16**	-.08*	.27**	-.28**	.40**	.14**	.23**	-.03	-.17**	.06	-.21**		
13. rural population	58.41	19.23	.18**	-.04	.24**	-.14**	.27**	-.02	.03	-.18**	.03	.03	-.72**	.32**	
14. (log) natural resources	2.36	1.04	.27**	.32**	.07	-.18**	.20**	.08*	.02	.35**	-.38**	.02	.12**	.11**	-.07

Note: M = mean; *SD* = standard deviation; * $p < .05$. ;** $p < .01$.

Appendix D5. Linear mixed models including the share of public-domestic ISPs

	Share of ISPs (foreign)		Share of ISPs (foreign-autocratic)		Share of ISPs (foreign-democratic)	
	Model 1	Model 2	Model 3	Model 4	Model 5	Model 6
Repression	0.01 (0.01)	0.01 (0.01)$^{\cdot}$	0.02 (0.01)*	0.02 (0.01)*	-0.00 (0.01)	0.00 (0.01)
Legislative chambers	0.02 (0.01)**	0.02 (0.01)$^{\cdot}$	0.01 (0.01)	0.01 (0.01)	0.01 (0.01)	0.01 (0.01)
Share public-domestic ISPs	-0.62 (0.03)***	-0.62 (0.03)***	-0.28 (0.03)***	-0.27 (0.04)***	-0.31 (0.03)***	-0.30 (0.03)***
Corruption		0.03 (0.01)**		0.03 (0.01)*		-0.02 (0.01)
Military control		0.03 (0.01)**		0.03 (0.01)*		-0.02 (0.01)
Hereditary control		-0.01 (0.01)		0.01 (0.01)		-0.01 (0.01)
Log GDP per capita		-0.10 (0.03)***		-0.03 (0.03)		-0.08 (0.03)*
GDP per capita growth		0.06 (0.02)***		0.03 (0.02)		0.04 (0.02)$^{\cdot}$
Rents natural resources (% of GDP)		-0.01 (0.01)$^{\cdot}$		-0.01 (0.01)		-0.00 (0.01)
Total population		0.01 (0.01)		0.02 (0.02)		0.00 (0.01)
Rural population (% of total)		-0.05 (0.03)		-0.08 (0.03)**		0.03 (0.03)
Trade (% of GDP)		0.11 (0.03)***		0.02 (0.03)		0.12 (0.03)***
Year	0.00 (0.00)***	0.00 (0.00)*	0.00 (0.00)	-0.00 (0.00)	0.01 (0.00)***	0.01 (0.00)***
(Intercept)	-7.37 (1.71)***	-5.61 (3.02)$^{\cdot}$	-2.45 (2.20)	0.46 (3.61)	-12.78 (1.94)***	-17.06 (3.68)***
R^2	0.86	0.87	0.58	0.57	0.76	0.80
No of obs.	683	582	683	582	683	582
No of obs. (country)	44	41	44	41	44	41

Note: $^{***}p$ <.001; $^{**}p$ < .01; $^{*}p$ < .05; $^{\cdot}p$ < .1; all predictors are z-standardised.

Appendix E

Appendix E1. Raw data

case: country-election year	ISP state ownership (≥ 51 percent)	autocracy (parcomp < 2 | ≠ 0; exrec < 5)	electoral violence (v2elpeace_ord ≤ 2)	shutdown
Benin 2015	Libercom (100); be.telecoms (100)	no (4; 8)	no (4)	no
Benin 2016	Libercom (100); be.telecoms (100)	no (4; 8)	no (4)	no
Botswana 2014	BTCL (100)	no (4; 7)	no (4)	no
Burkina Faso 2015	Onatel (20)	no (4; 7)	no (4)	no
Burundi 2015	Onatel (100)	yes (3; 3)	yes (0)	yes
CAR 2015	--	yes (-77)	no (3)	no
CAR 2016	--	no (3; 7)	no (3)	no
Chad 2016	Groupe Sotel (100)	yes (3; 5)	yes (1)	yes
Djibouti 2016	Djibouti Telecom (100)	no (0; 7)	no (4)	no
Equatorial Guinea 2016	Gecom (51); Getesa-Orange (60)	yes (2; 4)	no (3)	yes
Ethiopia 2015	Ethio Telecom (100)	yes (3; 3)	no (3)	yes
Gabon 2016	Gabon Telecom (49)	no (3; 7)	yes (0)	yes
Gambia 2016	Gambia Telecom (100)	yes (2; 5)	no (4)	yes
Ghana 2016	Vodafone Ghana (30)	no (4; 8)	no (3)	no
Guinea 2015	--	no (3; 7)	no (3)	no
Guinea-Bissau 2014	Guinetel (100)	no (4; 7)	no (3)	no
Ivory Coast 2015	--	no (3; 7)	no (3)	no
Ivory Coast 2016	Comium (100)	no (3; 7)	no (3)	no
Lesotho 2015	Econet Lesotho (30)	no (4; 8)	no (3)	no
Malawi 2014	--	no (3; 7)	no (3)	no
Mauritania 2014	Mauritel (45.5)	yes (0; 5)	no (4)	no
Mozambique 2014	Mcel (26); TDM (90)	no (4; 7)	yes (2)	no
Namibia 2014	MTC (66); Telecom Namibia (100)	no (4; 7)	no (4)	no
Niger 2016	Sonitel (100); Sahelcom (100)	no (4; 7)	no (3)	no
Nigeria 2015	ntel (100)	no (4; 8)	no (3)	no
Republic of Congo 2016	--	yes (2; 4)	yes (2)	yes
South Africa 2014	Telkom (51); MTN (17)	no (4; 8)	no (3)	no
Sudan-North 2015	Sudatel (30)	yes (2; 4)	yes (2)	yes
Tanzania 2015	Airtel (40); Tanzania Telecom (65)	no (3; 7)	yes (2)	no
Togo 2015	Togo Telecom (100)	yes (3; 3)	no (3)	yes
Uganda 2016	Uganda Telecom (31)	yes (3; 5)	yes (2)	yes
Zambia 2015	Zamtel (100)	no (4; 8)	no (3)	no
Zambia 2016	Zamtel (100)	no (3; 8)	yes (1)	no

Note: The Polity IV project codes cases that experience "complete collapse of central authority or a revolutionary transformation in the mode of governance" (Marshall et al. 2017: 35) with '-77'; the combined polity2 score converts this 'standardized authority score' to a score of '0', which falls within the category of autocracies.

Appendix E2. Truth table

ISP	*violence*	*autocracy*	*OUT*	*N*	*incl*	*PRI*	*Cases*
0	1	0	1	1	1	1	Gabon_2016
0	1	1	1	3	1	1	Republic of Congo_2016, Sudan-North_2015, Uganda_2016
1	0	1	1	4	1	1	Equatorial Guinea_2016, Ethiopia_2015, Gambia_2016, Togo_2015
1	1	1	1	2	1	1	Burundi_2015, Chad_2016
0	0	0	0	7	0	0	Burkina Faso_2015, CAR_2015, Ghana_2016, Guinea_2015, Ivory Coast_2016, Lesotho_2015, Malawi_2014
0	0	1	0	2	0	0	CAR_2015, Mauritania_2014
1	0	0	0	11	0	0	Benin_2015, Benin_2016, Botswana_2014, Djibouti_2016, Guinea_Bissau_2016, Ivory Coast_2016, Namibia_2014, Niger_2016, Nigeria_2015, Zambia_2015, South Africa_2014
1	1	0	0	3	0	0	Mozambique_2014, Tanzania_2015, Zambia_2016

Note: OUT = outcome value (here: internet shutdowns); *N* = number of cases; incl = sufficiency inclusion score (i.e. consistency measure); PRI = proportional reduction in inconsistency; incl and PRI are always equal for crisp sets.

Appendix E3. csQCA output with Gabon recoded as autocracy

	cases	conditions: *ISP state ownership*	conditions: *autocracy*	conditions: *electoral violence*	coverage: *raw*	coverage: *unique*	consistency
positive outcome	Equatorial Guinea_2016, Ethiopia_2015, Gambia_2016, Togo_2015; Burundi_2015, Chad_2016	●	●		0.60	0.40	1.0
	Gabon_2016; Republic of Congo_2016, Sudan-North_2015, Uganda_2016	○		●	0.40	0.00	1.0
	Gabon_2016; Republic of Congo_2016, Sudan-North_2015, Uganda_2016; Burundi_2015, Chad_2016		●	●	0.60	0.00	1.0
	Solution 1	ISP*AUTOCRACY + (isp*VIOLENCE) <=> SHUTDOWN			1.0	1.0	1.0
	Solution 2	ISP*AUTOCRACY + (VIOLENCE*AUTOCRACY) <=> SHUTDOWN			1.0	1.0	1.0
negative outcome	**Burkina Faso_2015, CAR_2016, Ghana_2016, Guinea_2015, Ivory Coast_2015, Lesotho_2015, Malawi_2014;** CAR_2015, Mauritania_2014	○		○	0.391	0.087	1.0
	Burkina Faso_2015, CAR_2016, Ghana_2016, Guinea_2015, Ivory Coast_2015, Lesotho_2015, Malawi_2014; Benin_2015, Benin_2016, Botswana_2014, Djibouti_2016, Guinea-Bissau_2014, Ivory Coast_2016, Mozambique_2014, Namibia_2014, Niger_2016, Nigeria_2015, South Africa_2014, Tanzania_2015, Zambia_2015, Zambia_2016		○		0.913	0.609	1.0
	Solution	autocracy + isp*violence <=> shutdown			1.0	1.0	1.0

Note: Empty circles depict the absence of the condition, shaded circles its presence. In line with Boolean operators, upper-case letters indicate the presence of an outcome or a condition, and lower-case letters indicate their absence; * designates logical AND, while + designates logical OR, and the logical (set-theoretical) relation <=> signals both necessity and sufficiency.

CV Lisa-Marie GARBE

Office address
Müller-Friedberg-Str. 8
Institute for Political Science
CH - 9000 St.Gallen
lisa.garbe@unisg.ch | +49 17666625406 | https://ipw.unisg.ch/

Private (correspondence) address
Sigmaringer Str. 10
DE - 10713 Berlin

RESEARCH INTERESTS Comparative Politics, Internet Governance, Information Controls, Political Economy, African Politics

EDUCATION

2021 **Ph.D. in International Affairs & Political Economy,** University of St.Gallen, Switzerland
Title: Authoritarian Survival in the Digital Age. Internet Access and Control in African Autocracies
Committee: Tina Freyburg (supervisor), Carl Henrik Knutsen (University of Oslo/Peace Research Institute Oslo), Joss Wright (Oxford Internet Institute)

2013 – 2016 **M.A. in European Studies,** University of Leipzig, Germany
Grade: 1.2 (GPA = 3.9)

2014 – 2015 **Exchange semestre** at École Normale Supérieure Paris, France
Focus: Geopolitics

2010 – 2013 **B.A. in Political Science** | Minor in Economics**,** University of Freiburg, Germany & University of Innsbruck, Austria

ACADEMIC EMPLOYMENT

Since 2017 **University of St.Gallen, Comparative Politics Research Group, Switzerland**
Research Associate. Project "Ownership of telecommunication companies and state control of the internet in authoritarian contexts" (PI: Tina Freyburg), funded by the Swiss Network for International Studies SNIS (2017/2018) and the University of St.Gallen (2019)

Key tasks: Conducting research on ownership of telecommunications infrastructure and internet disruptions; supervision of research assistants; field research in Uganda (Jul-Sep 2018)

2016 **German Centre for Integrative Biodiversity Research (iDiv), Leipzig, Germany**
Research Assistant. Project "Citizen Science" (PI: Aletta Bonn)
Key tasks: Designing, implementing and evaluating an online survey with citizen science researchers across Europe

Visiting Positions

2020 – 2021 **Visiting PhD researcher,** Centre for Digital Governance, Hertie School of Governance, Berlin, Germany
Mentors: Daniela Stockmann, Anita Gohdes

2019 – 2020 **Visiting PhD researcher,** Oxford Internet Institute, University of Oxford, UK
Mentor: Joss Wright

PUBLICATIONS

Articles in Refereed Journals

2020 'Influence of perceived threat of Covid-19 and HEXACO personality traits on toilet paper stockpiling', *PLOS ONE* 15(6), with R. Rau and T. Toppe [5-year-impact factor: 3.792, Citations: 10, Web of Science; 36, Google Scholar]

2019 'Droughts, vulnerability and human migration in Northern Ethiopia', *Regional Environmental Change, 19*(4): 1101-1111, with K. Hermans [5-year-impact factor: 3.792, Citations: 3, Web of Science; 6, Google Scholar]

2018 'Blocking the Bottleneck: Internet Shutdowns and Ownership at Election Times in Africa', *International Journal of Communication, 12*: 3896–3916, with T. Freyburg [5-year-impact factor: 1.641; citations: 7, Web of Science; 29, Google Scholar]

Book Chapters

2018 'European Citizen Science Landscape: A Snapshot', in: S. Hecker, M. Haklay, A. Bowser, Z. Makuch, J. Vogel, A. Bonn (eds.) Citizen Science: Innovation in Open Science, Society and Policy, *UCL Press,* with S. Hecker and A. Bonn [citations: 9, Google Scholar]

Online Publications

2020 'Digital democracy is still a long way off in Africa: it takes more than technology', *The Conversation*, with N. Cheeseman, 1 Oct 2020, https://theconversation.com/

2020 'What we do (not) know about internet shutdowns in Africa', *Democracy in Africa,* 29 Sep 2020, http://democracyinafrica.org/

2018 'Blocking the Bottleneck. Internet shutdowns at election times in Sub-Saharan Africa', *The Open Technology Fund*, with T. Freyburg, 30 Nov 2018, https://www.opentech.fund/

2018 'Exporting Repression? China's AI push into Africa', *Council on Foreign Relations*, with A. Gwagwa, 17 Dec 2018, https://www.cfr.org/

Manuscripts under review

1 'Telecommunications Ownership and Control (TOSCO). A new dataset to explore the political power of internet business in Africa, 2000-2019', with T. Freyburg and V. Wavre, under review with *Review of International Organizations* (Review & Resubmit)

2 'How African countries respond to hate speech and fake news', with LM Selvik & P. Lemaire, under review with *Information, Communication & Society* (Review & Resubmit)

Manuscripts to be submitted soon

1 'Authoritarian Elections 2.0: Internet Use & Electoral Violence in Uganda's 2016 Elections, Presented at the *AAG* Annual Meeting (2019), *GPSA* Congress (2020), targeted journals: Journal of Peace Research, Comparative Political Studies

2 'Political Determinants of Foreign Investment in Internet Service Provision in African Autocracies', Presented at the SPSA conference (2021), targeted journals: International Studies Quarterly, International Interactions

FIELD RESEARCH EXPERIENCE

2018 **Uganda** (~60 interviews, 3 months)
Social media use and shutdown in three Ugandan districts

2015/2016 **Ethiopia** (survey with 340 participants, 4 months)
Climate change, subsistence farming, adaptation strategies and migration

TEACHING

Autumn 2020 **'Strategies of Social Science Inquiry'**
St.Gallen, M.A. in International Affairs (60 students), tutorial in English, 24h.

Spring 2019 **'Introduction to Quantitative Methods'**
St.Gallen, B.A. in International Affairs (60 students), tutorial in English, 12h.

Autumn 2017 + 2018 **'Introduction to Comparative Politics'**
St.Gallen, B.A. in International Affairs (120 students), tutorial in English, 48h.

ADDITIONAL TRAINING (selection)

2019 **Technology and Regulation,** MSc and DPhil course, Oxford Internet Institute, Joss Wright

2019 **Regression Analysis for Spatial Data,** Global School in Empirical Research Methods, University of St.Gallen, Roland Füss/Zeno Adams

2018 **The Geopolitics of Cyberspace,** DPhil course, University of St.Gallen, Ron Deibert

2018	**Regression Analysis I&II,** Global School in Empirical Research Methods, University of St.Gallen, Timothy McDaniels
2017	**Time Series Analysis,** Global School in Empirical Research Methods, University of St.Gallen, Sara McLaughlin Mitchell

GRANTS & FELLOWSHIPS

2019/2020	**Swiss National Science Foundation (SNSF),** *Doc.Mobility grant,* Research stay at the Oxford Internet Institute as visiting PhD researcher for 12 months (CHF 80.000)
2018	**Swiss Academy of Humanities and Social Sciences (SGAW),** *Conference grant,* Participation in the annual meeting of the Midwest Political Science Association, Chicago (CHF 1.000)
2017	**German Zeit Foundation**, *Bucerius fellowship***,** Field research in Uganda October/November 2018 (€ 3.000)
2016	**German Academic Exchange Service (DAAD),** *Promos scholarship*, Field research in Ethiopia February-April 2016 (€ 1.500)

ORGANIZATION OF PANELS & WORKSHOPS

2019	'Identifying internet shutdowns at company-level', session at the **Summer Institute 'Monitoring Internet Openness and Rights',** CitizenLab at University of Toronto, with T. Freyburg and V. Wavre, Toronto
2019	'Business and Human Rights in Africa and South-Asia: Network shutdowns and data disclosure requests under conflicting legal frameworks', panel at **RightsCon**, with I. Ebert, Tunis
2018	'Ownership matters! The political effects of ownership patterns across key infrastructures', panel at **German Political Science Association** (DVPW) with T. Freyburg, Frankfurt
2018	'Internet Diffusion and its Political Effects in Authoritarian Contexts', panel at **Midwest Political Science Association** (MPSA) with T. Freyburg, Chicago
2017	'Telecommunication Politics in Authoritarian Contexts', St.Gallen, **Swiss Network of International Studies (SNIS) Workshop** with (associated) project members plus international academic experts and practitioners, St.Gallen

INVITED TALKS

2020	**Internews**, Network Measurement Training for human rights defenders from sub-Saharan Africa, 22 Oct 2020, online
2020	**Competence Center for African Research**, Launch Symposium, 14-15 Jan, St.Gallen
2020	**Oxford Internet Institute**, Brownbag Lunch Series, 5 Feb, Oxford
2019	**International Studies Association**, Research Workshop 'The Internet as a Research Tool: Bridging Politics and Technology in the Study of Internet Shutdowns', 26 Mar, Toronto

PRESENTATIONS (selection)

Conferences

2019	*American Association of Geographers Annual Meeting*
2018, 2020	*German Political Science Association Congress*
2018	*Gig-Arts Conference*
2019	*GIGANET Conference*
2019, 2021	*International Studies Association Annual Convention*
2019	Joint Austrian, German & *Swiss Political Science Association Conference*
2018	*Midwest Political Science Association Annual Conference*
2018, 2021	*Swiss Political Science Association Conference*

Workshops

2017	'Global Governance in the Internet Era', *Hertie School of Governance*
2017	'Empirical Study of Autocracy', *University of Konstanz*
2017	'Media and Democratization: Chances and Risks', *University of Zurich*

KNOWLEDGE TRANSFER

Animated Short Stories

2021	#KEEPITON — A GRAPHIC JOURNEY FROM INTERNET ARCHITECTURE TO SHUTDOWNS, project funded by SNF Agora, with T. Freyburg, V. Wavre, and P. Valär, https://ipw.unisg.ch/de/comparative-politics/knowledge-transfer

Video Documentary

2018	'Citizens offline: The state, telecom companies & internet shutdowns' [8 min.], with T. Freyburg, V. Wavre and N. Guignard, shortlisted for Best Documentary Film, Amakula International Film Festival, Kampala, Uganda & Fast Forward Science Award, Germany, https://www.youtube.com/watch?v=ccKLk-UKqhE&t=9s

Media Coverage (selection)

2020	*CNN*, 'Why are we hoarding toilet paper? It may be your personality type'
2020	*One Zero*, 'The Great Indian Internet Shutdown Is the Troubling Future of Protest Control'
2020	*AlgoRythms*, Weekly radio show on Oxide Radio featuring tech, tunes and research
2018	*Deutsche Welle*, 'Internet censorship in Africa threatens democracy, economy'

PROFESSIONAL ACTIVITIES

Referee Services	*International Journal of Communication*
Peer Mentoring	HSG student team QWERTY, annual Cyber Challenge in Geneva (April 2019)
Consulting	SCION-based networking software provider Anapaya. Main task: writing blog posts, e.g. about internet hijacking or public networks in B2B (since 09/2019)

LANGUAGES

German (native), English (fluent), French (intermediate), Spanish (intermediate)

REFERENCES

Tina Freyburg
Professor of Comparative Politics
University of St.Gallen
mail: tina.freyburg@unisg.ch

Carl Henrik Knutsen
Professor of Political Science
University of Oslo/Peace Research Institute
mail: c.h.knutsen@stv.uio.no

Joss Wright
Senior Research Fellow
University of Oxford
mail: joss.wright@oii.ox.ac.uk