COMPUTER WORLD: HOW DIGITAL TECHONOLOGIES INFLUENCE HUMAN RIGHTS

by
MERIDITH LAVELLE

(Under the Direction of K. Chad Clay)

ABSTRACT

How has the innovation, diffusion, and adoption of technology impacted human rights? Previous literature has extensively explored the mechanisms through which state leaders and their agents decide to engage in human rights abuses but more need to be understood when considering technology's role. This project addresses these topics along three dimensions. Chapter 2 assesses the relationship between digital repression, particularly digital disruptions, and transnational advocacy shaming efforts that target violating states' human rights practices. The third chapter explores how state leaders and their agents select from seemingly competing strategies of digital repressions repression tactics. Finally, the fourth chapter evaluates how legitimation strategies of leaders impact digital rights violations. The primary goal of this project is to develop a deeper understanding of mechanisms that lead to governments using repertoires of digital repression to dampen the effects of transnational advocacy as well as domestic advocacy, how governments can use digital repression to violate civil rights in less overtly violent ways, and how legitimacy factors into state policies of using digital repression.

Index words: Digital repression, Human Rights, Political Violence, Technology and Politics

COMPUTER WORLD: HOW DIGITAL TECHONOLOGIES INFLUENCE HUMAN RIGHTS

by

MERIDITH LAVELLE

A.B., University of Georgia, 2015
B.A., University of Georgia, 2016
M.A., University of Georgia, 2020

A Dissertation Submitted to the Graduate Faculty of the University of Georgia in Partial Fulfilment of the Requirements for the Degree.

DOCTOR OF PHILOSOPHY

ATHENS, GEORGIA

2025

COMPUTER WORLD: HOW DIGITAL TECHONOLOGIES INFLUENCE HUMAN RIGHTS

by

MERIDITH LAVELLE

Major Professor: K. Chad Clay

Committee: Daniel Hill Jr.
Amanda Murdie
Jeffrey Berejikian

Electronic Version Approved:

Ron Walcott
Vice Provost for Graduate Education and Dean of the Graduate School
The University of Georgia
August 2025

Dedication

This project is dedicated to my parents, Scot LaVelle and Christine LaVelle. Thank you for never giving up on me and always believing in me.

Acknowledgements

Without the unconditional support from my family, friends, partner, colleagues, and my two wonderful cats, it would not have been possible to complete this dissertation project or my Ph.D. program. My family and partner have shown nothing but love and support throughout this process. To my mother, Christine LaVelle, I can't thank you enough for wanting to read my papers throughout graduate school mostly for your own interest and desire to continue learning, for wanting to talk about these political topics and figure out ways to incorporate meaningful solutions to ongoing human rights challenges within our own communities, and for consistently encouraging me not to give up despite how tough life had gotten over the past few years. I'm so grateful that she and my dad raised me to value education, embrace critical thinking, and to stand up for what is right. She is the strongest person I know, and her unwavering support and encouragement to continue this journey will undoubtedly take me places that I never thought were possible, especially around the time I started graduate school almost seven years ago. My siblings, Alex, William, and Evelyn have, too, been crucial sources of support. They have all been interested in learning more about human rights, digital threats to our communities, and listening to each other to learn how we can lean into our own strengths to continue working towards a more equitable and loving world. They have also taught me so much throughout life and have also shared their knowledge and experiences of human rights issues. To my father, Scot LaVelle, whose passion for humanitarian work and giving back to his communities, led me to this specific path today. I write this in memory, as he passed during the week of Christmas of second year of my Ph.D. program. His unconditional love and support lives on through his family, friends, community, and all those who were lucky enough to ever know him. I know he would be so proud of me. He and the rest of our family have been my biggest supporters

in all I do in life. Finally, to my partner, Bradley Luhn, thank you for coming into my life when you did. On our first phone call, you were so genuinely interested in what I do and learning about this project. I remember explaining some of the chapters to you and being so shocked that you wanted me to keep talking more about it. That curiosity hasn't gone away, and I know it never will. I've never had a partner who has taken such an interest in the human rights research I do. You have been allied with the work that I've done alongside so many other people who work tirelessly to research, measure, and improve human rights for all. I've never had a partner so supportive, so encouraging of the work that I do. You have let me bounce ideas off you, listened to me ramble on about this project and others, read drafts of this project, taken my phone away so I can focus, asked to read anything I've published, and shared all of this with your family and friends. Having a partner who shows he's proud is one of the many things that sets you apart. And you keep me accountable and make sure I've taken care of myself throughout this process when I could have easily just forgotten to eat, get fresh air and exercise, and to make sure I just enjoy the things we love in life. Thank you.

To my friends who have been my support system throughout my seven years of graduate school and before – I couldn't have done it without you all. All of the laughs, concerts, travel, meals, getting together for tea, uplifting me when I wanted to quit, while I continue to grieve the loss of my dad, for celebrating milestones with me, and for knowing just how to motivate me and cheer me on, I can never thank you all enough. Thank you, Danny Pally, Nicole Smith, Sophie Hall, Riley Holmes, Carleen Mullins, Erika Aspenson, Sarah Douglass, Jon Hurst, Emma Reigel, Meg Scalise, Lizz Cambron, Jinny Jagoditsch, Devin Roth, Jenny VanHoy, and so many others.

I want to extend my deepest gratitude to the faculty and staff School of Public and International Affairs at the University of Georgia for the collaborative and supportive environment – among both faculty and my graduate school peers. Thank you for taking a chance on me. Being

trained by the some of the most brilliant and kindest people and instilling in me the values of intellectual curiosity, academic collaboration, humility, and choosing humanity and compassion over cutthroat competition allows me to impart these values to my next position and beyond. For faculty members, I especially want to thank my committee members, Chad Clay, Daniel Hill, Amanda Murdie, Jeff Berejikian, as well as Jerry Legge, Leah Carmichael, Maryann Gallagher, Orsolya Farkas, Audrey Haynes, Megan Turnbull, and Katey Stauffer. As for my peers, there many colleagues at the University of Georgia or who graduate and moved on that I truly could not have done this program and completed this dissertation without their guidance, patience, mentorship, and friendship: Matthew Rains, Hyunjoo (Jay) Lee, Eduardo Burkle, Jason Lian, Shanshan Lian, Annie Watson, Morgan Barney, and Asia Parker. Another special thank you to Jessica Dick at GLOBIS, who has been more of a source of support than she probably knows. Along with Jessica, there are several other colleagues at GLOBIS who have offered support and camaraderie along the way: Kianna Bussa, Hannah Kesner, Abby Crowe, and Alex Audrain. Finally, I would like to thank Stephen Bagwell, Skip Mark, and my colleagues at the Human Rights Measurement Initiative, and particularly Thalia Kehoe-Rowden. Stephen, Skip, and Thalia have been instrumental in helping me carve out my academic and practitioner paths through their mentorship. There truly is not enough gratitude in the world to express how fortunate I am to know each of these people. Even just smallest gestures – showing me the space where I would give my first presentation in grad school at GAHRNET Jr., to sitting in a diner in St. Louis meeting for the first time and hashing through future research projects, to preparing me for my first practitioner conference in a sports bar in Taipei – have never left me. These three people have worked with me, answered random text messages, met over dozens of zoom calls, and been there for me time and time again. Their support, patience, tolerance, mentorship, encouragement, and friendship have, too, propelled me professionally in ways I never thought imaginable. And to Stephen, thank you for everything over the past 10 years. Going from

being one of your undergraduate students, to being in graduate school together, to co-authoring, to connecting me with Skip and so many others, to answering all my thousands of questions about the things they don't necessarily teach you in grad school and sharing your confidence – you've been an awesome mentor. So awesome, that I want you to know that you're doing a great job.

I have also been fortunate to join a wonderful collective of other human rights measurement academics and friends through the Consortium of Rights Analysis and Measurement. Through their initiatives to foster mentorship for graduate students and junior faculty, CRAM has provided a constructive space share projects related to the measurement of human rights, including portions of this dissertation. Several of y'all of offered me wildly helpful feedback at our workshops, and I can't thank you enough. Through this network, I have also been fortunate to have friends who have helped me throughout the process. There's a lot of you to thank but just know that I value and appreciate each and every one of you for all that you do. Thank you for welcoming me.

One final shoutout to all the amazing students I've been honored to teach over the years at the University of Georgia – from teaching in Athens, to Verona, Italy, and Stellenbosch, South Africa. I want to also extend my gratitude for all the students who have come through the GLOBIS Human Rights Research Lab. With each opportunity to teach in the classroom, working with excellent students over the years has only solidified my commitments to academia, research, mentorship, and collaboration in the classroom.

Even with all of these incredible people, there is one person who I can confidently say has been so influential and pivotal in my academic career that I know without meeting him almost 10 years ago in his Human Rights course, I would not have come back to the University of Georgia to earn my master's degree and to write this dissertation for my Ph.D. – Chad Clay. Taking his class in Fall of 2015 allowed me to analyze the world through an entirely different lens that I had come across throughout my education, the lens of human rights. When I came back to UGA in 2018, I

was bound and determined to get to work with him, and fortunately I have since 2019. Chad has been the most wonderful mentor, believing in what I'm capable of – during both the ups and downs – and offering both constructive criticism when needed and validation during my worst periods of doubt. By offering my kindness, understanding, and flexibility when I lost my dad during Christmas of 2021. Through his mentorship, I have gained more confidence, been challenged, witnessed what meaningful and thoughtful collaboration looks like, learned accountability, and developed a stronger sense of community – academically and personally. By allowing me opportunities to co-author, work on data projects with him and our colleagues at the Human Rights Measurement Initiative, work and teach at GLOBIS, instruct alongside him in the GLOBIS Human Rights Research Lab, teach on study abroad, and ultimately provide a judgement free space where myself and others could thrive, he has time and time again demonstrated the that I do add value to this field and that I do belong. His unwavering commitments to empathy and inclusivity, dedication to all that is human rights, and emphasis on education, data, and research as being key forms of protest against challengers of human rights – these are qualities that I will never take for granted and will continue to share. Being his mentee, student, and friend is such a privilege, and even though I will be gone from the University of Georgia and GLOBIS after all these years, I'm eternally grateful for everything he has done for me and countless other students, friends, and colleagues. I'm looking forward to many more years of phriendship and collaborating with Chad on all the projects we're both terrible at saying no to. Enjoy your research leave and time off, Chad. You've more than earned it. Thank you for everything!

Table of Contents

List of Tables

List of Figures

Introduction

During the post-WWII era, Bell Nokia Laboratories in Murray Hill, New Jersey, carried out a secret project with the aim of pushing new, innovative technology. Seeing the opportunities ahead the physicists pioneering this project, John Bardeen and Walter Brittain, presented their fateful invention to executives at Bell Labs on December 16, 1947 -- the transistor. The significance tied to this invention is what we can now attribute to personal computing as we know today (Agar, 2000; Dye, 1997). This invention propelled the US and the rest of the world into what is now termed the information age – the current era where people across the globe have access to information at the tip of their fingers.

The iterations of personal computing have evolved exponentially since the advent of the first personal computer, which was adopted incrementally starting in the 1980s for at home usage. Since then, the innovations in computing have exploded, seeing the expansion of the internet worldwide, car phones morphing into cell phones morphing into smart phones, instant messaging being replaced by SMS and social media, and radio shifting from analogue all the way to satellite streaming and online music streaming. As artificial intelligence entered digital spaces, MapQuest shifted to Google and Apple Maps, translation services being more widespread than ever, and algorithms took over to curate our lives all the way from what we listen to and what we buy. E-commerce has transformed the ways in which economies conduct business domestically and locally, with social media, streaming services, and other paid apps forcing generating more revenue than ever with an oversaturated market of social media influencers and ads shilling products and services as cyclically as Apple releases new iterations of iPhones.

Yet, while our personal views of the world, what we buy, who we listen to, are inevitably tweaked by the social media companies who own these algorithms and information, how has the information era impacted more political spaces? It is common knowledge that platforms such as TikTok, Instagram, Facebook, and others often work to boost messaging of certain political leanings and information over other perspectives. These social media platforms have become the core spaces that people of all ages utilize for short reels and stitches to get quick, digestible information on news across the globe. Being able to feel more connected with others across the world, share information about events happening outside our own bubbles, and connect with others who we may otherwise have never met has been part of the camp of liberation technology theorists. These groups hold that social media and technology more broadly has the potential for a liberating power for politics, both domestically and internationally.

But have the liberation technology camp's theories come to fruition? The other side of the coin here is how governments themselves have adopted this technology. In the days of the Arab Spring starting in December of 2010, there was a shared sense of optimism that social media – specially Twitter and Facebook – could be mediums through which protesters and dissidents within the MENA region could mobilize and coordinate protests to demand reforms seeking to overthrow current rule in favor of a democratically elected government and addressing cost of living issues. Starting in Tunisia, Muhammad Bouazizi's attempt at self-immolation in protest of police harassment has been linked to the onset of political activism that rapidly swept the region (Al Jazeera, 2020; Angrist 2013; Robinson & Merrow, 2020). In Tunisia, as well as other surrounding states, social media was a primary tool critical to the mobilization efforts of the protesters, and which at that time had outpaced the abilities of local governments respond (Angrist, 2013). Protest continued to sweep the region: citizens demanding the resignation of Egyptian President Honsi Mubarak; protests took to Pearl Square in Manama where Bahrainis with more political demands of

government overhaul; and on the same day as Bahrain's demonstrations were those in Libya, where protests erupted demanding an end to Muammar Gaddafi's brutal regime ultimately result in a civil war and Gaddafi's death. Syria was the next domino to fall, where protesters demanded President Bashar al-Assad's ousting and eventually resulting in a decades long civil war. Yemen's former dictator, Ali Abdullah Saleh was also targeted by protests, resulting in his resignation in 2012 and yet another civil war in the region starting in 2014 (Al Jazeera 2020).

Since the Arab Spring, it has become increasingly evident that social media can be an effective tool to organise movements demanding political, social, and economic reform. However, as the international community watched the spread of protest and demands that equate to improved human rights outcomes across the MENA region, governments learned quickly from the shortcomings in some of the state responses to dissent. This period of optimism of the benefits of technology, social media, and the internet were swiftly tempered as the Egyptian government decided to shut off the internet – the key spaced used for orchestrating the movement that sought to stifle authoritarianism in the region. Although the movement didn't stop, Egypt was digitally cut off from the outside world (Al Jazeera, 2016).

Following the Arab Spring in 2012, internet shutdowns have increasingly spread. According to Access Now's Annual Report on Internet Shutdowns in 2024, more internet shutdowns have been ordered by governments than ever before. Moreover, these tactics continue to expand across new borders each year, with seven new offenders of state-ordered internet shutdowns (Access Now, 2025). The report details that 296 shutdowns in 54 countries in the year 2024, indicating "a 35% increase in the number of countries where shutdowns occurred compared with a previous high in 2022 (40)" (Access Now, 2025). These numbers do not include other types of shutdown events, ranging from blocking social media services and other apps digital curfews, shutting down the internet during national school exams, internet and SMS throttling, and more. These dynamics are

especially heightened in conflict contexts, whether it be the destruction of digital and telecommunications infrastructures in throughout Gaza and East and Southeast Ukraine or outside states ordering shutdowns across borders (i.e., China in Myanmar; Russia in Ukraine, and Israel in Gaza) (ibid).

What's more, is that governments have swiftly worked with tech firms, their own militaries, and other nefarious actors to adapt to the ways in which every day people are simply demanding change for a better quality of life. Another key weapon governments have used against civilian has been surveillance. For example, the proliferation of spyware to target journalists, critics, and other key persons of interest has been of particular concern. NSO Group, a private Israeli tech firm, and Paragon, a US-backed Israeli tech firm, have both been implicated in developing software used to spy on journalists, civil society members, government critics, and more (Citizen Lab, 2025; Franceschi-Bicchierai, 2025; Kinetz & Santalucia, 2025). Termed the "Mercenary spyware industry", these firms – NSO, Paragon, Intellexa, and likely others – have been tied to reports that government officials have ordered surveillance software from these companies to spy on its citizens, especially those in journalism and civil society (Kinetz & Santalucia, 2025) At the time of this writing, it has come out that the Italian Prime Minister, Georgia Meloni, may have ordered Graphite, spyware from Paragon, to spy on journalists and others who are critical of her government. This same software also been tied to at least 90 WhatsApp users in over two dozen countries, but primarily in Europe. Regarding Europe, this has been a growing concern. Hungarian Prime Minister, Victor Orbán, has been relying on spyware for years to keep tabs on journalists for their sources and other key opposition. In October 2023, a scandal broke that Predator spyware, designed by the Intellexa alliance -- a group of firms based in Northern Ireland who focus on the development of spyware, had targeted the President of the European Parliament (Roussi, 2023). Itellexa has not only loudly proclaimed its European roots, with offices across the continent and even in the United Arab

Emirates. In a 2023 report published by Amnesty International, it was discovered that its products had been purchased by several governments around the world: Switzerland, Austria, Germany, Oman, Qatar, among others.[1] And it hasn't stopped there. While relying on more traditional methods of surveillance, the Obama administration via the National Security Agency was caught tapping phone calls of Angela Merkel and her advisors (Reuters, 2015).

While these reports were damning, especially for European nations, surveillance and other forms of digital monitoring have been integrated into other regimes more swiftly, often used to target those who do not fit in with the government's definition of what it means to be a citizen of a given state, often rejecting groups more marginalized: immigrants, refugees, and asylum seekers, people from non-majority ethnic or racial groups, women, LGBTQ+ individuals, indigenous groups, unhoused populations, among other groups. From catfishing of queer men in Egypt by law enforcement to dissidents and critics in exile from authoritarian rule in China, Hong Kong, Myanmar, and Saudi Arabia having their social media monitored and endure other forms of transnational digital repression (Human Rights Measurement Initiative, 2025a, 2025b, 2025c, 2025d; Human Rights Watch, 2024b; Open Observatory Network of Network Interferences, 2022a). Over the years, technology has been a key mechanism to halt liberal democratic growth by authoritarian elites. Increasing numbers of this phenomena has rapidly increased over the years, including examples such as India being designated the number one global offender of internet shutdowns year after year; the Myanmar military junta being crowned the title of "Digital Dictatorship" since its military coup in 2021; countries throughout Africa such as Mozambique, the Democratic Republic of Congo, Burundi, Mauritania, Tanzania, Gabon, and Guinea where governments weaponizing the

[1] Other governments who bought Predator spyware systems: Congo, Kenya, the United Arab Emirates, Singapore, Jordan, and Vietnam. The Amnesty report also indicates that other governments have likely purchased the spyware: Sudan, Mongolia, Madagascar, Kazakhstan, Egypt, Indonesia, Angola, and others. See: https://www.amnesty.org/en/latest/news/2023/10/global-predator-files-investigation-reveals-catastrophic-failure-to-regulate-surveillance-trade/)

internet and other telecommunications service restrictions during election cycles; and cutting off the world to from witnessing mass protests demanding improved reforms on the economy, human rights, and other governance issues in Iraq, Iran, Belarus, New Caledonia, Senegal, Suriname, Türkiye.

Digital Repression and Digital Rights

The use of technology by governments to repress everyday citizens has come a long way since the first internet shutdown in 2011, with the state of today's digital political sphere being dominated with ever-evolving ways that government can weaponize the internet, social media, and technology to stifle advocacy efforts both at domestic and international levels. Although some of these processes have been detailed in a brief overview above, the ways in which governments have worked to curtail various freedoms within digital spaces and through digital means is far more spanning than internet shutdowns, service restrictions, and surveillance. With this project's contribution to the burgeoning literature on digital rights and digital repression, it is imperative to establish two critical concepts that underpin this dissertation project.

Digital rights are simply human rights as expressed and enjoyed through digital means. For example, one can express their opinions in physical spaces through having campaign signs displayed at their homes, wearing clothing that either supports or criticizes certain beliefs, attending protests, or performing some kind of artistic work to audiences carrying out a political or social message. To express these as digital rights means using digital spaces to carry out the same goals: posting on social media one's political, economic, social, or cultural views; sharing reels or live streams of protests or sending information on protests to broader audiences, selling clothing with political messaging on an online store, etc. These also span the right to digital privacy, which includes being free from surveillance or interference of one's online communications – be it through social media,

email, texting, etc.; online doxxing; and having one's personal, private information not being scraped, accessed, or taken without their consent.

Digital repression refers to the ways in which digital technologies are used to facilitate repression. This project relies on Conrad and Ritter's (2019) conceptualization of repression:

> *"Repression is any threatened limit or coercive action levied by government authorities to control or prevent domestic political challenges that would alter the status quo policy or distribution of power. Repression is motivated as a response to or in prevention of dissent. It can be legal or illegal, violent or nonviolent…Any behavior used to prevent people from participating in their own governance"* (Ritter and Conrad, 8-9).

Although Conrad and Ritter's (2019) conceptualization of repression inherently focuses on the domestic level, the nature of digital repression makes this a challenge at the international level as well. Referring to the cases of transnational repression, this is one area in which traditional forms of repression, such as the definition above, may be too narrow in scope. According to the Human Rights Measurement Initiative's 2024 data on transnational repression carried out by China, respondents not only indicated that China has engaged in traditional repression outside of its own borders, but it has done so across dozens of countries. This has occurred largely through digital tactics, including "spying, monitoring individuals through surveillance and social media, monitoring social media activities, phones and, and emails of Chinese nationals living abroad" as well as cyberattacks, online doxxing, pressuring foreign companies into censorship of state criticism, digital propaganda dissemination, and several other actions (Human Rights Measurement Initiative, 2025a). When thinking about international advocacy efforts, governments also often rely on digital repression tactics, such as internet shutdowns or communication service disruptions (e.g., limiting the ability to use Facebook Messenger, WhatsApp, Signal, or SMS services), these responses by the government also limit the ability of outsiders to assist in promoting better human rights conditions.

Further, there are cases where states may provide digitally repressive technologies and ideas to governments of other countries, such as the Chinese government's assistance in bringing digitally repressive systems to the military junta in Myanmar.

In each of the cases outlined above, the use of repression via digital tech is clear. For example, the government of Myanmar use of digital repression was used alongside the military coup on February 1, 2021, ousting democratically elected officials from the National League for Democracy's party including Aung San Suu Kyi. As soon as the junta took over, the government immediately relied on a series of internet shutdowns, digital curfews, ISP and SMS blackouts before shifting to a series of targeted, provincial (Hpakant) and township level internet shutdowns by September of 2021. As resistance and fighting ramped up between the military and rebels, other blackouts began spreading, often targeting Chin state, and parts of Magway and Saiging before spreading even further to Kayah and Shan states. Internet shutdowns - all the way from national shutdowns to more targeted level shutdowns that impact townships or entire provinces. Yet, this wasn't the only form of digital repression the Tatmadaw (i.e., the Burmese military) utilized. Outside of shutting down SMS and mobile capacities, the regime began monitoring and seizing bank accounts of those involved in or supporting revolutionary rebels. By September of 2021, one of the major telecoms providers, Telenor Myanmar, announced that their services would no longer be tenable within the country due to government demands to install surveillance equipment and systems that would impact their products. In January 2022, the government released its second draft of its draconian "Cyber Law", which included language that would ban VPNs and other services used to circumvent state censorship. Throughout this time, the government had also imposed taxes on SIM cards and other internet services, leading to a significant rise in the costs of telecommunications services. Six months later, the military government's State Administration Council (SAC) announced plans to build out a mass surveillance network using facial recognition

and CCTV systems, which were backed by the Chinese government. These tactics continued to grow overtime, and currently the Tatmadaw is working to create a national database of all citizens, working to find and arrest individuals whose bank accounts had been frozen, has created a list of over 50,000 activists, civil society members, individuals who defected or deserted the military or police and have submitted data to a monitoring system to arrest these individuals (Associated Press, 2024; Human Rights Myanmar, 2024, 2025; Myanmar Internet Project, 2025a, 2025b).

Project Goals and Outline

This dissertation will explore various facets of digital repression that have either not been addressed or that will continue to build on prior work in this area. Through detailing the cases included in the above sections, three core themes from these examples underpin the motivations for the questions proposed by this project. First, a growing trend in digital repression is the usage of internet shutdowns. Shutting down the internet definitively impact the lives of those who are subjected to this form of digital repression. Healthcare, education, commerce, emergency services, and other facets of everyday life become casualties of internet shutdowns and communications restriction. Politically, examples such as during election periods, some governments may restrict the flow of information on polling locations, voting times, and potential government-sanctioned violence against those seeking to vote for the opposition or to punish those who reject results of elections deemed not free and unfair. Military coups, restriction criticizing political elites in power, or using internet shutdowns to shut off avenues through which dissidents can organize are often other contexts where internet shutdowns have been justified by governments. Even in the context of conflict, the destruction of digital infrastructures has severely limited the ability of victims of state perpetrated violence to have little resource or voice to outside observers.

Yet one of the key mechanisms through which the human rights regime has facilitated the reduction in rights abuses throughout the world has been transnational advocacy. International members of human rights regime have worked in conjunction with domestic civil society and other relevant actors to call attention to government human rights violation within a country through pressure campaigns. By calling out the specific abuses and shaming government officials who give the thumbs up on carrying out violence and other violations, these collectives have been able to reduce human rights abuses by coercing states into human rights compliant behavior. With highlight such abuses, offending governments are at risk of various types of punishment: economic sanctions, loss of aid or investments, other forms of economic coercion, diplomatic responses, and possibly military interventions. Chapter 2 explores how transnational advocacy networks may impact internet shutdowns. Specifically, when these networks of human rights advocates come together to pressure governments into human rights compliant behavior, could this further motivate governments to shut off the internet to hide further evidence of abuses? This article evaluates both the roles of domestic and internet shaming in terms of their roles – independently and combined – in eliciting on of the harshest government responses to dissent. Further, the study includes some exploration into the role of state capacity – or the ability of a state to govern and engage in policy – as it may factor into internet shutdowns. This, too, is studied both independent and interacted with the effects of transnational shaming campaigns. Finally, the chapter addresses the question of whether states who have previously carried out internet shutdowns are more likely to do so again.

To continue building on the role of internet shutdowns as a tool of digital repression, Chapter 2 explores how governments decide to select from competing digital repression strategies. As Gohdes (2023) contends, the use of surveillance and internet shutdowns theoretically is at tension with one another. If the internet is completely shut down, it could be more difficult to surveil and monitor effectively. And in some cases, preference has been given to opting for

surveillance-based approaches over internet or other service blocking approaches. What influences governments to opt for surveillance-based approaches over reduce-connectivity approaches? Through using a series of seemingly unrelated regression, this study analyses this question. The results offer interest and unanticipated insights into domestic factors that could influence the decision calculus of regime elites, and this study sets the stage for other avenues to more directly get at these relationships.

Finally, the other clear theme from this introduction is the role of authoritarianism and democratic erosion. While there has been little debate regarding the recent backsliding of democracies across the globe (Freedom House, 2025; Idea International, 2025; Levitsky & Way, 2020; Lührmann & Lindberg, 2019; Varieties of Democracy, 2025), how has this relationship between digital repression and the ride of authoritarianism evolving? Chapter 3 evaluates this relationship from the framework of legitimation. As Linz and Stepan (1989) argued years ago, that legitimacy may a starting path for a liberal democratic decline. When democratically elected officials win through free and fair elections, this exemplifies one of Max Weber's (1980) concepts of legitimacy: rational-legal legitimacy. Here, citizens are able to participate freely in regular, free and fair competitive elections and accept the results that have been justified through laws and norms of a given state. In democratic societies, citizens' perceptions and acceptance are bolstered states' constitutions, laws, and norms surrounding democratic systems. However, as Linz and Stepan argue, there are always those that deny widely held legitimacy.

In the information age, where digital technology aides instantaneous and far-reaching audiences, messaging surrounding denial of rational legal legitimacy is more likely than ever. With common issues of social media companies, hyper polarized media, and political leaders' ability to censor and monitor information being spread, these conditions make it easier than ever to spread misinformation, propaganda, hate speech, and other illiberal ideas or rhetoric. In turn, some tech has

made it even easier for authoritarian wannabes to garner greater attention, leading more frequently to the rise of authoritarian, illiberal, and other extreme populist leaders to achieve positions of power. Often, their key messaging centers on the preservation of national identity, law and order, anti-immigration, and other key stances that tend to further place marginalized peoples in national out-groups. Once in power – regardless of being accepted through means of rational legitimacy or through personalist legitimacy – how does legitimacy function into the erosion of empowerment rights enjoyment? What could this mean for privacy rights violations and digital repression more broadly? Chapter 4 answers this question, building off the work of Bagwell, Rains, and LaVelle (2023) which found that personalist leaders, compared to other leaders who derive their legitimacy from other means, are more likely to engage in physical integrity rights abuses.

The final section of the dissertation will focus on the key takeaways from the three chapters. Chapter 2 finds that mass mobilization does increase the rate of internet shutdown events, which in this chapter include both traditional internet shutdowns and other service stoppages. It also finds that as the number of transnational shaming events rise, there is a rate increase of internet shut down events. However, there is a weak conditional effect when pairing domestic mass mobilization with shaming. The only point at which this effect becomes significant is when both shaming events are increasing at points where mass mobilization is growing – protests, demonstrations, and other forms of non-violent dissent are more frequently occurring and shaming is increase, but once mobilization hits its peak, the effect washes away. Chapter 3, which evaluates the role of prolonged dissent or sporadic dissent as being a key driver of how leaders may substitute or complement other forms of traditional repression with surveillance-based approaches or reduced connectivity approaches, respectively, the results are mixed. While the preliminary results may suggest that as dissent movements grow and persist will lead to greater levels of surveillance and to suggest an interactive effect between sporadic or sudden dissent with internet shutdowns, there should be more

work done on this relationship. Chapter 4 provides evidence to suggest that personalist leaders are likely to violate empowerment rights across the board – the very rights that facilitate freedom of expression and opinion, assembly and association and more that are key to digital rights enjoyment online. Regarding privacy rights and digital rights more broadly, support is only found for the latter: Personalist regimes are more likely than other regimes to engage in digital repression. Following a revisit of the results and what they mean substantively, the project will conclude with next steps and future research avenues.

References

Access Now. (2020). "Belarusian election tainted by internet shutdown and state-sponsored violence." https://www.accessnow.org/belarusian- election- tainted- by- internet-shutdown- and- state- sponsored-violence

Access Now. (2024a). Authorities and internet service providers in mozambique must respect human rights and keepiton during protests. https://www.accessnow.org/press-release/keepiton- mozambique-authorities-must-respect-human-rights/?tztc=1

Access Now. (2024b). "The world must bring down myanmar's digital iron curtain." *Access Now* https://www.accessnow.org/press-release/third-year-myanmar-coup

Access Now. (2025). Lives on hold: Internet shutdowns in 2024. Retrieved June 12, 2025, from https://www.accessnow.org/internet-shutdowns-2024/

Agar, J. (2000). [Review of *Crystal Fire: The Birth of the Information Age*, by M. Riordan & L. Hoddeson]. *The British Journal for the History of Science*, *33*(2), 245–247. http://www.jstor.org/stable/4027936

Al Jazeera (2016). "Arab Spring Anniversary: When Egypt cut the internet" Retrieved June 12, 2025, from: https://www.aljazeera.com/features/2016/1/25/arab-spring-anniversary-when-egypt-cut-the-internet

Al Jazeera (2020). "What is the Arab Spring and how did it start?" Retrieved June 5, 2025, from: https://www.aljazeera.com/news/2020/12/17/what-is-the-arab-spring-and-how-did-it-start

Angrist, M.P. (2013). "Understanding the Success of Mass Civic Protest in Tunisia" *Middle East Journal,* 67(4): 547-564.

Associated Press. (2023). "2023 country reports on human rights practices: Egypt." https://www.bbc.com/news/world-middle-east-64390817

Associated Press. (2024). Myanmar's embattled military government cracks down on free flow of news by blocking vpns. Retrieved July 3, 2024, from https://apnews.com/article / myanmar-censorship-virtual-private-network-facebook 79fb4cc0c3c4317844d0c00b0be1d9d1

Bagwell, S., Rains, M., & LaVelle, M. (2023). Of one's own making: Leadership legitimation strategy and human rights. Journal of Conflict Resolution, 68 (10), 1994–2018. https://doi.org/https://doi.org/10.1177/00220027231220006

Bureau of Democracy, Human Rights, and Labor. (2023). 2023 country reports on human rights practices: Egypt. https://www.state.gov/reports/2023-country-reports-on-human-rights-practices/egypt/

Citizen Lab. (2025). Graphite caught first forensic confirmation of paragon's ios mercenary spyware finds journalists targeted. Retrieved June 12, 2025, from https://citizenlab.ca/2025/06/first- forensic-confirmation-of-paragons-ios-mercenary-spyware-finds-journalists-targeted/

Conrad, C. & Ritter, E.H. (2019). *Contentious Compliance* Oxford University Press: New York

Deutsche Welle. (2018). Dr congo: Internet, sms shutdown after election. https://www.dw.com/en/dr-congo-internet-sms-shutdown-threatens-crediblity-of-election/a-46917740

Dye, L. (1997). "50 years ago, information age begins in Bell Labs. Retrieved June 12, 2025, from: https://www.latimes.com/archives/la-xpm-1997-dec-22-fi-1177-story.html

Franceschi-Bicchierai, L. (2025). "Researchers confirm two journalists were hacked with paragon spyware" *Tech Crunch* Retrieved on June 12, 2025, from: https://techcrunch.com/2025/06/12/researchers-confirm-two-journalists-were-hacked-with-paragon-spyware/

Gohdes, A. (2024). *Repression in the digital age: Surveillance, censorship, and the dyanmics of state violence.* Oxford University Press.

Human Rights Measurement Initiative. (2025a). China: Transnational repression. https://rightstracker.org/country/CHN?tab=transnational-repression

Human Rights Measurement Initiative. (2025b). Freedom in the world 2025: The uphill battle to safeguard rights. https://freedomhouse.org/report/freedom-world/2025/uphill-battle-to-safeguard-rights

Human Rights Measurement Initiative. (2025c). Safety from the state - overview (2023). https://rightstracker.org/country/SAU?tab=report-physint

Human Rights Measurement Initiative. (2025d). Safety from the state - overview (2024). https://rightstracker.org/country/SAU?tab=report-physint

Human Rights Myanmar. (2024). The great firewall of myanmar. https://humanrightsmyanmar.org/the-great-firewall-of-myanmar/

Human Rights Myanmar. (2025). Myanmar's cyber law a serious threat to privacy, speech, and security. https://humanrightsmyanmar.org/myanmars-cyber-law-a-serious-threat-to-privacy- speech-and-security/

Human Rights Watch. (2019). *Human Rights Watch* A web of impunity: The killings iran's internet shutdown hid. https://iran-shutdown.amnesty.org/

Human Rights Watch. (2023). Iran: Events of 2023. https://www.hrw.org/world- report/2024/country-chapters/iran#3b97c4

Human Rights Watch. (2024a). Mozambique: Post-election internet restrictions hinder rights. https://www.hrw.org/news/2024/11/06/mozambique-post-election-internet-restrictions-hinder-rights

Human Rights Watch. (2024b). Saudi Arabia: Events of 2023. https://www.hrw.org/world- report/2024/country-chapters/saudi-arabia#c4123b

Idea International. (2025). The global state of democracy 2024. Retrieved June 5, 2025, from https://www.idea.int/gsod/2024/

Kinetz, E. & Santalucia, P (2025). "US-backed Israeli company's spyware used to target European Journalists, Citizen Lab finds" *Associated Press* Retrieved on June 12, 2025, from: https://apnews.com/article/spyware-italy-paragon-meloni-pegasus-f36dd32106f44398ee24001317ccf2bb

Lawal, S. (2024). 'Ready to die': Protesters face bullets for political change in mozambique. https://www.aljazeera.com/features/2024/10/31/ready- to- dieprotesters- face- bullets-for-political-change-in-mozambique

Levitsky, S., & Way, L. A. (2002). "Elections without democracy: The rise of competitive authoritarianism." *Journal of Democracy*, 13 (2), 51–65.

Lürhmann, A., & Lindberg, S. I. (2019). A third wave of authocratization is here: What is new about it? Democratization, 26 (7), 1095–1113.

Meng, A., Kelly, T., & Belson, D. (2025). Mozambique's post-election fallout: Fatal protests and widespread internet shutdowns. https://ioda.inetintel.cc.gatech.edu/reports/mozambiques-post-election-fallout-fatal-protests-and-widespread-internet-shutdowns/

Myanmar Internet Project. (2025a). Internet shutdown by each region. https://www.myanmarinternet.info/digital-coup

Myanmar Internet Project. (2025b). Recent developments (digital coup). https://www.myanmarinternet.info/digital-coup

NBC. (2023). Grindr sends Egypt users a warning after alleged entrapments and arrests https://www.nbcnews.com/nbc-out/out-news/grindr-sends-egypt-users-warning-alleged-entrapments-arrests-rcna76349

Netblocks. (2018). Evidence of internet shutdowns in DRC amid election unrest. https://netblocks.org/reports/evidence-of-internet-shutdowns-in-drc-amid-election-unrest-PW80YLAK

Netblocks. (2023a). Internet cut in Gabon on election day. https://netblocks.org/reports/internet-cut-in-gabon-on-election-day-Q8oxM3An

Netblocks. (2023b). Social media restricted in Suriname amid cost-of-living protests. https://netblocks.org/reports/social-media-restricted-in-suriname-amid-cost-of-living-protests-QAdPQNAl

Netblocks. (2023c). Social media restricted, mobile internet cut in Senegal amid political unrest. https://netblocks.org/reports/social-media-restricted-and-mobile-internet-cut-in-senegal-amid-political-unrest-W80QkaAK

Open Observatory of Network Interference. (2020a). Belarus protests: From internet outages to pervasive website censorship. https://ooni.org/post/2020-belarus-internet-outages-website-censorship/

Open Observatory of Network Interference. (2020b). Burundi blocks social media amid 2020 general election. https://ooni.org/post/2020-burundi-blocks-social-media-amid-election/

Open Observatory of Network Interference. (2020c). Tanzania blocks social media (and tor?) on election day. https://ooni.org/post/2020-tanzania-blocks-social-media-tor-election-day/

Open Observatory of Network Interference. (2021). Zambia: Social media blocked amid 2021 general elections. https://ooni.org/post/2021-zambia-social-media-blocks-amid-elections/

Open Observatory of Network Interference. (2022a). Imap state of internet censorship report 2022 – hong kong. https://ooni.org/post/2022-state-of-internet-censorship-hong-kong/

Open Observatory of Network Interference. (2022b). Technical multi-stakeholder report on internet shut-downs: The case of iran amid autumn 2022 protests. https://ooni.org/post/2022-iran-technical-multistakeholder-report/

Reuters. (2015). U.S. spy agency tapped German chancellery for decades: Wikileaks. Retrieved June 12, 2025, from https://www.reuters.com/article/world/us-spy-agency-tapped-german-chancellery-for-decades-wikileaks-idUSKCN0PI2AD/

Robinson, K., & Merrow, W. (2020). The Arab Spring at ten years: What's the legacy of the uprisings? Retrieved June 12, 2025, from: https://www.cfr.org/article/arab-spring-ten-years-whats-legacy-uprisings#chapter-title-0-6

Roussi, A. (2023). How europe became the wild west of spyware. Retrieved June 12, 2025, from https ://www.politico.eu/article/how-europe-became-wild-west-spyware/

United Nations Office of the Commission on Human Rights. (2025). Iran: Government continues systematic repression and escalates surveillance to crush dissent in the aftermath of protests, un fact-findingmission says. https://www.ohchr.org/en/press-releases/2025/03/iran-government-continues-systematic-repression-and-escalates-surveillance

Varieties of Demmocracy. (2025). Democracy report 2025: 25 years of autocratization - democracy trumped?Retrieved June 5, 2025, from https://v-dem.net/documents/61/v-dem-dr 2025 lowres v2.pdf

Chapter 2

GOING OFF THE GRID: HOW DIGITAL REPRESSION DISRUPTS TRANSNATIONAL ADVOCACY NETWORK SHAMING [2]

[2] Lavelle, Meridith. To be submitted to a peer-reviewed journal.

Abstract

How do human rights advocacy efforts impact internet shutdowns? Scholars have long assessed the utility of shaming campaigns, finding evidence that under the certain conditions, naming and shaming can be an effective approach to improving human rights outcomes. Yet, as governments are increasingly being shamed for human rights violations in the digital era, regimes may have more incentive to deflect or hide information on abuses. When internet shutdowns are ordered by regime elites or leaders themselves, domestic civil society may be unable to mobilize as readily, consequently inhibiting international responses to state repression due to weakened information environment. Using a series of negative binomial count models, this study finds that mass mobilization and shaming events increase frequency of shutdowns, and there is an interactive effect on internet shutdowns when mass mobilization is experienced at higher levels as state capacity diminishes.

Introduction

In August of 2017, a long history of oppression and persecution of the Rohingya, a Muslim minority ethnic group in Myanmar, came to a head. When the Burmese military, also known as the Tatmadaw, carried out a genocidal campaign that triggered international condemnation. The violence against the Rohingya by the Burmese military government hardly came out of nowhere. Since the 1990s, the Tatmadaw has targeted the Rohingya with violence, triggering the first of many involuntary displacements of the Rohingya in the modern era. The early 2010s marked a significant rise in violence against the Rohingya by Burmese state agents, culminating in the genocide of the Rohingya, particularly those living in Rakhine and Chin provinces (Human Rights Watch, 2022; US Holocaust Memorial Museum, n.d.). As more information about the burning of Rohingya villages, sexual violence against Rohingya women, and extrajudicial killings surfaced, the international

community swiftly labelled these actions as state-sanctioned genocide (Albert & Maizland 2020). Human rights organizations worldwide pressured the state to halt its egregious policies of genocide and broader violence towards Rohingya. Violence continued, and in turn so did the international pressure by civil society networks via the use information on acts of violence committed by the Burmese military. International pressure also came in the form of economic sanctions, arms embargoes, and recognition of violence as genocide and crimes against humanity (Council of the European Union, 2024; Spetalnick & Brunnstrom, 2018). In 2019, the Tatmadaw ordered that all internet capabilities were to be shut down in Rakhine state, with communications only coming back online in early 2021, although more shutdowns have been ordered since the military coup in the same year (Myanmar Internet Project, 2025a). By limiting these communications while monitoring and restricting movement in and out of Rakhine, the military government of Myanmar sought to control the informational flows of the area, limiting direct information on violence against the Rohingya. At the time of writing, this shutdown episode is the longest recorded anywhere in the world (Human Rights Watch, 2020; KrASIA, 2021).

Despite the 2017 international shaming campaigns, the Burmese military government initially only ordered internet shutdowns in the areas where the government was forcing Rohingya people to live and did so after four years following pressure. This case highlights the strategic nature of restricting information by the government, which may have widespread impacts on how human rights advocates who rely on this information to pressure abusive governments to make changes. More pointedly, for networks of human rights advocates (i.e., transnational advocacy networks) that rely on evidence of state violence from people on the ground, does restricting access to internet and other telecommunication services by governments impede naming and shaming efforts? Moreover, as states become repeated targets of naming and shaming campaigns, do they learn and adapt to

these strategies by using strategies of internet and telecoms shutdowns to slow or completely cut off information flows to prevent information on widespread repression on the ground?

This article seeks to evaluate the relationship between governments' decision to engage in digital repression within the context of human rights violations and how these dynamics are shaped by naming and shaming campaigns in the digital era. Naming and shaming has been used for years as a strategy of coordinating efforts between domestic and international civil society, NGOs, INGOs, governments and other related actors to call attention to governments engaging in human rights abuses and pressure offending regimes into human rights compliant behavior. Crucially, these campaigns are perceived as being threatening to ruling regimes who engage in human rights abuses. As a result, governments will likely respond to shaming through strategic avoidance with the goal of minimizing costs in the face of international pressure. One such method that governments have increasingly been utilizing to avoid the shaming spotlight centers on digital repression tactics. By manipulating digital technology, communications, and other means to transmit information, state leaders and their agents can maintain a grip on the control and transmission of information, particularly that which may implicate the regime in human rights abuses. In turn, these responses have significantly hindered informational flows between domestic actors and transnational advocates. This article contextualizes the theoretical arguments within two key strands of literature: repression and the closing of civil society spaces. The main theoretical arguments contends that states' usage of digital repression provides violating governments a prime option to swiftly disrupt informational flows, hide evidence of abuses, and incentivize self-censorship of individuals within a state. This ultimately creates significant barriers for exchanging critical details about violence carried out by the state between domestic targets, local civil society, and outside advocacy partner. With informational flows inhibited between key opposition on the ground, who are often backed by human rights civil society organizations (CSOs) and their international partners, the efficacy of

coordinated shaming campaigns is drastically reduced. Further, the purposes of a government's decision to employ digital repression differ for domestic and international audiences. In other words, the processes for each audience must be borne out to better understand how these processes work together to combat advocacy efforts from shaming campaigns.

The article will proceed as follows: it will begin by offering a conceptualization of digital repression. Then, the article will provide a brief review of the repression-dissent nexus and the closing of civil society spaces, particularly focusing on why states want to avoid shaming and the mechanisms by which governments have at their disposal to achieve these goals. By focusing on threats to regime leadership through the lens of repression dynamics and the targeting of civil society spaces, transnational advocacy networks who are the primary sources of collecting evidence on human rights abuses and sharing information to broader audiences pose a significant threat to continued leadership in the violating country. Because of this threat to regime tenure, governments are more likely use digital means to disrupt global human rights advocacy networks that seek to reduce violent human rights issues. With internet shutdowns, human rights abusing regimes may find a swift strategy to hide information to evade accountability through TAN shaming. To test the main arguments, the article will present the empirical strategy, key variables, results, and discussion of findings. Finally, the article will conclude with some potential implications and policy suggestions.

The role of information technology in repression and dissent

What is digital repression? This project conceptualizes digital repression much in the same way as Feldstein (2021): ``the use of information and communications technology to surveil, coerce, or manipulate individuals or groups in order to deter specific activities or beliefs that challenge the state" (Feldstein, 2021) This includes violations at the level of policy, not just practice. The decision for a state's government and its agents to engage in policy options where digital technologies are

used or targeted for political purposes should be understood as a form of repression. Standard forms of digital repression include internet shutdowns, SMS and other service throttling, censorship, content moderation or filtering, surveillance, data harvesting, banning of VPNs, spyware, and online propaganda, among others. For example, following 9/11, the United States government passed the Patriot Act in 2001, which legally expanded domestic surveillance capacity of the government on citizens and other foreign nationals within (and outside of) US borders. Through expansion of the executive and broadening to powers of the National Security Agency (NSA), it eventually came to light just how vast these powers were. In 2013, Edward Snowden, revealed that the NSA had been secretly collecting data from telecommunications providers on tens of millions of US citizens. Further, the media published documents detailing the "Prism" program carried out by the NSA where the agency also tapped into servers of several major internet companies to monitor communications of US citizens (BBC, 2014). In Saudi Arabia, both ordinary citizens and Saudis in exile are routinely monitored online and are met with arrest based on their online activities (Amnesty International, 2023; Human Rights Measurement Initiative, 2024b). According to the 2024 press release by the Human Rights Measurement Initiative on digital rights, governments in India, Sri Lanka, Malaysia, Vietnam, Mexico, Kazakhstan, China, Angola, and Saudi Arabia engaged in a variety of digital rights violations. Across these contexts, journalists, human rights defenders, NGOs, marginalized groups, and critics experienced various types of digital rights violations, ranging from arrest, torture, and being handed the death penalty for simply engaging in criticism online (Human Rights Measurement Initiative, 2024a).

Why would a government engage in digital repression, especially given more traditional versions of state repression that have been historically available to governments? One generally consistent finding about repression is that it is commonly used to deter or respond to internal threats to a regime (Davenport, 2007). When states weigh their options of how to respond to

demands or challenges from their populaces, leaders have various ways in which they can respond. Traditionally, this menu of options has been stylized to include accommodation, co-optation, repression, or no response. Given various institutional constraints (e.g., regime type, degree of state capacity, level of development, etc.), states make the decisions that will achieve their goals at the minimal costs (Poe, 2004). Even when choosing repression, government officials weigh the costs and benefits to engaging in this strategy, opposed to other options, to quell dissent. When the benefits outweigh the costs and repression is seen as the most cost-efficient option to the state, the state is most likely to opt for this policy option (Davenport, 2007). This is not to say that this option is chosen in isolation; repression is often chosen alongside other options.

Given the calculated nature of choosing repression, this decision is also considered to be strategic -- states will not only choose this option when it is deemed the most efficient to accomplish goals of the regime, but it can be in anticipation of or in response to episodes of dissent (Ritter & Conrad, 2016). However, opting for repressive responses may also elicit further problems for a government when carried out, especially when highly visible to broader domestic and international audiences. Domestically, this may not only mean an increase in violence against those who oppose a regime, but once violence is brought into political contention, challengers of the regimes may also respond with violence. This would escalate tensions within the state and could lead to civil conflict. Internationally, violent state actions could lead to massively negative consequences from the international community. These negative responses include (but are not limited to) threats to economic, social, political, communal, and societal security, both from internal and external actors.

Transnational advocacy in the digital age

Modern episodes of contention - both violent and non-violent - have witnessed increased reliance on social media, communications technologies, and online journalism, all of which are

inherently rooted in the sharing of information instantaneously across the globe. While controls on information, surveillance, and telecommunications blackouts tend to be more characteristic of autocratic regimes, the role of technology as it relates to digital repression, too, has seeped into democracies (Feldstein, 2021; Earl, Maher, & Pan, 2022; Zeitzoff, 2017). Since being more broadly adopted, the internet and online social media tools have led to shocks in traditional pathways groups must overcome for addressing collective action problems (Chen, Oh, & Chen, 2021; Enikolopov et al., 2018; Pierskalla & Holldenbach, 2013). Digital capacities have reduced these barriers, namely as shifting to conceptualizing collective action in digital spaces as ``a set of communication processes involving the crossing of boundaries between private and public life" (Bimber et al. 2005, 367). Governments, particularly autocracies, have taken note of this and have increasingly adapted by using technology to their own benefits -- consolidating power via controlling and monitoring online spaces to counter dissident movements (Earl, Maher, & Pan, 2022; Gohdes, 2015, 2018, 2023; Weidman & Rød, 2015; Rød & Weidmann, 2019; Xu, 2022). As a result, both governments and their challengers have experienced changes in the ways in which communication plays a role in politics, with such changes evolving all the time (Howard & Hussain 2013). In the same realm, the ability of individuals to freely share information has traditionally underpinned the ability and success of civil society actors in all countries to be able to hold human rights abusing regimes accountable. From cases such as the coup and Rohingya genocide in Myanmar (Albert & Maizland, 2020; Human Rights Watch, 2020), Russia's invasion into Ukraine, the ongoing conflicts (and genocides) in Sudan and Ethiopia, electoral violence episodes in Uganda, the Democratic Republic of Congo, and Burundi, and calls for independence in New Caledonia, civil society organizations across these types of cases rely on the ability of individuals to share information about human rights violations occurring on the ground by governments in order to activate transnational advocacy networks.

Transnational advocacy networks (TANs), which are composed of domestic actors (civil society groups, dissidents, opposition members, grassroots organizations, human rights defenders) and international actors (INGOs, intergovernmental organizations, and other entities who share similar views on human rights), carry out essential functions of collecting and disseminating information to one another that functions as a way to monitor and hold states and their agents accountable for behavior regarding human rights abuses. These mechanisms extend to both policies that may curtail or violate human rights of people within a given border as well as the actions (or inactions) of state agents who abuse individuals' rights. Their overarching goal of TANs is to alter target state's behavior and policy making into complying with international human rights law (Keck & Sikkink, 1998). Linkages established throughout these networks work to promote human rights norms internationally, making these connections especially critical in terms of collecting information of rights violations at domestic and regional levels where international actors may have less access to information on the conditions of human rights (Keck & Sikkink, 2014). TANs become key actors in the promotion of compliance to human rights norms particularly in cases where domestic populations in a given state may effectively hit a wall with demanding improve rights respect by its government, as is still the case in autocratic regimes in the digital era (Dragu & Lupu, 2021; Rød & Weidman, 2019; Weidman & Rød, 2015). In cases where abusive regimes are non-responsive or respond with more violence when faced with domestic demands for change, domestic groups can also work to "activate" TANs to assist with influencing governments to change their behavior. In other words, domestic actors, pressure states, "from below" and international actors' pressure abusive regimes "from above" simultaneously to achieve their overarching goals: compliance with international human rights standards (Brysk, 1993; Murdie & Davis, 2012).

In the face of an increasingly autocratizing world where many democracies have eroded and backslid (Amnesty International, 2024; Feldstein, 2021; Kendall-Taylor & Frantz, 2015; Varieties of

Democracy, 2024; Human Rights Watch, 2024), there is ample room for concern of how to hold those accountable who engage in human rights violations. Given the continued diffusion of the internet and digital technologies alongside the rise of autocrats, this poses the question of how domestic actors and the international community can continue to engage in non-violent coercive campaigns to shame human rights violating governments accountable in such way to push for compliance for human rights norms. This is especially pertinent in that autocratic regimes continue to work to close this space between human rights advocacy and civil society spaces. In this context, governments have relied on various policy options to neutralize the work of civil society organizations and weaken human rights accountability mechanisms at the source. These actors in particular - CSOs, human rights defenders, journalists, and others seeking accountability -- are likely deemed as threats to the offending regime. While digital repression is one of many strategies to temper domestic advocacy power, other tactics at regimes' disposal include banning civil society organizations, restricting travel of CSO employees, limiting CSO funding (both domestic and international), forcing CSOs to register as foreign entities, among others (Bakke et al. 2020; Smidt et al. 2016b). Those in power who are more likely to consolidate power by whichever means necessary, including the co-optation of digital means, will have a relatively greater control of information flows. How does the propensity of autocrats, and even some democrats, to engage in digital repression factor into the continued efficacy of transnational shaming campaigns? Further, given the increasing support for autocrats worldwide, what could shaming campaigns mean for domestic audiences who support the autocrat in the country being targeted for its government's human rights violating behaviors?

How digital repression complements physical repression

States have a variety of policy options at their disposal for responding to civilian grievances. Yet, states may also face constraints that often factor into decision-making calculus when choosing how to respond to dissent (Mason, 2008). Because leaders want to remain in power at the lowest cost possible, repression may present itself to be a viable option, particularly in conjunction with other policy responses. However, when regimes opt for repression as a response to domestic challenges, other costs can arise both domestically and internationally that pose threats to continued regime tenure.

Domestic threats to governments in digitally contentious environments

Seeking out ways to coerce state challengers while minimizing human and other subsequent costs functions as the most desirable option for the government elites. By reducing human costs incurred by violent state-ordered repression and resultant consequences from shaming campaigns as TANs receive documentation of abuses, leaders have incentives to find alternative means to address challenges to mitigate costs down the line. Given that state repression has often taken the form of either physical integrity rights abuses or civil liberties, shifting the focus away violent repression to greater curtailment of civil liberties may be appealing for leaders to reduce the appearance of overt violence. This strategy may help governments obtain their goals, especially with the threat of campaigns of naming and shaming by TANs. If a governments and their agents aim to counter challenges in such a way that they see as involving less overt violence, such as through engaging in surveillance of the population or through reducing online connectivity (i.e., internet shutdowns or telecommunications throttling), then the state may find itself in a more advantageous position: less overt violence could elicit a weakened international response to domestic human rights abuses while simultaneously compromising traditional mechanisms through which dissidents, CSOs, and other

human rights organizations typically organize. In the face of the ever-increasing reliance on the internet for coordinating dissent, expressing political opinions, sharing knowledge and educational materials, and circulating pertinent information on violence or other human rights violations committed by the state by civil society and other related actors, cutting off these channels make strategic sense for the state. Additionally, forms of repression that center on curtailing civil liberties, such as mass surveillance, censorship, etc., can compound the negative impacts experienced by human rights advocates whose work heavily relies on sharing information with international actors to pressure governments into respecting human rights. By directly attacking the internet, communications apps, and other services that domestic civil society and other human rights organizations utilize to transmit information to activate shaming campaigns, this provides a dual response when reassessing state policies of repression: less overt violence may elicit a weaker international response when a state engages in more non-violent forms of repression while simultaneously weakening the networks that advocate on behalf of human rights worldwide.

Mounting challenges to human rights abusing regimes, even in digital spaces, inherently means that domestic political challengers will still have to overcome collective action problems. There are many key actors necessary in keeping international and domestic actors informed on the conditions of political violence and human rights abuses, namely civil society groups, independent media, opposition group leaders, activists, and human rights lawyers.[3] Because these actors are the ones on the ground reporting on events and engaging in information sharing, interviewing participants of protest/dissident activity or victims of state violence, documenting abuses, and/or coordinating responses to state actions against challenges, these actors are inherently privy to critical first-hand details and accounts of what abuses may have ensued during particular episodes of state

[3] This study excludes state-sponsored civil society organizations. These are not the types of civil society organizations that are likely to contribute to human rights advocacy in the face of government repression or other abuses.

violence. These groups provide critical information about who may have been targeted with human rights violation, the intensity of these rights violations, specific rights violations that civilians are enduring at the hands of the regime, how often the government and its agents are committing abuses, and which government actors or agencies are the primary perpetrators of violence. As domestic civil society actors (including independent media) have evidence that they can use in calling out specific cases of violence, pointing to larger trends in human rights abuses carried out by state agents as political conditions continue to deteriorate, the executive, regime elites, and other key government officials are unlikely to cave on such demands for leadership to step down, particularly when episodes of repression were premised on consolidating power in the first place. As government opposition groups continue to make demands, eliciting a broader public support and heightening perceived threats of the state and the state refuses to make these concessions, these domestic actors are more inclined to seek support elsewhere with the goal of pressuring states to halt violence committed by the state and hold violators accountable.

As interactions of state repression and civilian dissent recur and escalate, violence often becomes a key element of government responses to challengers. The primary goals of aggrieved groups in these contexts are to call attention to cases of state violations of human rights and to demand that states change their behavior to comply with international and domestic human rights legal obligations. As opposition groups collect information on abuses carried out against those who challenge the status quo -- including photos, witness accounts, videos, etc. -- these pieces of evidence become critical for domestic actors to use in attempting to pressure governments to concede, give in to demands, and halt abuses against opposition. From the perspective of the government, however, these items provide damning evidence of abuses carried out by the state and can result in punitive measures by those attempting to coerce it into human rights compliant behavior. As governments may face backlash to both domestic and international audiences if

documentation of abuses are widely released, these regimes have great incentives to hide evidence of violent human rights abuses in particular. Domestically, sharing evidence of abuses to people outside of an effected area could rally further challenges against the government. Given the increasing access to the internet and other instantaneous forms of communication that have continued to expand over the past several decades, the transmission of evidence that documents human rights abuses is also becoming exponentially easier. One such way that states have begun combating the quick transmission of this type of information is through shutting down or disruption of internet and/or telecom services at local, regional, or national levels. These tactics include governments ordering that internet service providers and/or telecommunication companies either completely cut off internet, mobile, SMS, phone services, block specific websites, or severely throttle their capacities as to slow down the transmission of information domestically and internationally. In some cases, such as during elections or political unrest, governments seek to justify internet shutdowns under the guise of halting the spread of misinformation. There is evidence to suggest that governments are more likely to engage in these tactics when their information communication technologies (ICTs) capacities are lower (Krcmaric, 2019).[4] However, even when states have higher levels of ICT penetration, governments can adapt to these constraints of disrupting services by engaging in targeting specific areas or regions with shutdowns, such as in India and China (Access Now, 2024). Regardless, shutting off the internet and other communication services would likely contribute to escalated tensions at the domestic level as families and communicates are unable to share critical information with one another, the general public may have little idea of what is truly going on, emergency services would likely be impacted, among dozens of other potential negative outcomes.

[4] ICTs refers to any technology used to communication information. These can include the internet, phone (landline or mobile), radio, television, newspaper, etc.

International threats in the face of digital repression

As campaigns of repression surge during cycles of contentious episodes between the government and its challengers, domestic opposition actors will likely seek assistance from other outside entities that can assist in providing resources for influencing the government's behavior in terms of reducing state-based violence, particularly when governments refuse to redress on-going injustices and violations of power. Moreover, as dissidents make these explicit demands of the government and the government does not concede and/or continues to repress, this will push domestic opposition actors who are aggrieved by ongoing state violence towards other outfits that sympathize with their demands. Information gathered by domestic actors that detail the nature of rights abuses is one of the most crucial components underpinning the activation of TANs. When domestic actors can utilize broader advocacy networks to share credible information on state violence to outsiders, this allows more power behind the shaming campaigns and provides both domestic and international audiences with evidence of abuse.

Regarding international threats to regime tenure in contentious environments, regime elites face multiple threats when information on abuses are revealed to international actors working to coerce rights violating regimes into human rights compliant behavior. While these costs can pose a threat to regime tenure for executives and their inner circles, subsequent threats from naming and shaming campaigns can pose further risks to the ability of state leader to remain in power. These risks can lead to an increase in various forms of economic statecraft: economic sanctions (Murdie and Peksen, 2012), loss of aid (Lebovic and Voeten, 2009; Murdie, 2009), loss of foreign direct investment (Barry et al., 2013; Jensen, 2003; Vadlamannati et al., 2018), decrease in sovereign credit rating (Bagwell and Hall, 2020), boycotts (Scruggs et al., 2011) among others. When facing these potential threats, leaders must account for these outcomes as well when deciding policy responses to dissent. As such, leaders are motivated to find ways to circumvent being thrown into the

international spotlight for their human rights violating behaviors to mitigate potential reputations costs and associated financial losses from being shamed. Further, incurring these costs undoubtedly leads to additional pressure by domestic challengers already demanding changes from the status quo. Exacerbating these tensions would compound the threats a regime is already facing. In cases where leaders are already facing financial constraints to remain in office, options to respond to domestic demands are similarly limited.

Conditions in neighboring countries may also influence governments' propensity to repress at home and in turn lead to motivations for violating regimes to evade the spotlight. As Danneman and Ritter (2014) argue, regime leadership may find conflict in neighboring states as a threat due within their own borders. As rebellion ramps up in a neighboring state, regime elites in the nearby state facing threats may be more likely to pre-emptively strike targets, or work to hide or manipulate information, influence, or other potential incentives that could drive domestic contention in the conflict state. In anticipation of these dynamics, leadership in a neighboring state not in conflict could see the conflict state's actions as drawing attention to the region, which could elicit shaming campaigns on the region, not just the conflict state. This heightens concerns of the governments as they are aware that they are being monitored, which often contributes to a reduction in human rights abuses (Kaire, 2024). Given the nature of information environments in these scenarios, restricting information access at home may prove advantageous for governments who are working to deter challengers and violate human rights with impunity in the face of monitoring mechanisms working more regionally. Monitoring mechanisms of state repression largely comes from the presence of human rights INGOs located in surrounding states. Bell, Clay, and Murdie (2012) argue and find evidence to suggest that when neighboring states have high numbers of HROs, these organizations can provide additional assistance in coordinating resources across borders to nearby states, as well as information sharing to broader, global audiences. This, too, can function as a threat to regimes

wanting to engage in campaigns of repression as these organizations function to hold human rights violating governments accountable for abuses. Given these arguments, this article presents the following hypotheses:

Hypothesis 1: *When a government is facing high levels of internal dissent, the state is more likely to engage in internet shutdowns and/or other telecommunication shutdowns.*

Hypothesis 2: *When a government is the target of a TAN shaming campaign, that state is more likely to engage in internet shutdowns and/or other telecommunication shutdowns.*

Hypothesis 3: *When a government is facing both high levels of internal dissent paired with TAN shaming, the state is more likely to engage in internet shutdowns and/or other telecommunication shutdowns.*

This logic does not mean that states will always opt for shutting down the internet in the face of contention where governments engage in human rights abuses and seek to hide or slow down evidence. They may resort to various types of digital repression. Regimes may opt for internet shutdowns alongside other strategies of repression to deter challenges, prevent coordinated protests or other violent civilian or insurgent attacks on government officials or agents, or minimize the amount of information shared on the ways in which government has repressed civilians from making public demands of the state. In such cases, these strategies to minimize challenges should signal that governments intuit that their perceived legitimacy of being having the monopoly of violence is diminishing in the eyes of the population. Under such circumstances, pairing the already deteriorating perceptions and satisfaction of the public with information and ally-ship bolstered by TANs would likely further heighten government fears of losing power. Further, in the face of

international involvement via shaming and information sharing with domestic actors, these fears on behalf of the government could further push elites in considering that punitive measures may be able to be taken against them. Therefore, engaging in internet shutdowns, which hinders the flow of critical information on the conditions of violent repression on the ground in the face of widespread dissent should lead the government to prefer to use shutdowns to weaken dissent efforts.

This should be the case particularly when a state is faced with an environment of a robust, independent civil society but constrained financially to directly target vast networks of CSOs. In cases where a government is resource-strapped with a thriving civil society, governments are further constrained on policy options by weakened state capacity in the face of dissent and accountability. State capacity, defined here as the government's ability or willingness to carry out policy and govern (Englehart, 2009), would limit a regime's ability to have its agents effectively carry out orders that may directly target CSOs when weakened. If a government cannot afford to compensate its agents to carry out policies of repression or other human rights abuses, then the government runs the risk of agency loss. In this situation, internet shutdowns may prove to be a favorable option in these contexts as this policy response could more swiftly and instantaneously disrupt the information environment as to prevent civil society from sharing documented rights abuses going on at home to broader audiences, including other domestic, regional, and/or international audiences. Moreover, being financially constrained could limit government abilities to engage in other forms of digital repression given reduced state capacity. This leads to asserting the following:

Hypothesis 4: *When a robust civil society exists in a state with weak capacity, the state is more likely to engage in internet shutdowns and/or other telecommunication shutdowns.*

A final aspect to consider is that many governments have been targets of shaming campaigns previously. What does it mean for states that have previously been shamed for using internet shutdowns as a means to repress? While the theory anticipates that states that engage in widespread rights violations are more inclined to order in internet shutdowns, it can be argued that states that have been previous targets of shaming campaigns by TANs have learned from prior experience that internet shutdowns are an effective means to weaken these networks. Because these states have experience with how TANs work in conjunction with domestic and regional NGOs to coordinate placing pressure on regimes to change their behavior through shaming and persuasion, which relies heavily on the transmission of information among actors both at the domestic and international actors, states who have been targets of shaming previously would want to shut off informational flows to the best of their abilities, avoiding the spotlight of another human rights shaming campaign and their subsequent consequences.

Hypothesis 5: *When a government has previously engaged in strategies of shutting down the internet and/or telecommunication services, they are more likely to do so again.*

Methodology

Model Selection

The data used in this study covers all countries for the years 2016-2022. The unit of analysis is the country-month. To test the arguments presented in the substantive portion of this paper, the article uses series of negative binomial count models given that the dependent variable, internet shutdowns and telecoms disruptions, are measured as a count of each event. The study relies on data sourced from the Varieties of Democracy (Coppedge et al., 2024a), Access Now's Shutdown Tracker

Optimization Project (STOP) (Rossen & Anthonio, 2024) and the Integrated Crisis Early Warning System Events Data (ICEWS) (Boschee et al., 2014).

Dependent Variable

This study utilizes one key dependent variable across all hypotheses being tested, internet shutdowns and telecommunication disruptions. These data come from Access Now's #KeeptItOn Internet Shutdown Tracker Project. While some years of the data do contain duration of shutdowns, not all years do. As such, this project will utilize counts of internet shutdowns and service stoppages as counts of these events are included consistently within the dataset. In these data, shutdown events are defined as ``an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information." (Access Now 2021). Further, they elaborate that instances are considered ongoing even when internet or other telecommunications services are restored but quickly disrupted again, varied services are targeted, and/or the scope of the event changes throughout the episode.

Independent Variables

This analysis relies on several key independent variables: internal dissent, TAN shaming events, civil society robustness, state capacity, and prior use of internet shutdown. Hypotheses 1-3, employ measures to capture the extent of domestic dissent and TAN shaming. The extent of domestic dissent is measured using V-Dem's mass mobilization indicator. This measure captures the size and frequency of various types of dissent events: demonstrations, strikes, sit-ins, etc. Further, this measure specifically captures that these events are explicitly coordinated by non-state actors but can theoretically capture state-sanctioned rallies that may support an existing (autocratic) government

(Coppedge et al., 2024). This is an interval measure, ranging from -3.44 to 3.99 where lower values indicate less attended, infrequent mobilization levels and higher values more frequent and/or larger events of mass mobilization. For the shaming measure, the project relies on daily information from the Integrated Crisis Early Warning Systems (ICEWS) dataset to develop a different indicator for shaming than those traditionally used and aggregates to the country-month level. ICEWS events data uses CAMEO (Conflict and Mediation Event Observation) code book guidelines, primarily drawing from CAMEO's Verb codebook to define the types of interactions between socio-political actors (e.g., government or military officials, HROs, IOs, etc.) (Boschee et al., 2015). Using these CAMEO codes/verbs to form the basis of the shaming variable, the variable is first constructed as a dichotomous variable, *shame*, where an observation received a one if the verb used to describe the interaction could be perceived as shaming. For example, observations that received a 1 often included the CAMEO verb codes for "Make an appeal or request" (20), "Appeal for political reform" (24), "Appeal for humanitarian aid" (0233), or "Demand settling of dispute" (107). More generally, CAMEO codes indicated an event where the action could be perceived as a form of shaming. Some of these shaming actions included appealing for political reforms, yielding to ease administrative sanctions, demanding political reform, criticizing or denouncing, or rally opposition against.[5] Next, another variable called *TAN_shame* was created to capture the source of the shaming (i.e., the group or individual who shamed the target actor). This is also a dichotomous variable. Using the "source sector" variable within the ICEWS data, which describes the type of actor as the source of an interaction (e.g., Intergovernmental Organization [IO]), a value of one is assigned when the source actor included any entity that could perceivably be involved the transnational advocacy network. This included coding sources that included phrases such as "NGOs", "Human Rights", "Nongovernmental Organization (International)", etc. The next step focused on the target of the shaming event. Another

[5] Several other codes were included, which are all included in the replication materials.

binary indicator, *target*, was generate and assigned a value of one if the target of the shaming was either a government, military, or police. The final variable, *shame_event*, received a one when the conditions of *shame*, *TAN_shame*, and *target* were each met.[6] This measure, therefore, includes all events where TAN organizations shamed governments and/or its agents. The *shame_event* variable was then used to generate the variables for the six-month and 12-month moving average of shaming. These moving averages are used to test for hypothesis: whether a state that has previously been shamed is more likely to shut down the internet again when facing another TAN shaming episode.

To test the hypothesis related state capacity and a robust civil society, two additional indicators are used. For state capacity, the variable used here is an index loosely based on Englehart's (2009) conceptualization. Englehart argued that three key elements comprise state capacity: law and order, state corruption, state sources of revenue. To operationalize these, law and order is measured using V-Dem's rule of law index, which captures the extent to which "laws transparently, independently, predictably, impartially, and equally enforced, and to what extent do the actions of government officials comply with the law" (Coppedge et al., 2024). Lower measures indicate lower rates of law and order. Corruption is measured by V-dem's Political Corruption Index. This measure captures how widespread political corruption is in a given state, which covers six key areas that include all branches of government, including both elites at each level as well as lower levels of the public sector. This is an interval measure, where lower levels reflect higher levels of corruptions and higher values capture lower levels of corruption.[7] The final component to this index is state fiscal source of revenue. Englehart argues that tax extraction is a crucial indicator of states' abilities to effectively govern and carry out policies given that tax revenues often fund crucial state actions, such as development and maintenance of infrastructure, provision of public goods, compensation of state agents, and much

[6] I.e., when *shame, shame, TAN_shame,* and *target* all are all coded as ones within the same observation
[7] The original data has this scale reversed. I opted to reverse the scale to substantively keep all measures operating in the same direction.

more (Englehart, 2009). As such, this ordinal measure includes information on the sources of revenue that a central government primarily relies upon to finance state action, including taxes (Coppedge et al., 2024). These three measures were loaded into a factor model and are being used as a single state capacity index, where lower values indicate lower levels of state capacity and higher values indicate higher state capacity. Finally, the data for civil society activity comes from V-Dem's civil society participation index. This measure is intended to capture whether a state has a robust civil society, particularly in terms of being free from influence from the state (either threatened or coerced). This is an interval measure, ranging 0-1, where low levels of civil participation are reflected by values closer to 0 (ibid).

Controls

Several covariates are included in this analysis. Using the UCPD Armed Conflict Data, I include a count of each domestic or international conflict in which a government is a participant (Gleditsch et al., 2022; Pettersson & Öberg, 2020), which is increasingly relevant for digital repression and internet shutdowns. A key component to the argument implies that individuals must have access to the internet and other forms of mass/rapid communications. While all states do have access, this access and level of infrastructure required widely varies. For this reason, the study includes the World Bank's measure for internet users (percentage of population) ("Percentage of Individuals Using the Internet", 2021). Also, from the WBI data, I include variables for GDP per capita (logged), population (logged), and trade (as a percentage of GDP) to account for trade openness ("Gross Domestic Product", 2021; "Total Population", 2021; "Trade (% of GDP)", 2021). Due to conceptual overlap between human rights and democracy (Hill, 2016), I use V-Dem's higher court independence measure, an interval value that measures the frequency of whether high court rulings reflect a government's will (Coppedge et al., 2024). Finally, elections likely can impact digital repression in some contexts. As

such, I include a binary variable, where 1 indicates an election year. These data come from the Voter Turnout Database by International IDEA (IDEA, 2024).

Results and Discussion

Table 2.1: Summary Statistics for Variables used Negative Binomial Count Models

Variable	N	Mean	Min	Max
Mass Mobilization	14942	.164	-3.441	3.999
Shutdown Counts	15009	.246	0	32
Shaming Events	15009	2.581	0	101
CSO Participation	15009	.663	.025	.988
6 Month Moving Avg	15009	2.651	0	81.333
12 Month Moving Avg	15009	2.751	0	71.538
Judicial Independence	15009	.35	-3.446	3.453
State Censorship	15009	.263	-3.611	2.661
Conflict	15009	.116	0	1
Election	15105	.129	0	1
Internet Users (% of Total Population)	12923	57.015	1.084	100
Population (Logged)	14921	16.196	11.445	21.072
GDP (Logged)	14506	24.825	19.376	30.879

Table 2.2 below includes the results of each of the negative binomial count models. Rather than publishing the model coefficients, the table reflects the incident rate ratios to provide more direct interpretation. This approach allows for the results of the model to be analyzed through discussing how each exponentiated beta coefficient ($\hat{\beta}_k$) experiences a factor change by which the expected number of events (λ) either increases or decreases by a one unit change in the independent variables. Because incident rate ratios are interpreted in terms factor increases or decreases of expected number of events, substantive interpretations based on these values are much easier to discuss compared to the raw coefficients originally generated by the model.

Hypotheses 1-3 focus on the relationships between mass mobilization and internet shutdowns, TAN shaming campaigns and internet shutdowns, and the potential interactive effect of

Table 2.2: Incident Rate Ratios and Standard Errors for Models 1-7

	(1)	(2)	(3)	(4)	(5)	(6)	(7)
Mass mobilization	1.316***		1.259***				1.387***
	(0.035)		(0.036)				(0.043)
Shaming Events		1.017***	0.998				0.978*
		(0.004)	(0.006)				(0.009)
Mobilized Dissent * Shaming			1.014**				1.020***
			(0.005)				(0.005)
Civil Society Participation	0.084***	0.289***	0.099***	0.071***	0.299***	0.302***	0.012***
	(0.019)	(0.059)	(0.023)	(0.016)	(0.061)	(0.062)	(0.003)
State Capacity				3.459***			8.356***
				(0.465)			(1.274)
State Capacity * Civil Society Participation				0.054***			0.022***
				(0.010)			(0.005)
Six Month Moving Average of Shaming					1.020***		1.020*
					(0.004)		(0.009)
Twelve Month Moving of Shaming						1.020	
						(0.004)	
Judicial independence	0.819***	0.727***	0.796***	0.934	0.723***	0.721***	0.926
	(0.032)	(0.029)	(0.032)	(0.038)	(0.029)	(0.029)	(0.039)
Conflict	0.696***	0.896	0.738***	0.922	0.906	0.908	0.889
	(0.063)	(0.080)	(0.068)	(0.084)	(0.081)	(0.081)	(0.081)
Election	1.513***	1.511***	1.548***	1.618***	1.521***	1.527***	1.823***
	(0.134)	(0.133)	(0.136)	(0.141)	(0.134)	(0.134)	(0.158)
Internet Users	1.012***	1.014***	1.013***	1.016***	1.014***	1.014***	1.015***
	(0.003)	(0.003)	(0.003)	(0.003)	(0.003)	(0.003)	(0.003)
Population Logged	2.528***	2.665***	2.455***	2.548***	2.628***	2.615***	2.317***
	(0.161)	(0.169)	(0.158)	(0.172)	(0.167)	(0.166)	(0.163)
GDP Logged	0.718***	0.669***	0.710***	0.742***	0.670***	0.672***	0.743***
	(0.042)	(0.038)	(0.041)	(0.046)	(0.038)	(0.038)	(0.046)
Observations	12702	12759	12702	12759	12759	12579	12702
Log Likelihood	-5349.15	-5349.07	-5337.78	-5232.61	-5392.478	-5391.95	-5116.05
AIC	10718.29	10808.13	10699.56	10487.22	10804.96	10803.90	10262.10
BIC	10792.79	10882.67	10788.96	10569.22	10879.50	10878.44	10373.84

**** p<.001, ** p<0.01, *p<0.05*

both mass mobilization and TAN shaming on internet shutdowns, respectively. In terms of internal dissent, this study relied primarily on the V-Dem measure of mass mobilization, which captures both the size and frequency of various forms of mobilization to challenge the state and the status quo. Crucially, this variable focuses on mobilization events, such as protests, demonstrations, sit-ins, etc. that are organized by non-state actors. Model 1 demonstrates that there is a positive, statistically significant relationship between the mass mobilization measure and internet shutdowns: cetaris paribus, for each additional unit increase of mobilization (i.e., domestic dissent), this leads to a 32% estimated increase (i.e., IRR of 1.316) in the expected rate of internet shutdowns and/or telecommunications shutdown episodes.

To demonstrate the effect and magnitude of this relationship, Figure 2.1 below shows the predicted number of internet shutdown events across all levels of mass mobilization.

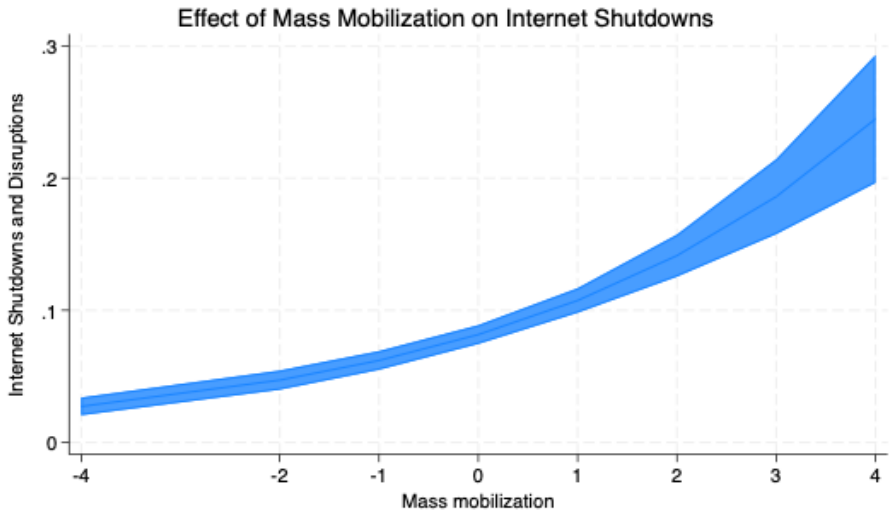

Figure 2.1: Effect of mass mobilization on internet shutdowns/telecoms disruptions

Regarding the control variables, most of them perform in the anticipated directions. As judicial independence improves, courts are able to better restrain state executives from engaging in

disruption events. Interestingly, the relationship between conflict and internet shutdown events is negative. This could be a result of conflict unfolding in areas where internet shutdowns and other telecoms disruptions have already been utilized as state responses to ongoing dissent rather than utilizing them at the conflict's onset. In years where elections occur, there is a greater probability that digital disruptions are used by the state. This result substantiates many cases that incorporate digital shutdowns and disruptions during periods of elections. Some examples include the 2018 national election in the Democratic Republic of Congo (Netblocks, 2018), the 2024 election in Mozambique (Access Now, 2024a, 2024b, 20204c), the 2023 election in Gabon (Netblocks, 2023), and Belarus in 2020 (Open Observatory of Network Interference, 2020). Internet users and population were also statistically significant and had positive relationships with internet shutdowns. This evidence reaffirms that states with larger populations are likely to be repressed (Davenport 2007), and it also may extend to large digital populations as well.

Hypothesis 2, which tests the relationship between shaming campaigns and internet shutdowns is arguably at the core of the substantive argument above: effective shaming campaigns rely on accumulating information from sources on the ground in areas dealing with state violence, which is often transmitted most efficiently via the internet and other telecommunications services. Based on the results presented in Table 2.2, the study has also found that this relationship demonstrates statistical significance. For each additional unit increase of a state being targeted with shaming, there is a 1% (i.e., IRR of 1.017) increase in the expectation that a state will engage in

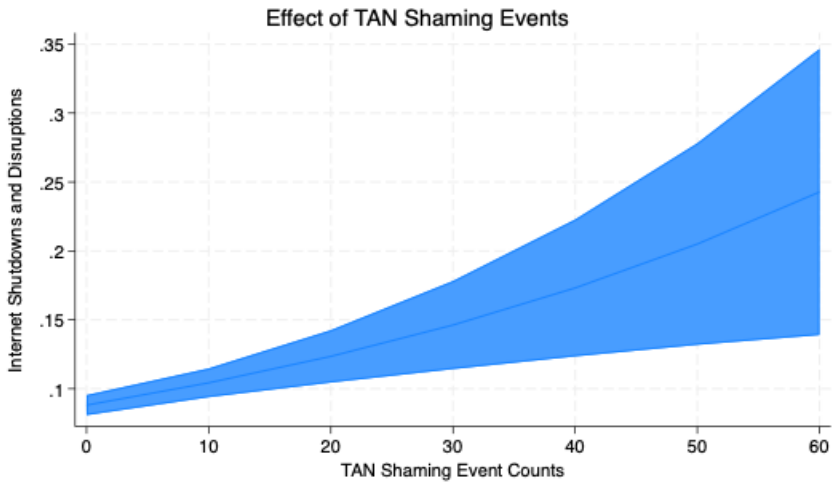

Figure 2.2: Effect of TAN shaming on internet shutdowns/telecoms disruptions

another episode of shutdown or disruption, holding all else equal. The effect is demonstrated in Figure 2.2. There are a couple of important items to note with the inference of the internet shutdown measure. First, the measure is not restricted to only nationwide internet shutdowns. This measure includes regional and local shutdowns as well as other forms of service throttling, such as restricting access to social media, SMS services, and VPNs. As such, it's imperative to not substantively interpret these results as shaming has a strong relationship with internet shutdowns, but rather that shaming campaigns lead to target states engaging in various forms of internet or internet-related service shutdowns. There are various mitigating factors, some of which are included in the model (e.g., judicial independence as a stand-in for regime type, substitution/complementary nature of repression, etc.), however there are likely other factors outside the scope of this paper that temper a government's ability to engage in a full network, nationwide shutdown. Given the results, hypotheses one and two are supported. Regarding hypothesis one, as mobilization – or protests, demonstrations, strikes, etc. increase in frequency and in size, we can anticipate a greater probability that the state will shut down the internet and other telecommunications services. Further, the

evidence suggests support for hypothesis two, where the same outcome should be observed as instances of shaming against a human rights abusing state occur. As governments are targeted with increased TAN shaming efforts, governments are more likely to engage in internet shutdowns, other forms of filtering, or blocking of various online services. Both mass mobilization and shaming events both have an independent and positive relationship with a government's propensity to shut down the internet. Hypothesis 3 seeks to test whether there may be some interactive affect between mass mobilization and TAN shaming regarding outcomes of shutdown and disruption events. When infrequent, sparsely attended mobilization events occur with little international attention drawn to government abuses, there is still a somewhat significant impact on the rate of internet shutdowns. Figure 2.3 demonstrates that there is a period where a rise in mass mobilization interacts with heightened shaming efforts to produce a greater likelihood that states will respond with internet shutdowns and other associated actions, but as these two dynamics continue to increase, the effect

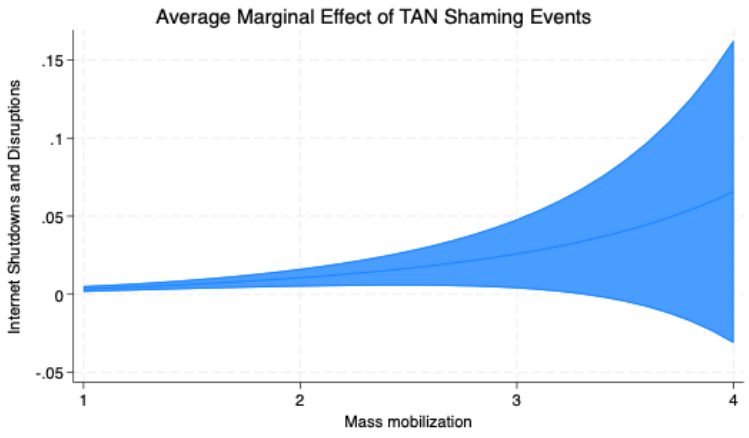

Figure 2.3 Average marginal effect of mass mobilization across levels of TAN shaming

washes away. This likely demonstrates that in cases where groups are beginning to mobilize a government and outside audiences have yet to catch on, some governments may be more inclined to

swiftly respond with shutdowns, possibly to snuff out any form of dissent to deter rebellion from growing. However, once mobilization hits a certain threshold and TAN shaming campaigns have begun to coerce offending regimes into stopping human rights abuses, governments are more likely to react to stave off other international responses that threaten leadership, whether through sanctions (blanket or targeted), reputational costs, loss of aid or other acts that can weaken leaders' abilities to maintain their grip on power. As such, hypothesis three is supported.

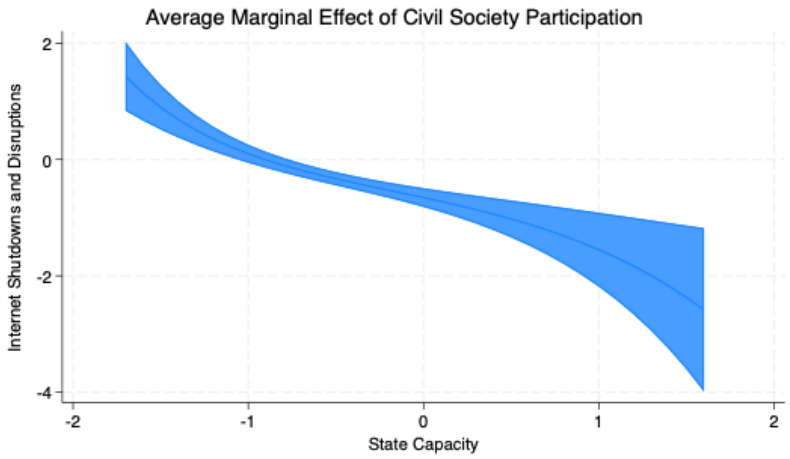

Figure 2.4 Average marginal effect of civil society participation across levels of state capacity

Given how pivotal civil society is in facilitating the transmission of information to broader audiences and potential TAN shaming, hypothesis four set out to explore another facet of civil societies and shaming. Here, the argument contends that states with a robust civil society and lower state capacity should witness a higher degree of internet shutdowns. Governments with lower degrees of state capacity (i.e., the ability and willingness to govern), may not be able to send out agents to coerce civil society members efficiently, and as such, may seek to rely on alternative means to disrupt the work of civil society. Model 4, which tests this proposition, finds statistical significance to suggest that this may be the case. Figure 2.4 above offers some insight into this

relationship. When civil society is active and able to carry out its work, but the government does have the capacity to effectively govern or engage in meaningful policy work, there is a greater probability that these governments will response to mass mobilization with internet shutdowns or other forms of reduced connectivity, such as blocking social media or other digital services. However, as states are increasingly able to carry out their capabilities to govern, state reliance on internet shutdowns as a policy option diminishes when faced with a weakened civil society environment. Given these results, hypothesis four is supported.

The final relationship to discuss with the first series of hypotheses is that which involves previous shaming, which may point to some type of learned behavior or adaptation mechanism of the target state. Hypothesis 5 asserts that states that have been previously shamed are more likely to engage in internet shutdowns when shamed again. To capture this relationship, this study opted to use two moving averages of shaming variables - one using a six-month moving average and another using a 12-month average. This allowed for the analysis to push further by incorporating an element of the intensity of previous shaming, as this could also have a bearing on the impact of previous shaming (i.e., it is not only that a state has previously been shamed, but it's also how much/how often a state has previously been shamed). Models 5 and 6 both capture this with incorporating moving averages of six months and 12 months, respectively. Due to the similar estimates produced across the models, the analysis and discussion will primarily focus on Model 5, or the six-month moving average model. Figure 2.5 portrays this relationship.

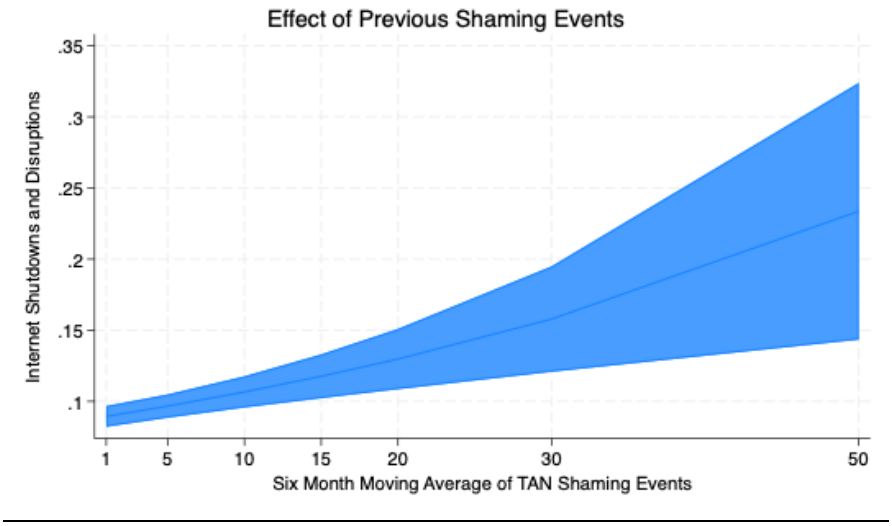

Figure 2.5: Effect of previous shaming

Based on the IRRs, the results indicate both a positive and statistically significant relationship. For each additional unit increase (i.e., each additional case of shaming within a six-month period), it is estimated that a target state is 2\% more likely to engage in an internet shutdown episode (i.e., IRR = 1.020), holding all else equal.

While the interpretation seems straightforward, some discussion on substantive interpretation is warranted. Again, there are mitigating factors that would inhibit states from engaging in shutdowns that warrant further investigation. Some states simply are less likely to engage in reduced connectivity behavior, be it institutional constraints or economic connectedness. In cases like the United States or other Western states where internet shutdowns are less likely for reasons of position in the global economy or liberal democratic institutions, additional instances of shaming likely would not result in increased chances of internet shutdowns. While this strategy to limit the flow of information is still very much on the table for regimes across the world - particularly autocratic regimes - there are other, more discreet avenues that governments can and do take when it comes to digital repression. Further, while engaging in reduced connectivity practices, such as

ordering internet shutdowns or other social media and telecoms disruptions, shutting off the internet inherently impacts those in the regime as well. This may function as a double-edge sword in the sense that given the circumstances that may lead to a shutdown - such as a coup or election violence - shutting down the internet can result in leaders and inner circles taking on their own risks of reduced communication capacities. While this tends to be the case in situations of nationwide shutdowns, using more targeted forms of internet shutdowns, which is common in India (Access Now, 2024), likely reduces these risks. Finally, Model 7 includes all variables from the previous models, and the results are largely consistent with the previous six models. Most interestingly, the effect of an independent judiciary mirrors the results of Hypothesis 4, which tested the interactive relationship between state capacity and civil society on internet shutdowns and other telecoms disruptions. This could be a function of evaluating shutdowns differently to see if state owned telecoms companies versus privately owned companies are the driving mechanisms behind this result. More work needs to be conducted on this specific relationship to understand why state capacity may outweigh the ability of courts to constrain this type of repression.

Discussion

The results from this study largely support the theoretical claims asserted. The results of this study provide evidence to suggest that mass mobilization events (i.e., those that are frequent and have large numbers of individuals in attendance), a robust civil society, and state capacity are key driving factors for state decisions to utilize internet shutdowns in the face of domestic threats. Moreover, there was evidence to support the claim that shaming does have an impact on these decisions as well. As framed in the theoretical arguments, threat is likely a predominate driver of these outcomes. Even though shaming campaigns on target countries often lead to many undesirable consequences that would make regime tenure more untenable (e.g., economic sanctions,

loss of aid, reduced access to international credit, reputational costs, etc.), governments clearly have more direct and swift options to stop these campaigns in their tracks. If abusive governments can go directly to the source and stop the flow of information before a shaming campaign can come to fruition, then these threats can be effectively neutered before there's a chance to make the international community aware of much wrongdoing. This means that governments are much more incentivized to target civil society organizations more directly, and when they do not have the capacity to do so, then internet shutdowns can do achieve what the state and its agents cannot. As evidenced by this study, there is reason to believe that the viability of large mobilization events against the state pose a significant threat, and often these events are at least partially coordinated alongside some sector of civil society. These types of events often garner international attention, which as stated repeatedly, lead to consequences that are unfavorable to regime members and their ability to maintain positions of power within the government. These findings are in line with much of the literatures related to the closing of civil society space and repression more broadly.

One other critical takeaway from these results points to the role of state capacity in the contexts of digital repression. In this study, the results suggest that states are more likely to shut down the internet in the face of conditions where the state experiences lower capacity alongside robust civil society and subsequent mass mobilization, which again is often facilitated through an active CSO environment. Substantively, this points to the idea that when regimes experience higher degrees of state capacity, they have other options available for engaging in strategies of digital repression. How does leadership decide which campaigns of digital repression it will choose? As discussed in the theoretical arguments section, there remains a preference for governments to reduce threats, and employing internet shutdowns may only be a viable option for cash or resource strapped countries, yet there are some examples of states with marginal levels of capacity that utilize internet shutdowns in a more targeted fashion. In these circumstances, it may be probable that greater levels

of state capacity will permit governments to utilize other options, especially given the extreme nature of internet shutdowns. Employing an internet shutdown, especially when nationwide, should be viewed as one of the direst options a state can select, as shutting off the internet and other telecommunication services for an entire country leads to significance economic downturn, disruption of healthcare and educational services, and broader violations of human rights obligations more broadly. Also, there are other reasons to investigate the role of state capacity on internet shutdowns and digital repression more broadly. Models 4 and 7 demonstrated that state capacity may wash out the impact of independent judiciaries, but why? In what other ways might state capacity influence internet shutdowns, disruption events, and digital repression more broadly?

Conclusion

This article empirically tested the theoretical arguments underpinning on how mass mobilization, shaming, civil society, state capacity, and prior shaming impact state decisions to engage in internet shutdowns and other telecommunication disruptions. The primary arguments contended that mass mobilization events, transnational actor network shaming, robust civil societies existing in low-capacity states, and previous decisions to shut down the internet should all lead to greater likelihoods that a government will opt to shut down the internet. Governments choose this strategy as these environments are indicative of major threats, either real or perceived, to a given regime. While internet shutdowns are increasingly seen as being a more extreme policy option in the face of dissent and other challenges to the status quo, these tactics are utilized in situations of threat to a government. Governments' preferences are to avoid any threats - reputational, financial, or others that could lead to a reduction or total loss of power.

This area of the literature - digital repression - is a burgeoning one. As the world continues to increasingly rely on and integrate technology into our everyday lives, it is imperative to understand

how these forms of tech may or may not be used against citizens for means of repression. Whether through use of surveilling social media, limiting streaming services, shutting off entire internet to parts of a country or nationwide, or targeting specific CSOs online, there is an urgent need to develop a framework to understand the state's decision calculus in terms of engaging in technologically based repression. By understanding the circumstances that lead to extreme options such as internet shutdowns by autocrats, international legal frameworks and domestic policy can catch up in ways to regulate these abuses of power. Moreover, by addressing this gap in tech policy - one of countless gaps that persist - individuals living in these contexts are less at risk for being able to engage in everyday life when internet shutdowns occur. The risks from internet shutdowns are far reaching - education, business, healthcare, and countless other sectors are negatively impacted when shutdowns occur. Future work in this area should continue to evaluate the roles that malicious uses of tech have on all facets of society as well as working to build a cohesive framework to understand the autocratic tech responses. Finally, greater attention is needed to comprehend the ways in which civil society is weakened because of repressive tech practices.

References

Access Now. 2021. "Methodology: March 2021 updates." Access Now. https://www.accessnow.org/cms/assets/uploads/2021/03/KeepItOn-report-on-the 2020data Mar-2021 3.pdf (accessed May 5, 2020).

Access Now. (2024). "#Keeptiton." *Access Now* https://www.accessnow.org/campaign/keepiton/ (accessed August 12, 2024).

Access Now. (2024a). "2024 elections and internet shutdowns watch." *Access Now*. URL: https://www.accessnow.org/campaign/2024-elections-and-internet-shutdowns-watch/#Mozambique

Access Now. (2024b). "Africa in 2023: Internet shutdowns attack democracy." *Access Now*. https://www.accessnow.org/press-release/africa-keepiton-internet-shutdowns-2023-en/

Access Now. (2024c). "Authorities and internet service providers in Mozambique must respect human rights and #Keepiton during protests." *Access Now*. URL: https://www.accessnow.org/press-release/keepiton-mozambique-authorities-must-respect-human-rights/

Albert, Elanor., and Lindsay Maizland. (2020). "The Rohingya crisis." *Council on Foreign Relations*. https://www.cfr.org/backgrounder/rohingya-crisis - main-content (accessed April 6, 2021)

Amnesty International. (2023). "Saudi Arabia: Alarming crackdown on online expression." *Amnesty International*. February 14, 2023. https://www.amnesty.org/en/latest/news/2023/02/saudi-arabia-alarming-crackdown-on-online-expression/ (accessed July 2, 2024).

Amnesty International. (2024). The state of the world's human rights: April 2024. *Amnesty International*. https://www.amnesty.org/en/documents/pol10/7200/2024/en/ (accessed July 2, 2024).

Bagwell, Stephen, and Shelby Hall. 2020. "Publicity and perceptions of risk: The effects of HRO naming and shaming on sovereign credit rating. *Journal of Human Rights* 19 (3): 379–391.

Bakke, Kristen. M., Neil J. Mitchell, and Hannah M. Smidt. 2020. "When states crack down on human rights defenders." *International Studies Quarterly* 64 (1): 85–96.

Barry, Colin M., K. Chad Clay, and Michael M. Flynn. 2013. "Avoiding the spotlight: Human rights shaming and foreign direct investment. International Studies Quarterly, 57, 532–544.

BBC. (2014). "Edward Snowden: Leaks that exposed US spy programme" *BBC*. URL: https://www.bbc.com/news/world-us-canada-23123964

Bell, Sam, K. Chad Clay, and Amanda Murdie. 2012. "Join the chorus, avoid the spotlight: The effect of neighborhood and social dynamics on human rights organization shaming." *Journal of Conflict Resolution* 63 (1): 167–193.

Boschee, Elizabeth, Jennifer Lautenschlager, Sean O'Brien, Steve Shellman, James Starz, and Michael Ward. 2015a. ICEWS Coded Event Data. https://doi.org/10.7910/DVN/28075 (accessed June 10, 2019).

Boschee, Elizabeth, Jennifer Lautenschlager, Sean O'Brien, Steve Shellman, James Starz, and Michael Ward. 2015b. "Icews coded event data read me.pdf." Harvard Dataverse. https://doi.org/10.7910/DVN/28075/1GGS5G

Bruce Bimber, Andrew J Flannigan, and Cynthia Stohl. 2005. "Reconceptualizing collective action in the contemporary media environment." *Communication Theory*, 15 (4): 365–388.

Brysk, Alison. 1993. "Turning weakness into strength: The internationalization of Indian rights." *Latin American Perspectives* 23 (2): 38–57.

Chen, Zhuo, Poong Oh, and Anfan Chen. 2021. "The role of online media in mobilizing large-scale collective action." *Social Media + Society* 7 (3).

Coppedge, Michael, John Gerring, Carl Henrik Knutsen, Staffan I. Lindberg, Jan Teorell, David Altman, Fabio Angiolillo, Michael Bernhard, Cecilia Borella, Agnes Cornell, M. Steven Fish, Linnea Fox, Lisa Gastaldi, Haakon Gjerløw, Adam Glynn, Ana Good God, Sandra Grahn, Allen Hicken, Katrin Kinzelbach, Kyle L. Marquardt, Kelly McMann, Valeriya Mechkova, Anja Neundorf, Pamela Paxton, Daniel Pemstein, Oskar Rydén, Johannes von Römer, Brigitte Seim, Rachel Sigman, Svend-Erik Skaaning, Jeffrey Staton, Aksel Sundström, Eitan Tzelgov, Luca Uberti, Yi-ting Wang, Tore Wig, and Daniel Ziblatt. 2024. "V-Dem Codebook v14" Varieties of Democracy (V-Dem) Project.

Council of the European Union. 2024. "Timeline - EU sanctions against Myanmar." *Council of the European Union*. https://www.consilium.europa.eu/en/policies/sanctions- against-myanmar/timeline-sanctions-against-myanmar/ (accessed June 17, 2024)

Danneman, Nathan and Emily Hencken Ritter. 2014. "Contagious rebellion and preemptive repression. *The Journal of Conflict Resolution* 58 (2): 254–279.

Davenport, Christian. 2007. "State repression and political order." *Annual Review of Political Science* 10 (1): 1–23.

Dragu, Tiberiu and Yonatan Lupu. 2021. "Digital authoritarianism and the future of human rights." *International Organizations* 75 (4): 991–1017.

Earl, Jennifer, Thomas V. Maher, and Jennifer Pan. 2022. "The digital repression of social movements, protest, and activism: A synthetic review." *Science Advances* 8 (10).

Englehart, Neil. J. 2009. "State capacity, state failure, and human rights." *Journal of Peace Research* 46 (2): 163–180.

Enikolopov, Ruben, Maria Petrova, and Konstantin Sonin. 2018. "Social media and corruption." *American Economic Journal: Applied Economics* 10 (1): 150–174.

Feldstein, Stephen. 2021. *The rise of digital repression: How technology is reshaping power, politics, and resistance.* New York, New York: Oxford University Press.

Gleditsch, Nils Petter, Peter Wallensteen, Mikael Eriksson, Margareta Sollenberg, Håvard Strand. 2002. "Armed conflict 1946-2001: A new dataset." *Journal of Peace Research* 39 (5): 615–637.

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

Gohdes, Anita. 2024. *Repression in the digital age: Surveillance, censorship, and the dynamics of state violence.* New York: Oxford University Press.

Gross domestic product. 2021. *World Bank.* http://data.worldbank.org/indicator/NY.GDP.MKTP.CD (accessed June 20, 2019).

Hill, Daniel. W. 2016. "Democracy and the concept of personal integrity rights." *Journal of Politics* 108 (3), 822–835.

Howard, Phillip N. and Muzammil M. Hussain. 2013. *Democracy's fourth wave? digital media and the Arab spring.* New York: Oxford University Press.

Human Rights Measurement Initiative. 2024a. *Human Rights Measurement Initiative* Press release: Increased incidences of digital rights violations worldwide. https://humanrightsmeasurement.org/press-release-increased-incidences-of-digital-rights-violations-worldwide/ (accessed July 5, 2024).

Human Rights Measurement Initiative. 2024b. "Rights tracker: Saudi Arabia." https://rightstracker.org/country/SAU?tab=report-physint (accessed July 5, 2024).

Human Rights Watch. 2020. "Myanmar: End world's longest internet shutdown lift restrictions in embattled Rakhine, Chin states. *Human Rights Watch.* https://www.hrw.org/news/2020/06/19/myanmar-end-worlds-longest-internet-shutdown (accessed April 6, 2021).

Human Rights Watch. 2022. "Myanmar: No justice, no freedom for Rohingya 5 years on." *Human Rights Watch.* https://exhibitions.ushmm.org/burmas-path-to-genocide/timeline (accessed September18, 2024).

Human Rights Watch. 2024. "Human rights watch world repot 2024: Events of 2023." *Human Rights Watch*. https://www.hrw.org/sites/default/files/media2024/01/World%20Report%202024%20LOWRES%20WEBSPREADS 0.pdf (accessed July 1, 2024).

International IDEA, Voter Turnout Database. 2024. "Voter turnout database." *International IDEA*. https://www.idea.int/data-tools/data/voter-turnout (accessed July 6, 2024).

Jensen, Nathan. 2003. "Democratic governance and multinational corporations: Political regimes and inflows of foreign direct investment. International Organization" 57 (3): 587–616.

Kaire, J. 2024. "Get the word out: Monitoring human rights reduces abuse." *Journal of Peace Research,* 61(5), 808-824

Keck, Margaret E. and Kathryn Sikkink. 1998. "Transnational advocacy networks in international and regional politics." *International Social Science Journal* 51: 89–101.

Keck, Margaret E. and Kathryn Sikkink. 2014. Activists Beyond Borders: Advocacy Networks in International Politics. Ithica, NY: Cornell University Press.

Kendall-Taylor, Andrea and Erica Frantz. 2015. "Mimicking democracy to prolong autocracies." *The Washington Quarterly* 37 (4): 71–84.

KrASIA. 2021. "Myanmar: End world's longest internet shutdown in the Rakhine and Chin states" *KrASIA* https://kr- asia.com/myanmar- ends- worlds-longest-internet-shutdown-in-the-rakhine-and-chin-states (accessed April 6, 2021).

Krcmaric, Daniel. 2019. "Information, secrecy, and civilian targeting." *International Studies Quarterly* 63: 322–333.

Lebovic, James H and Erik Voeten. 2009. "The cost of shame: International organizations and foreign aid in the punishing of human rights violators." *Journal of Peace Research* 46 (1): 79–97.

Mason, T. David. 2008. *Caught in the crossfire: Revolution, repression, and the rational peasant.* Lanham: Rowman and Littlefield Publishers, Inc.

Murdie, Amanda. 2009. "The impact of human rights NGO activity on human rights practices." *International NGO Journal* 4 (10): 421–440.

Murdie, A., & Davis, D. R. (2012). Shaming and blaming: Using events data to assess the impact of human rights ingos. International Studies Quarterly, 56 (1), 1–16.

Murdie, Amanda and Dursen Peksen. 2012. "The impact of human rights ingo activities on economic sanctions." *The Review of International Organizations* 8: 33–53.

Myanmar Internet Project. (2025a). Internet shutdown by each region. https://www.myanmarinternet.info/digital-coup

Netblocks. (2018). Evidence of internet shutdowns in DRC amid election unrest. https://netblocks.org/reports/evidence-of-internet-shutdowns-in-drc-amid-election-unrest-PW80YLAK

Netblocks. (2023a). Internet cut in Gabon on election day. https://netblocks.org/reports/internet-cut-in-gabon-on-election-day-Q8oxM3An

Open Observatory of Network Interference. (2020a). Belarus protests: From internet outages to pervasive website censorship. https://ooni.org/post/2020-belarus-internet-outages-website-censorship/

Percentage of individuals using the internet. 2021. *World Bank*. http://data.worldbank.org/indicator/IT.NET.USER.ZS

Pettersson, Therese and Magnus Öberg. 2020. "Organized violence, 1989-2019." *Journal of Peace Research* 57 (24).

Pierskalla, Jan. H. and Florian M. Hollenbach. 2022. "Technology and collective action: The effect of cell phone coverage on political violence in Africa." *American Political Science Review*, 107 (2): 207–224.

Poe, Stephen. C. 2004. *Understanding human rights violations*. Randolph: Ashgate.

Ritter, Emily Hencken and Courtenay R. Conrad. 2016. "Preventing and responding to dissent: The observational challenges of explaining strategic repression." *American Political Science Review* 110 (1): 85–99.

Rød, Espen Geelmuyden and Weidmann, Nils. 2015. "Empowering activists or autocrats? The Internet in authoritarian regimes." *Journal of Peace Research* 52 (3): 338–351.

Rossen, Zach and Anthonio, Felicia. 2024. Shutdown tracker optimization project (STOP). *AccessNow* https://www.accessnow.org/guide/shutdown-tracker-optimization-project/ (accessed September 19, 2024).

Scruggs, Lyle, Shareen Hertel, Samuel J. Best and Christopher Jeffords. 2011. "Information, choice and political consumption: Human rights in the checkout lane." *Human Rights Quarterly* 33: 1092–1121.

Smidt, Hannah, Dominic Perera, Neil J. Mitchell, Kristin M. Bakke. (2016). "Silencing their critics: How government restrictions against civil society affect international 'naming and shaming'." *British Journal of Political Science* 51 (3): 1270–1291.

Spetalnick, Matt and David Brunnstrom. (2018). US. imposes sanctions on Myanmar military over Rohingya crackdown. *BBC* .URL: https://www.reuters.com/article/idUSKBN1L21KO/

Total population. 2021. *World Bank*. http://data.worldbank.org/indicator/sp.pop.totl

Trade (% of gdp). 2021. *World Bank*. https://data.worldbank.org/indicator/NE.TRD.GNFS.ZS

US Holocaust Memorial Musesum. (n.d.). "Burma's path to genocide: Timeline." *US Holocaust Memorial Museum* https://exhibitions.ushmm.org/burmas-path-to-genocide/timeline (accessed September 18, 2024).

Vadlamannati, Krishna Chaitanya, Nicole Janz, Øyvind Isachsen Berntsen. 2018. "Human Rights Shaming and FDI: Effects of the UN Human Rights Commission and Council." *World Development* 104: 222–237.

Varieties of Democracy. 2024. Democracy Report 2024: Democracy winning and losing at the ballot. *Varieties of Democracy* https://www.v-dem.net/documents/43/v-dem_dr2024_lowres.pdf

Weidmann, Nils. B. and Espen Geelmuyden Rød. 2019. *The internet and political protest in autocracies*. New York: Oxford University Press.

Xu, X. 2022. "To repress or to co-opt? authoritarian control in the age of digital surveillance." *American Journal of Political Science* 65 (2): 309–325.

Zeitzoff, Thomas. 2017. "How social media is changing conflict." *Journal of Conflict Resolution* 61 (9): 1970–1991.

CHAPTER 3:

UNDERSTANDING HOW GOVERNMENTS SELECT FROM COMPETING STYLES OF DIGITAL REPRESSION[8]

[8] LaVelle, Meridith. To be submitted to a peer review journal.

Abstract

How do political elites decide the role that technology will play to facilitate state repression? Governments across the world are increasingly relying on technology for various political purposes. Yet, the ways in which technology is incorporated into state responses to dissent, the choices governments have at their disposal range from censorship to surveillance as well as internet shutdowns. However, options such as internet shutdowns and surveillance may be at tension with one another. Moreover, officials may perceive one type of strategy as having greater utility over the other. This study explores the domestic conditions and policy goals that influence state decisions to engage in digital repression, namely through surveillance-based or reduced-connectivity approaches. Using two sets of seemingly unrelated regressions, there are mixed results.

Introduction

On October 6, 2024, Mozambicans went to the polls to vote in the country's general elections. The main Presidential candidates vying for the top position were Venâncio Mondlane, an independent candidate backed by the country's main opposition party, Partido Optimista pelo Desenvolvimento de Moçambique (PODEMOS), and Daniel Chapo of the Frente de Libertação de Moçambique (FRELIMO) party, which has ruled the country since independence over 50 years ago. Despite EU and local election observers claims that election irregularities occurred, on October 24, the Mozambican election commission announced that Chapo and his party won the election. Prior to this public announcement, Mozambican police engaged in violence against various opposition party members and supporters, including election observers and protesters, killing two. When election results were announced on October 24, PODEMOS members went online to call for citizens to protest the election results, claiming the election had been rigged. Protests swept the country for the next two months, where further violence erupted throughout the country. During this period of

electoral violence, it was reported that at least 11 Mondlane supporters had been killed, hundreds were injured, and over 400 people were detained (Access Now, 2024c; Lawal, 2024; Meng at al., 2025). Two of Mondlane's associates were shot and killed, while Mondlane himself was faced with police showing up on his doorstep the day the protest began. To disperse protesters, including journalists and human rights advocates, riot police crashed demonstrations shooting bullets into the crowds (Al Jazeera, 2024) By the end of 2024, at least 277 people were killed, and more than 600 had been injured (Amnesty International, 2024a). Protests have continued into 2025, where estimates of over 300 people have been killed through several peaceful protests since the October protests began (Meng et al., 2025).

Yet, the government also relied on other campaigns of state-sanctioned repression during this time. Short periods of internet shutdowns began as polls closed on October 11 (Access Now, 2024a). Soon after, multiple internet shutdowns coincided with the initial protests on October 24 with another government sanctioned internet black out occurred again on October 31. However, this isn't the first time that the FRELIMO party has resorted to this strategy. In 2023, Mozambique held local elections across the country, where the internet was cut off for several hours on election day, citing the government's first use of internet shutdowns (Access Now 2024b). According to Access Now, this seriously hampered citizens from being able to share critical information regarding voting and the election more generally (Access Now, 2024c). In both cases, the goal of resorting to internet shutdowns and other digital blackouts signaled the government's desire to reduce the ability of people to share information - whether on violent human rights abuses carried out by the state or on freely sharing information on elections, effectively preventing meaningful political participation.

Since the 1990s, the threads of Venezuela's democracy have gradually unraveled. Gamboa (2024) argues that this was done in multiple phases, ultimately setting the stage for Nicolás Maduro's contentious election of 2019 (Gamboa 2024), which received widespread international condemnation

(US Department of State, Bureau of Western Affairs, 2019). Leading up to the election, Maduro's government had worked to ensure that the election was not free and fair, in large part by restricting certain online services. For example, there were several instances where the main opposition candidate, Juan Guaidó, sought to address the Venezuelan public. Maduro's government would order the state-run telecoms provider, CANTV, to block media outlets, social media, and other streaming services including Periscope, Twitter, and YouTube to prevent Guaidó from being able to reach he public more broadly (CBC Radio, 2019; Netblocks, 2019b, 2019c, 2019d, 2019e). Further, the Maduro government also ordered similar service stoppages through national telecoms providers to block the state's legislature from broadcasting some of its live sessions (Netblocks 2019a, 2019f).

Throughout the Covid-19 pandemic, the Venezuelan government continued to clamp down on dissent and government critics, but in largely different capacities. The UNHCR estimated that as of May 2025, around 7.9 million Venezuelans have left the country, largely due to continued threats of state violence and sharp economic downturn (UNHCR, 2025). For those who remained, especially critics of Maduro's regime during and after the 2024 elections, Venezuelans are now experiencing new forms of digital repression beyond censorship: mass surveillance, both digitally and through citizen informant programs. In 2022, the Maduro government worked with a tech firm to create VenApp, an app that was alleged to be used for citizens to submit concerns and complaints regarding weak or ineffective public services and utilities. However, in the wake of the 2024 election, government rhetoric shifted surrounding the app, where Maduro encouraged his supporters to use VenApp to report protesters and other government critics (Amnesty International, 2024b).

The repressive component of this strategy is nothing new, but the digital ones are. ``Operation Tun Tun", the informal name for Venezuelan repression campaigns against opposition supporters since the mid 2010s, facilitated an environment of government intimidation and terror. By arresting, detaining, imprisoning, and often disappearing political opposition and dissidents in the early hours

of the morning, commonly without notice and no due-process, targets, numbering in the thousands, were victimized by Maduro's regime. In turn, this has fostered a culture of citizen informant networks on possible government critics, which has only made the transition to VenApp much more seamless (Sequera & Guanipa, 2024). Earlier policies codified in 2011 have also made it much easier for the government to demand communications and data from state telecommunications providers. For example, estimates of around 20% of Telefonica customers private communications were monitored and/or passed along to government officials at the state's request (Alarcón, 2024). Other key forms of digital repression, surveillance, and intimidation include the use of drones during protest events, online doxxing and harassment by government officials of critics, and the eventual goal of developing state databases used for the continued monitoring of those deemed enemies of the state (ibid).

These examples demonstrate that there is so no single form of digital repression that governments rely on. Rather, there are seemingly competing and complementary strategies that governments can utilize in contentious environments to respond to anticipated or actualized dissent alongside traditional forms of state repression. Further, governments often substitute one approach for another, especially if repression campaigns may become more successful on the side of the government in the face of trying to stifle dissent. How do governments decide on which types of digital repression to use in contentious environments? In some instances, governments may opt to shut down the internet or specific services, such as messaging apps, VPNs, streaming services, among others. On the other hand, some states clearly utilize surveillance-based campaigns. Yet, the latter approach may not be feasible given that when the internet is shut down, internet services typically required to digitally surveil individuals in the first place (Gohdes, 2023).

This article will begin by exploring two key strategies through which government decision making processes have been contextualized in the repression literature: substitution and complementarity. By using this framework to understand when and why governments may opt for

one of these competing strategies, we may be then able to understand how these types of digital repression translate to intensity of offline, violent state repression. This article contends that in the face of international constraints and incentive structures, governments are motivated to use what resources they have at their disposal to reduce the appearance of state violence against dissidents. Because of these incentive structures, political elites will likely incorporate technology into their responses to domestic dissent. Depending on the intensity and frequency of dissent activity, of which is likely calculated into perceived threat on the government's end, this should be a key factor that informs elites' decisions on digital repression strategies. When events organized by dissidents are more frequent and have greater attendance, which likely means that there is a prolonged dissent environment, this should lead governments to opting for surveillance-based strategies of digital repression. As a result, governments will rely on information gathered to engage in more targeted violence, reducing the overall appearance of physical integrity rights abuses. When dissent events (e.g., protests) are less frequent and have fewer attendees, governments are more likely to utilize reduced-connectivity approaches, such as internet shutdowns or blocking social media. In turn, this should lead to greater levels of human rights abuses as governments make it more difficult to share information on mass violence episodes. To test this argument, the study uses two seemingly unrelated regressions. Following a discussion of these results, the article will then conclude offering insights into future research and policy implications.

Background on Strategies of Substitution or Complementarity in Contentious Contexts

How do states choose among a variety of digital repression tactics to deploy against their populations in the face of collective dissent? To begin answering this question, this study integrates two strands of literature: theories of substitution and complementarity within the repression-dissent nexus literature and the emerging literature on the use of technology in state repression. When dissidents or

governments and their agents engage in substitution, this means that one of the groups of actors alter their behavior in anticipation of or in response to anticipated outcomes of the other group and do so to maximize their desired policy outcome. For example, a government may shift from non-violent forms of repression (e.g., censorship or banning assemblies) to violence, such as ordering state agents to show up to demonstrations to beat, detain, or kill participants. When actors use tactics to complement their ongoing strategies, this means that they add in additional responses alongside existing repression campaigns to maximize their desired policy outcomes.

For decades, scholars have analyzed both the behavior of governments and of dissident to explain the shifts in decisions making when responding to one another in contexts of contention. Given this strategic nature of repression and dissent (Ritter and Conrad, 2016), much attention has been dedicated to explaining why state or dissident behavior may change over time. Lichbach (1987) argues that on the side of dissidents, those who are challenging the government have the options of either engaging in violent or non-violent methods of protest. In some cases, dissidents may substitute violence for non-violence when non-violent behavior may increase the probably of a desired policy outcome. Moore (1998) tests this proposition, along with two other explanations for the shift in contentious behavior and finds evidence to support Lichbach's (1987) argument: dissidents will act in a way that will align more closely with their policy preferences but said costs may be constrained by regime responses as well as costs required to overcome collective action problems within the dissident movement. In particular, when dissidents are met with violent repression by state agents as a response to their challenging of the status quo (even if non-violent), they may then substitute violence as a strategies to respond to the government if this will help them to achieve their goals (Lichbach 1987; Moore 1998). This demonstrates that state responses of repression can influence the behavior of dissidents (ibid). On the side of the state, countless examples have been cited where governments have shifted from one type or set of repressive policies in favor of others. One common example of

substitution is the use of disappearance. In some cases, a previous government may have opted for the use of torture and arbitrary detainment, but a newer government substituted this set of rights violations with policies of enforced disappearances. Another general example of governmental substitution in contentious contexts involves the state delegating traditional forms of repression conducted by state agents to non-state paramilitary groups as a means to claim plausible deniability for abuses (Berman & Clark, 1982). Given the increased legalization of the human rights regime since the mid-20th century, international legal treaties, treaty bodies, and other modes of legal accountability structures have sought to reduce and eventually eliminate impunity of those state leaders who engage in violent human rights violations. As such, some have found that this, too, has raised the costs of engaging in violent human rights violations, such as extrajudicial killings, and resort to other types of rights violations that is more difficult to pin onto an offending government (Payne & Abouharb, 2016). However, Ritter (2014) argues that states won't necessarily respond with repression in each instance of contention. Rather, state leaders who enjoy a greater degree of job security will engage in lower rates of repression, but the severity of when governments do repress will increase (Ritter, 2013). This largely aligns with arguments that states will respond more harshly when their strength is perceived to be lower compared to those who are challenging the state's power (Poe, 2004).

The rise of naming and shaming has also been one of the key mechanisms that may explain why some governments alter their behavior to be more compliant with international human rights norms. Naming and shaming, the process where coalitions of domestic actors, NGOs, INGOs, and more call out attention to various human rights abuses being carried out by a specific government and its agents. This functions as an accountability mechanism through which the calling out behaviors and shaming violators brings about public awareness, which may lead to further negative sanctions via reputational costs (Murdie & Davis, 2012). However, these goals aren't always achieved. DeMeritt and Conrad (2019) have found that when states have been shamed for engaging in physical integrity rights

violations, this can often lead to states engaging in strategies of substitution. Rather than continuing to engage in violent human rights abuses, a shamed government may opt to engage in other non-violent human rights violations to reduce the optics of mass violence and subsequently appear in line with human rights norms.

Yet there is another critical component to consider with these various dynamics. Earl (2011) reviews that the standing of the repression literature at the time, covering topics such as conceptual debates, research that was recent at the time, and other key themes in the repression literature. Most crucially, she discusses overt versus covert repression. The former is traditionally what has been studied more by academics and often includes rights violations such as extrajudicial killings, disappearance, arrest, etc. Covert repression, on the other hand, is less viable to the public, and has received comparatively much less attention by scholars (Earl 2011).

Finally, when governments use additional strategies to complement existing policies of repression, this often for reasons of making ongoing campaigns of violence more efficient, targeted, or simply to keep tabs on civilians or political opposition deemed a threat to the continued survival of the state and its agents. Governments have increasingly been relying on digital tech for these purposes as well as to hide abuses and slow down the information about abuses from spreading. This is particularly the case with mass violence episodes (Krcmaric, 2019). For example, when information first started to spread internationally about the Rohingya genocide in Myanmar, especially over Facebook, the Burmese government responded with internet shutdowns in Chin and Rakhine states, the states where most Rohingya were forced to live. In turn, less information was released on specific abuses within the borders of Myanmar as the internet shutdowns persisted for years, but once more Rohingya were able to escape to neighboring Bangladesh, more information was shared on abuses conducted by the Burmese military, also known as the Tatmadaw.

Linking Substitution and Complementarity to Digital Repression and Human Rights Outcomes

By integrating the logics of substitution and complementarity, it is clearer how these dynamics influence human rights outcomes across two major digital repressive contexts: contentious political environments where the government and its agents rely on surveillance-based forms of repression and those that utilize internet and other telecommunications shutdowns. On the surface, a state's decision to switch from violent repression tactics to digital forms of repression could reduce some immediate costs, most importantly human lives. These costs may reduce as digital repression in and of itself appears less violent: monitoring of social media alone involves no violence. However, other benefits arise from the use of digital forms of repression: reduction in the cost of obtaining information, which in turn, makes it easier for states to shift from indiscriminate forms of repression to more targeted forms of repression. This type of information gathering comes in the form of digital surveillance, be it through malware, monitoring online activities, data harvesting, physical tracking, etc. Additionally, some forms of digital repression allow for state control over the flow of information. This type of control comes in the form of internet shutdowns, telecommunications disruptions, content moderation, censorship, among other tactics.

The critical factor here that links the use of repression (both indiscriminate and targeted) with why digital repression could seemingly reduce the appearance of violent repression is information scarcity. Prior to the adoption, diffusion, and expansion of the internet, obtaining detailed and accurate information on targeted individuals was much more costly (Gohdes, 2023). This required not only the ability of the state to extensively recruit, train, monitor, reward, and punish state agents who facilitated intelligence gathering operations, but it would necessitate intelligence gathering apparatuses, which were also costly and limited technologically. Implicitly, this also meant that even if the state had each of these in place, agents would need to be trained and

share in the preferences of the state to carry out orders to engage in information gathering as agency loss (Mitchell, 2004). Given the high price tag associated with precise forms of intelligence gathering, many regimes throughout history often resorted to indiscriminate violence to threaten, coerce, and carry out violence in order for citizens to inform on individuals of interest by the state. As Kalyvas (2006) argues, indiscriminate violence offers a pathway by which innocent people being targeted with state violence should influence a change in the guilty's behavior either through sheer force by the innocent or through the guilty's realization of their actions on innocent people (Kalyvas, 150). In other words, if the state doesn't have the information necessary to identity certain individuals of interest, then violence against innocent individuals - particularly those somehow close to the guilty - should function as a motivator to alter the guilty's behavior to fulfil the government's will. To reiterate, this historically has been the option selected by violent regimes when the information environment has been lacking and the state's capacity to engage in intelligence gathering has been limited (ibid). This preference, again, has been rooted in financial, human, and technological constraints imposed on the state, which factor into the overall decision-making of a government. States have other policy options available, and often will chose other options alongside repression, but repression is more often selected by states because its overall lower financial costs compared to other policy options (Poe, 2004). Referring to the case of Mozambique, there have been sparse allegations of illegal surveillance by opposition members of the Frelimo government, members of the media, some civil society organizations, and social media by members (Unites States Department of State, 2024). However, greater attention has been drawn to the government of Mozambique relying more heavily on internet shutdowns and restricting social media in cases of the 2023 and 2024 elections (Access Now, 2024d; Untied States Department of State, 2024).

The ability to engage in targeted or selective repression hinges upon the ability of the state and its agents to overcome exorbitant capacity costs to obtain accurate information on targeted

individuals. In such environments, agents still rely on individuals for intelligence collection and do so in ways that produce the image to civilians of vast networks of informants (Kalyvas, 2006). This form of repression is seen by officials as being preferable to indiscriminate violence because of the signals that it sends to the rest of the population that providing information to the regime and aligning with its interests means that less violence will occur (Garbe, 2023; Kalyvas, 2006). Further, violent coercion is reduced and instead citizens are merely threatened with the potential of violence in the face of non-compliance with state agents.

Even outside of conditions of extreme conflict and autocracies, information is still king. When considering the national security and judicial models in democracies, as presented by Rejali (2007), both place pressure on information acquisition. In the former, environments of domestic security incidences, crises, conflict, and wartime necessitate the state to acquire information pertaining to individuals who are perceived to be threats. Despite democracy's theorized institutional protections for human rights (Cingranelli & Filippov, 2010; Davenport, 2007; Hill & Jones, 2014; Moore & Welch, 2015), episodes of national security crises, bureaucratic breakdowns, and military empowerment may lead to conditions where state institutions are no longer willing to or cannot stop state violence used to elicit information from targets. In the latter model, judicial systems that highly value confessions of those accused of crimes place a premium on information. Here, state agents are motivated to obtain information (i.e., confessions, evidence of wrongdoings) of those arrested to ensure imprisonment, both for political and non-political crime. Again, state violence is often used to acquire information and obtain confessions from detainees - regardless of the validity of information provided (Rejali, 2007). In the case of Venezuela, Maduro's regime has done just this through its evolving policies of digital repression. Recently, there have been reports of Venezuelan officials engaging in Stalin and Maoist forms of "self-criticism", the undercurrent of show trials as known today. Here, state agents of the Bolivarian National Guard (BNG) and the broader

government use social media to disseminate reels and other short video footage to demonstrate three key messages as a form of propaganda to continue mass intimidation: showing "wrong-doings" of critics, locating enemies of the regime, and forcing targets to then engaging in "self-criticism", where they recount their "wrong-doings" and apologize to the regime, often begging for forgiveness. These videos are shared virally prior to the target's trial, with the final scene including intelligence, military, or other state officials (Areistegui, 2024). Additionally, with the regime's encouragement of its supporters to report on critics, human rights defender, and others who counter the government's goals, these informant apps provide further "evidence" to use against opposition.

Across each of the examples above, obtaining information remains the primary objective of the state and acquiring it typically comes at high costs - human, economic, financial, security etc. Moreover, these traditional ways in which governments have engaged in violence to acquire information have often been overt. Like the mechanisms behind state agents shifting from scarring to clean forms of torture, governments that shift from overt forms of intelligence gathering to more covert likely do so for purposes of plausible deniability and reducing certain associated costs (Conrad & Moore, 2010).

The allure of governments to shift from traditional and violent methods of information gathering to using digital tools is evident. First, while human capacity is still required to carry out information gathering, much more of this can be done remotely than ever before and does not require as many bodies on the ground. This reduces several facets of overt coercion that indiscriminate state violence has historically imposed on violent regimes – the maintenance of state agents, reducing agency loss, and reducing the appearance of informant networks that many regimes across time and space have utilized. Given the reduction of indiscriminate violence to procure information from swathes of a population, this would mean that governments are engaging in less overt violence, which in turn, should elicit less international attention from mass atrocity events. In

turn, governments can use these modalities to engage in more targeted repression campaigns against regime challengers. In essence, the adoption, diffusion, and innovation of repression technology should expedite targeted repression, which would lead to the appearance in a reduction of violent repression. Once surveillance and monitoring practices are routine within a state, this makes it to where information collected by government surveillance programs can be used to more effectively seek and detain anyone who opposes or is perceived as a threat to the state. Once targets are detained, governments may make an example out of these individuals to both deter others within the population from engaging in similar behaviors and to clue in people living with the country that they are also being monitored. The precedent would be set for individuals in these contexts to know they are being surveilled and know the repercussions of engaging in anti-state rhetoric or behavior. This should lead to the overall appearance of mass violent events decreasing, which could lead to the international community to shift shaming campaigns elsewhere. In this scenario of surveillance-style digital repression campaigns, citizens may be less frequently subjected to campaigns of violence in the name of information, but this comes at the cost of other rights violations, which typically include violations to the rights to privacy, freedom of expression and opinion, political participation, assembly and association, among others.

When considering how these dynamics factor into government approaches where the focus shifts from surveillance to a preference of withholding information from outside observers to internet shutdowns, telecoms blackouts, and other communication app blockages, these strategies are likely to have major implications. In cases where there may be situational or sporadic dissent against the government, state officials may seek a different response compared to long term, sustained movements. From the side of civilians, dissatisfaction and challenges to the status quo in this context may arise from advancement of unpopular policies, irregular elections leading to unexpected results, other response to government scandal. For instance, from 2020-2021, the Indian

government under Narendra Modi proposed a series of farming reforms which would have had drastic financial consequences on Indian farmers, namely through repealing several financial protections for farmers and the sector as well as weakening collective bargaining power of unions. While the protests remain peaceful throughout the country, including planned hunger strikes by farmers, the Indian government targeted locations around the capital with internet and other mobile services in response (BBC, 2021). Contention escalated to violence in October 2021 when eight people were killed, including four farmers (The Times of India, 2021). Regarding electoral contention and state decisions for reduced connectivity, both Venezuela and Mozambique cases demonstrated how this played out. In Venezuela, public addresses of Juan Guaidó and the National Assembly were frequently censored while during the 2024 election in Mozambique, the government ordered shutdowns of internet service providers and had WhatsApp blocked for citizens. In the former, reduced connectivity approaches included blocking of services and apps to prevent opposition from addressing the public. In Mozambique, this was done to halt the spread of information on polling centers, specifically their locations and opening hours. Further, once the internet had been shut down, mass violence ensued where over 400 people were arrested, 11 opposition members were killed, and hundreds were injured during the episodes of state-sponsored violence. In all cases, governments sought more immediate solutions to quash imminent threats.

In situations where states opt for reducing access to the internet, telecommunications services, social media, and other means of rapid communication, government agents are not necessarily reducing their usage of violence. Across these cases, violent repression did not stop, but this strategy makes it possible for governments to reduce the amount of information that's available to outside audiences. As a result, this often reduces the amount of information available on abuses carried out during periods of internet black outs or other service stoppages, as civilians who are brutalized by governments may have a more difficult time accessing emergency services or be able to

share documentation of human rights violations by state agents with their community or other outside observers (e.g. journalists, human rights organization, etc.). This can significantly reduce the sharing of documentation and evidence of abuse carried out by state agents during of periods of violence. Moreover, from the state's perspective, government elites have several incentives to hide abuses, as episodes of mass violence and killings would likely elicit some form of sanction and repercussion. In the face of harsh international, regional, and domestic responses, this could make maintaining their positions of power much more difficult. With these motivations of wanting to stave off threats - from outside observers or domestic challengers - relying on a more immediate, shorter-term solution to shut down the internet and reduce communications, governments have the motivation to threaten, detain, kill, torture, or disappear those who impose on their will. With internet shutdowns and other service stoppages, governments have means to coerce challengers, keep the rest of the world in the dark on state violence, and delay the spread of information about what is happening within the state to outside audiences. These periods also buy time for agents to confiscate devices that may have evidence of illegal conduct by state agents that could be used against them in the future.

To summarize, states have incentives to reduce the appearance of violent repression by substituting or complementing existing policies of overt repression with various repertoires of digital repression. The use of digital repression capacities doesn't erase violent repression; it reduces its visibility while simultaneously complementing targeted forms of repression. Because governments and their agents are faced with accountability structures such as transnational naming and shaming campaigns that would impose significant costs on the use of widespread violence against populations, government that would traditionally use indiscriminate have an incentive to strategically engage in digital repression to improve their information scarcity problems. On one hand, states can utilize certain methods of digital repression to collect information on particular individuals who the

regime views as a real or perceived threat at a much lower cost than traditionally has been the case. On the other hand, when states are anticipating that mass violence episodes will be shamed by the international community, particularly in cases of electoral or other political dissent, the state should be more inclined to engage in more internet shutdowns and other forms of digital repression that function to disrupt the flow of information to the international community. As such, I propose the following hypotheses:

Hypothesis 1a: When a government is facing prolonged environments of dissent, the government will choose to engage in more surveillance-heavy forms of digital repression

Hypothesis 1b: Surveillance-style forms of digital repression should be associated with lower levels of overall violent human rights abuses

Hypothesis 2a: When a government is facing singular events of dissent, the government will opt for reduced-connectivity forms of digital repression.

Hypothesis 2b: Reduced connectivity forms of digital repression will be associated with increased levels of violent repression.

Methodology

In the theory described above, leaders have multiple options available to them when facing contexts of dissent: employ mass networks of surveillance to gather information on potential threats or to restrict or completely shut down the internet and other communications technologies. In turn, these decisions of a government to engage in one of these options should lead to varying degrees of the severity of human rights violations: mass surveillance should lead to fewer cases of violent repression while internet shutdowns should lead to more violent human rights abuses. To model this dynamic, this study will model two systems of equations using seemingly unrelated regressions.

Because each of the regressions within the two systems have varying dependent variables but the outcomes are related, the model selection strategy should account for these theoretical dependencies. Although these regressions could be tested separately, there is reason to believe that the error terms are likely correlated, meaning that the fit is better than separate ordinary least squares modelling. Further, this approach allows for the modelling of substitution and complemtarian effects. Finally, the use of seemingly unrelated regressions should mitigate concern of endogeneity, which is a frequent concern in the repression-dissent literature. The sample contains all countries from years 2000 to 2022. The unit of analysis is the country-year.

Dependent Variables

This study relies on three primary dependent variables: surveillance-based forms of digital repression, violent human rights abuses (i.e., violent repression), and reduced-connectivity forms of digital repression. To measure these, this study relies on two indicators from the Varieties of Democracy and another measure from the CIRIGHTS data project (Cingranelli et al., 2014; Coppedge et al., 2025; Mark et al., Forthcoming; Pemstein et al., 2025). Starting with the surveillance measure, this comes from V-Dem's social media monitoring variable. Although this is not conceptually holistic of surveillance, data on surveillance is severely limited. This indicator is initially measured as an ordinal variable, where respondents are asked, "How comprehensive is the surveillance of political content in social media by the government and its agents." Answers range on a scale of 0, where government surveillance is widespread on all content on social media, to 4, where governments effectively does not surveil political content online. It was then converted to an interval variable using Bayesian ordinal item response theory measurement modelling techniques. The interval scale ranges from -3.59 to 2.992, where lower values indicate greater degrees of social

media surveillance by the government and its agents and higher values indicate lower levels of surveillance (Pemstein et al., 2025).

To operationalize reduced-connectivity, this studies also relies on V-Dem's data and uses the internet shutdowns in practice variable. This measure captures how often governments shut down the internet. Using the same methodology described above, the interval variable used here ranges from -3.968 to 2.063, where lower values indicate more frequent internet shutdowns and higher values represent less frequent internet shutdowns (Pemstein et al., 2025).

The final dependent variable, violent human rights abuse, comes from the CIRIGHTS Data. Specifically, this study utilizes the Physical Integrity Rights Index, which is a sum of how states score along the individual physical integrity rights. These rights include disappearance, torture, political imprisonment, and extrajudicial killings (Mark et al., forthcoming). These rights violations are some of the traditional forms of violent repression used by governments in contentious contexts.

Independent Variables

The study primarily relies on the following set of indicators to test the surveillance-based and reduced-connectivity arguments: mass mobilization, a multiplicative interaction term of mass mobilization with government social media monitoring, and another multiplicative interaction term comprised of mass mobilization and government internet shutdowns in practice. Each indicator comes from the Varieties of Democracy dataset. Mass mobilization is measured as an ordinal variable ranging from -3.6 to 4.1, where lower values indicate fewer instances of mass mobilization and higher values reflect greater instances of mass mobilization. The measure captures not only the frequency of mass mobilization events, but it also includes whether events were large or small-scaled (Pemstein et al., 2025). These events are specifically capturing non-violent events, such as demonstrations, strikes, and sit-ins. Although these events are typically organized by non-state

actors, this measure also includes government led rallies. Mass mobilization is used across both surveillance and reduced-connectivity hypotheses, as it is argued to be a primary mechanism where frequency and intensity of dissent mobilization events drive decision making among the chief executive and political elites. Regarding hypothesis 1b and 2b (i.e., the second equations in across the two models with the interaction term), this measure is used in multiplicative interactions with surveillance-based approaches and reduced connectivity, respectively. The other main arguments here are that these competing strategies should lead to lower or higher levels of violent human rights abuses. In turn, interactive terms are necessary here to capture the conditional effect that mass mobilization and digital repression strategies have on violent human rights outcomes.

Controls

There are other factors that also matter for these theoretical arguments. First, elections are often a driver of digital repression. Whether campaigning on behalf of opposition parties, electoral violence episodes where government may want to hide state violence on civilians, among other cases, these events surely factor into outcomes. The measure included here, elections, is a binary indicator where 0 indicates no election in a given year and 1 indicates that there was an election in the year. This data comes from the Idea Voter Turnout Data Base (IDEA, 2024).

Next, the study controls for judicial constraints on the executive. This is included for two key reasons. First, due to conceptual overlap between human rights measures and democracy indicators (Hill & Jones, 2014), one effective way to address this is through using another measure that is a key attribute of democracy, judicial independence. The other reason to rely on this indicator over a democracy measure is that a stronger judiciary should be able to thwart government attempts to engage in either type of digital repression strategy through judicial checking of the executive. If an executive was to order telecoms companies to limit or stop their services or ramp up mass

surveillance efforts, independent courts should be able to temper these executive actions without manipulation by the ruling leader. To measure this, the study relies on V-dem's judicial constraints on the executive, which is measured on an interval scale ranging from 0-1, where lower values indicate less judicial constraint on the executive (Pemstein et al., 2025).

Other potential confounders include conflict, internet users within a country, GDP, and the population of a country. Conflict in this study is measured by counts of conflicts that have occurred within a given country-year. These data come from the UCDP Battles-Related Deaths Dataset (Davies et al., 2024). The final three covariates all come from various World Bank data sources: the internet users variable is measured as a percentage of internet users within a country, while GDP and population numbers are logged (The World Bank, 2024a, 2024b, 2024c).

Results and Discussion

Table 3.1 presents the coefficients and standard errors of the first seemingly unrelated regression. The first equation of the model, *Social Media Surveillance,* evaluates the impact of the key independent variable, mass mobilization, on a government's decision to use surveillance technologies in response to highly attended and frequent dissent events (e.g., protests, demonstrations, etc.). The second column of Table 3.1, *Violent Repression,* presents the results of the second equation from this seemingly unrelated regression: the mass mobilization's conditional relationship with surveillance-based approaches and the subsequent impact on violent repression (i.e., violent human rights abuses). In the first equation, the model performs according to expectations across all variables. The results suggest that there is a positive, statistically significant relationship between mass mobilization and a government's propensity to use surveillance to monitor individuals within the state.

Table 3.1: SUR Results for Surveillance-Based Approaches

	Model 1, Equation 1 **DV: Social Media Surveillance**	Model 1, Equation 2 **DV: Violent Repression**
Mass Mobilization	0.045*** (0.015)	-0.147*** (0.018)
Social Media Surveillance		0.390*** (0.022)
Social Media Surveillance*Mass Mobilization		0.063*** (0.011)
Elections	0.289*** (0.049)	0.039 (0.061)
Judicial Constraints	3.096*** (0.067)	1.448*** (0.106)
Conflict	-0.305*** (0.035)	-0.781*** (0.042)
% Internet Users	-0.001 (0.001)	0.010*** (0.001)
GDP (logged)	-0.066*** (0.022)	0.175*** (0.027)
Population (logged)	0.000 (0.025)	-0.632*** (0.031)
$\varrho_{1,2}$	1.000	1.000
N	3,385	3,385
R^2	0.462	0.663
Df	7	9

**** p<.001, ** p<0.01, *p<0.05*

For a one unit increase in mobilization activity, there is an associated 0.045 increase in a state's use of social media surveillance. To reiterate, this measure for surveillance only incorporates the use of social media monitoring by the government. Other common forms of surveillance such as facial recognition, CCTVs, wiretapping, etc. are excluded from this indicator.

One of the main hypotheses of this study proposes that when states use surveillance practices during periods of prolonged dissent, agents may do so to more efficiently individuals who they perceive to be threats. Given multiple domestic and international motives to reduce the

appearance of violent human rights abuses, surveillance approaches should allow for state agents to avoid using mass coercion or violence to gather information on potential threats to the government. In turn, this reduces the appearance of human rights violations, periods or episodes of mass violence, or other broad state-sanctioned campaigns of violence because agents have the information to target individuals. However, while violent human rights abuses would appear to have reduced with a rise in surveillance technology, this comes at the cost of other civil rights violations.

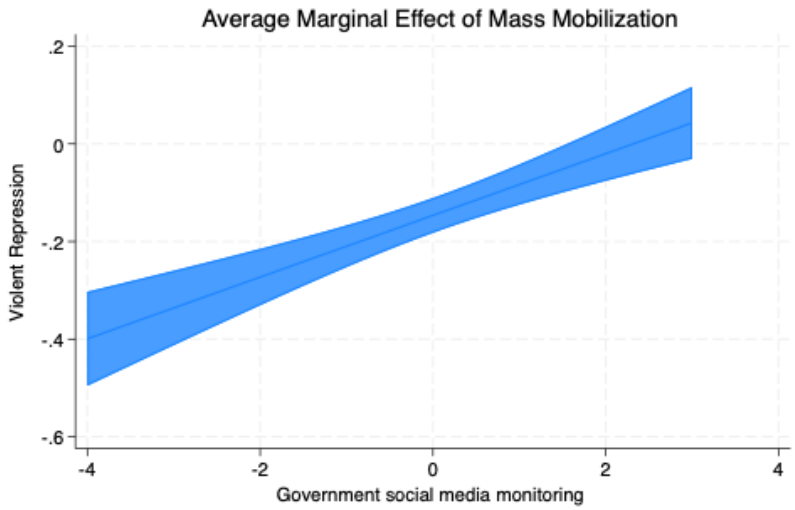

Figure 3.1: Average marginal effect of mass mobilization across different levels of surveillance

Figure 3.1 presents evidence that counters these expectations. First, the theory posited that when surveillance was met with prolonged contention environments, this should reduce violent repression. However, Figure 3.1 above demonstrates that this relationship is positive. When lower levels of mass mobilization are met with the highest levels of social media surveillance, the probably that the government will engage in violent repression in contentious environments is lower. Conversely, when mass mobilization is more frequent and better attended and levels of government

social media monitoring is lower, there is a great probability that violent repression will be used by a government and its agents. As such, Hypothesis 1b is rejected.

Table 3.2: SUR Results for Reduced Connectivity Approaches

	Model 2, Equation 1 **DV: Reduced Connectivity**	Model 2, Equation 2 **DV: Violent Repression**
Mass Mobilization	0.040*** (0.011)	0.014*** (0.004)
Internet Shutdowns		0.005 (0.006)
Internet Shutdowns*Mass Mobilization		0.009*** (0.003)
Elections	0.225*** (0.037)	0.010 (0.013)
Judicial Constraints	2.568*** (0.050)	-0.138*** (0.024)
Conflict	-0.376*** (0.025)	-0.014 (0.009)
% Internet Users	0.004*** (0.001)	-0.002*** (0.000)
GDP (logged)	-0.040** (0.016)	-0.020*** (0.006)
Population (logged)	0.019 (0.019)	0.052*** (0.007)
$\varrho_{1,2}$	1.000	1.000
N	3,385	3,385
R^2	0.557	0.180
df	7	9

****p<.001, **p<0.01, *p<0.05*

The reduced connectivity approach posited that there are more one-off or sporadic demonstrations or other non-violent political gatherings occurring, this will more likely lead to governments to choose to shut down the internet and other communication services. In turn, this should lead to a greater likelihood that elites order agents to carry out more violent human rights

and repression to protect the state. Because information channels are effectively cut off, and the government wants to stifle situational dissent, this will lead to a context where officials are more inclined to hide evidence of violence to outsiders, such as the case in Mozambique. Table 3.2 provides the results from the second seemingly unrelated regression. The first equation the model, *Reduced-Connectivity*, demonstrates a positive and statistically significant relationship between mass mobilization and internet shutdowns. As movements and demonstrations increasingly sustain participation over time, the model suggests that there should be more internet shutdowns or other telecommunications disruptions as a result, which is counter to the arguments presented.

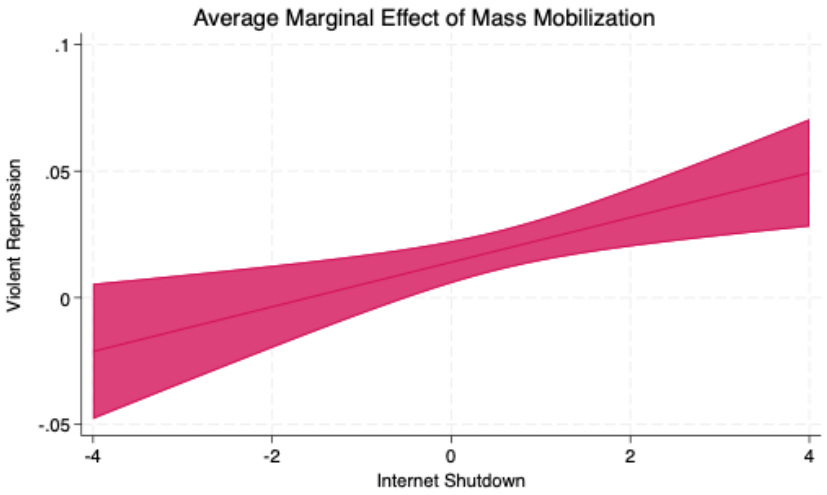

Figure 3.2: Average marginal of mass mobilization across different levels of internet shutdowns

The relationship of interest focuses on the interactive effect between mass mobilization and internet shutdowns on overall levels of violent repression. Figure 3.2 above presents these results. Although the results for the interactive term are somewhat statistically significant (p=0.09), when internet shutdowns are at their highest and mass mobilization is low, the probability of state ordered violent repression is much lower. In a closer examination of which countries comprise the higher

levels of internet shutdowns, a few include Belarus, Myanmar, Chad, Eritrea, India, Iran, Iraq, North Korea, Turkmenistan, among others. This is not surprising, given the degree to which most, if not all, of these countries have been able to either completely control the internet with providing little to no meaningful access to citizens (e.g., Turkmenistan, North Korea, Eritrea), are repeat offenders of ordering internet shutdowns (India, Myanmar, Iraq, or Iran), or have been involved with conflict to varying degrees (Sudan, South Sudan, Belarus, Chad). Further, while internet shutdowns are happening more each year (Access Now, 2025), these are still fairly rare events. In countries with stronger democracies, these are less likely to happen given institutional mechanisms that should both keep executives from resorting to this extreme response in the face of political demonstrations. Democratic institutions also have institutional means to both provide and protect individuals who wish to engage in some form of non-violent protest. The effect of the interaction terms becomes significant around 0 on both axes. Between 0 and 2 on the X-axis, there is evidence to suggest that cases where internet shutdowns are not as frequently used or the internet is severely restricted, this leads to a greater probability of violent repression being ordered by state officials when mass mobilizations are smaller and still infrequent. As protests, demonstrations grow and happen more often, internet shutdowns have a lesser impact on the relationship.

Discussion

The models presented above seem to provide evidence to support for two of the four hypotheses: greater political mobilization should lead to more state surveillance and contexts where political movements mobilize to challenge the state are met with internet shutdowns face a greater chance of violent political repression by government agents. However, because the empirical strategy used was a seemingly unrelated regression, to meet one of the key assumptions of this approach, there much be evidence to suggest that the errors are correlated across the system of equations. Upon

conducting a Breusch-Pagen to test whether the errors are correlated, this resulted in a p=1.000, which indicates that there is no meaningful relationship between the residuals of the equations. Ultimately, this means that there would need to be further testing conducted to find a better model fit and to deal with the issues of endogeneity.

Even with this caveat, is still worth discussing some of the initial results from the models. Although the results did not find statistical support, it is still important to discuss these results to carve a path forward in approaching this topic in the future. Further, keeping in mind the case studies presented in the beginning of this article, pairing this information with the unsubstantiated results can also offer a blueprint in overcoming theoretical pitfalls.

First, protests, demonstrations, and other non-state agent mobilization efforts have long been established as being a key factor in state repression, be it preventive or in response to challenges of the status quo. Through combining some of the case study information with some of the initial results, there is reason to believe that this relationship extends to the same dynamics of physical repression and dissent. Theoretically, digital repression and even digital dissent are ultimately still assumed to adhere to the general findings of the traditional repression-dissent nexus literature, but the online nature of these dynamics are still important to understanding how challengers and governments have adapted with tech during contention. Preliminary tests in this study evaluated whether smaller and more infrequent demonstrates should elicit a greater response of internet shutdowns versus those that are sustained. While the results here need further study, Chapter 2 of this dissertation still provided evidence in line with traditional findings: as mass mobilization increases during periods of domestic contention, state-ordered internet shutdowns or disruptions are more likely to occur. When considering the cases that have been evaluated in this study, as well as general trends surrounding the relationship between electoral violence internet

shutdowns, there are reasons to suggest that mass mobilization on its own isn't necessarily the only driver of internet shutdowns.

These results from Chapter 2, the cases included in this study, and the initial (but limited) results suggests that there is a substitution and complementary effect occurring. This was often the case with Venezuela, where the Maduro government relied heavily on reduced connectivity approaches prior to his second term to target political opposition candidates and their supporters within the government, this time around, his regime has leaned much more heavily into institutionalizing surveillance-based practices to target civilians, critics, and other opposition sympathizers. Even in Mozambique, government attempts to surveil as early as 2022 have been at play, despite FREMILO's repeated uses of internet shutdowns during and following the 2024 election (Access Now, 2024a, 2024b). In both cases, states are strategically using various digital repression strategies to complement larger goals (e.g., reduced connectivity to silence opposition, surveilling and detaining opposition supporters). The findings here call for deeper theorizing of cases to better understand what drives the sequencing, selection, and constraints imposed that would factor into the decision making of a government to utilize either of these approaches. For example, constraints exist that may limit some states from relying on internet shutdowns as an option in the face of mass discontent. Trade volume, capital-centered economies, international human rights law, and other legal obligations may limit the abilities of states to not use extreme approaches like internet shutdowns, and even app-based service blocks. Given the constraints of some aspects of the international system, these factors may alter escalation of digital strategies of governments to carry out extreme options such as total or even regional internet shutdowns. Alternatively, states may have the option to engage in much more targeted internet shutdowns down to local or village levels. The Indian government, which has been the prime offender of internet shutdowns until 2025, has been able to carry out internet shutdowns using this strategy for years and still maintain its

economic standing (Access Now, 2025). Further, studying how states begin to make the transitions to either substituting out surveillance-based and reduced connectivity approaches or learning how to use them to complement one another to maximize the government's goals, would be telling of and allow for stronger policy prescriptions towards working to limit these digital abuses.

With this study, there are some additional shortcomings regarding data and measurement. In addition to needing better model specification, one key drawback is the operationalization of state surveillance. The measure used to test for surveillance only captures government surveillance of social media, which is hardly comprehensive of the full repertoire of surveillance tactics available to states and their agents. Improved measures would capture a broader spectrum of government sanctioned surveillance and monitoring strategies: numbers and locations of CCTVs, license-plate readers, wiretaps, access and reading of private communications (e.g., email, physical mail, social media accounts, etc.), spyware, among others. While these data are limited in scope globally, there are some sources available that could provide insight in more specific locations. For example, the Atlanta Press Collective has recently obtained information through an open records request on the locations of 1,755 surveillance cameras and license plate readers for Fulton County. Through compiling this data along with information on even more proposed locations for surveillance tech around Atlanta, the group was able to publish data on the known locations of some these devices (Shelton, 2025). However, this is only a fraction of cameras -- over 60,000 are in use throughout the city, with 45,000 being considered "active". Given that Atlanta is the most surveilled city in the United States and the only other place in the world with more surveillance being China, being able to study these dynamics with this granular level of data would provide crucial insights into the relationship between state violence and surveillance (ibid).

The other pitfall with measurement is the reduced-connectivity variable, which only captures internet shutdowns and no other telecommunications, SMS, social media, or other service-based

shutdowns. This is crucial to include in this measure given that resorting to internet shutdowns tend the be the direst option that a government has at its disposal. As such, full or even partial internet shutdowns still tend to be relatively rare events, but the targeting of other related services is far more common.

Conclusion

This study focused on the question of how state leaders select from two major forms of digital repression in environments of political contention: surveillance-based and reduced connectivity. The argument asserted that when mobilization levels were higher, states would rely on surveillance tactics to gather information on dissidents, and in turn, this would facilitate state agents in engaging in lower overall levels of human rights abuses, or violent repression, to make the appearance of violence lower from outside audiences. If facing more sudden, situational mobilization, states may be more inclined to rely on reduced connectivity approaches as a swifter option as well as to buy time to hide and destroy evidence of rights abuses by state agents. In both scenarios, governments would rely primarily on one strategy over the other (i.e., substitution) while simultaneously relying on one of these approaches to complement other more traditional repertoires of repressions carried out by state agents used to reduce information or appearance on abuses. On the surface, the results indicate that there is certainly evidence to suggest a relationship across the board, but not in the ways that were theorized. At first glance, it appeared that mass mobilization will lead to greater social media surveillance by the government and governments facing sporadic dissent that have already implemented an internet shutdown are more likely to engage in violence against civilians. However, given that there was no evidence of correlation between the error terms across both sets of the seemingly unrelated regressions, no support for the hypotheses could be

substantiated using the seemingly unrelated regression as the empirical strategy. As such, further work and improved model specification are necessary to find evidence among these relationships.

There are some weaknesses with this current approach: theoretically, in terms of measurement, and regarding model selection. More theoretical development is needed to understand the processes through which states either substitute out one approach over the other and to understand what may lead states to transitioning away from one form of digital repression over another, such as the case of Venezuela. Measurement-wise, more valid measures are needed to continue these studies, particularly when it comes to surveillance practices of governments. For model selection, a better approach may be to develop an instrumental variable to circumvent issues of endogeneity. Alternatively, a series of bivariate probits or three stage least squared may be more could be viable options.

Ample room for research exists in this area. First, to address the gaps presented above, researchers may need to shift away from studies involving a global scope and lean into comparative or qualitative approaches to illuminate some of the processes and mechanisms through which governments engage in during ramping up digital repression and transitioning between these tactics. These should also include an emphasis on the sequencing of digital repression tactics, focusing on the transitions in and out of various digital repression approaches, and potential neighboring effects. Further, more data is necessary to study governments surveillance practices, and largely how governments engage in privacy rights violations at large. Future studies could also evaluate how spatial diffusion of digital repression tactics of one state impacts surrounding countries and their decisions to digitally repress as well as what constraints exist to deter governments from relying on extreme forms of digital repression, especially internet shutdowns. It is also important to evaluate the ways in which surveillance technologies are impacting other areas of human rights, especially

when considering how artificial intelligence is increasingly being incorporated in repertoires of digital repression.

References

Access Now. (2024a). "2024 elections and internet shutdowns watch." *Access Now*. URL: https://www.accessnow.org/campaign/2024-elections-and-internet-shutdowns-watch/#Mozambique

Access Now. (2024b). "Africa in 2023: Internet shutdowns attack democracy." *Access Now*. https://www.accessnow.org/press-release/africa-keepiton-internet-shutdowns-2023-en/

Access Now. (2024c). "Authorities and internet service providers in Mozambique must respect human rights and #Keepiton during protests." *Access Now*. URL: https://www.accessnow.org/press-release/keepiton-mozambique-authorities-must-respect-human-rights/

Access Now. (2025). "Emboldened offenders, endangered communities: Internet shutdowns in 2024." *Access Now*. Retrieved March 27, 2025, from https://www.accessnow.org/keepiton-2024-report

Alarcón, A. (2024). "Venezuela's many means of surveillance and control." *Access Now*. https://www.accessnow.org/the-many-means-of-surveillance-and-control-in-venezuela/

Al Jazeera. (2024). "Police in Mozambique disperse opposition protest after disputed election." *Al Jazeera* URL: https://www.aljazeera.com/news/2024/10/21/police-in-mozambique-disperse-opposition-protest-after-disputed-election

Amnesty International. (2024a). "Mozambique 2024." *Amnesty International*. URL: https://www.amnesty.org/en/location/africa/southern-africa/mozambique/report-mozambique/

Amnesty International. (2024b). "Venezuela: Tech companies set dangerous precedent with app for reporting anti-government protesters." *Amnesty International* URL: https://www.amnesty.org/en/latest/news/2024/08/venezuela-tech-companies-set-dangerous-precedent-with-app-for-reporting-anti-government-protesters/

Aristegui. (2024). "Maduro activa el linchamiento 2.0 de opositores." *Aristegui*. URL: https://aristeguinoticias.com/1308/mundo/maduro-activa-el-linchamiento-2-0-de-opositores/

BBC. (2021). "India protests: Internet cut to hunger-striking farmers in Delhi." *BBC*. Retrieved June 5, 2025, from https://www.bbc.com/news/world-asia-india-55872480

Berman, M. R., & Clark, R. S. (1982). State terrorism: Disappearance. Rutgers Law Journal, 13 (3), 531–578.

CBC Radio. (2019). "Why Venezuela's internet shuts down every time Juan Guaidó speaks."

CBC Radio. URL:https://www.cbc.ca/radio/day6/venezuela-media-censorship-impeach-o-meter-supreme-court-nomination-leaks-horror-movie-hype-and-more-1.5074901/why-venezuela-s-internet-shuts-down-every-time-juan-guaido-speaks-1.5074909

Cingranelli, D., & Filippov, M. (2010). "Electoral rules and incentives to protect human rights." *The Journal of Politics*, 72 (1), 243–257.

Cingranelli, D. L., Richards, D. L., & Clay, K. C. (2014). The CIRI Human Rights Dataset. *CIRI*. https ://doi.org/http://dx.doi.org/10.2139/ssrn.4625036

Conrad, C. R., & Moore, W. H. (2010). "What stops the torture?" *Journal of Political Science*, 54 (2), 459–476.

Coppedge, M., Gerring, J., Knutsen, C. H., Lindberg, S. I., Teorell, J., Altman, D., Angiolillo, F., Bernhard,
M., Cornell, A., Fish, M. S., Fox, L., Gastaldi, L., Gjerløw, H., Glynn, A., God, A. G., Grahn, S., Hicken, A., Kinzelbach, K., Krusell, J., . . . Ziblatt., D. (2025). V-dem codebook v15 varieties of democracy (v-dem) project. Varieties of Democracy. https://doi.org/https://doi.org/10.23696/vdemds25

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

Davies, S., Engström, G., Pettersson, T., & Öberg, M. (2024). "Organized Violence 1989-2023, and the prevalence of organized crime groups." *Journal of Peace Research*, 61(4): 673-693.

Earl, J. (2011). "Political repression: Iron fists, velvet gloves, and diffuse control." Annual Review of Sociology, 37, 261–84.

Gamboa, L. (2024). "Plebiscitary override in Venezuela: Erosion of democracy and deepening authoritarianism." *The Annal of the American Academy of Political and Social Science*, 712 (1), 124–136.

Garbe, L. (2023). "Pulling through elections by pulling the plug: Internet disruptions and electoral violence in Uganda." *Journal of Peace Research*, 62 (3).

Gohdes, A. (2024). *Repression in the digital age: Surveillance, censorship, and the dynamics of state violence.* Oxford University Press.

Hill, D. W., & Jones, Z. M. (2014). "An empirical evaluation of explanations for state repression." *American Political Science Review,* 108 (3), 661–687.

IDEA, I. (2024). Voter turnout database. *International IDEA* URL: https://www.idea.int/data-tools/data/voter-turnout-database

Kalyvas, S. N. (2006). *The logic of violence in civil war*. Cambridge University Press.

Krcmaric, D. (2019). "Information, secrecy, and civilian targeting." *International Studies Quarterly*, 63, 322–333.

Lawal, S. (2024). "'Ready to die': Protesters face bullets for political change in Mozambique." *Al Jazeera* URL: https://www.aljazeera.com/features/2024/10/31/ready-to-dieprotesters-face-bullets-for-political-change-in-mozambique

Lichbach, M. I. (1987). "Deterrence or escalation? the puzzle of aggregate studies of repression and dissent." *Journal of Conflict Resolution*, 31, 266–297.

Mark, S., Cingranelli, D. L., & Filippov, M. (Forthcoming). "Cirights: Quantifying respect for all human rights."

Meng, A., Kelly, T., & Belson, D. (2025). "Mozambique's post-election fallout: Fatal protests and widespread internet shutdowns." *Internet Outage Detection and Analysis*. URL: https://ioda.inetintel.cc.gatech.edu/reports/mozambiques- post- election-fallout-fatal-protests-and-widespread-internet-shutdowns/

Mitchell, N. J. (2004). *Agents of atrocity: Leaders, followers, and the violation of human rights in civil war*. Palgrave Macmillian.

Moore, W. H. (1998). "Repression and dissent: Substitution, context and timing." *American Journal of Political Science*, 42 (3), 16–42.

Moore, W. H., & Welch, R. M. (2015). "Why do governments abuse human rights*?" Emerging Trends*, 1–16.

Murdie, A. M., & Davis, D. R. (2012). "Shaming and blaming: Using events data to assess the impact of human rights ingos." *International Studies Quarterly*, 56 (1), 1–16.

Netblocks. (2019a). "Streaming services disrupted in Venezuela prior to Guaidó speech on national assembly blockade." *Netblocks*. URL: https://netblocks.org/reports/streaming-services-disrupted-in-venezuela-prior-to-guaido-speech-on-national-assembly-blockade-QAd2kRyl

Netblocks. (2019b). "Streaming services restricted in Venezuela as Guaidó discusses national plan from André's bello catholic university." *Netblocks*. URL: https://netblocks.org/reports/streaming-services-restricted-in-venezuela-as-guaido-discusses-national-plan-from-andres-bello-catholic-university-PyXR1zAE

Netblocks. (2019c). "Streaming services restricted in Venezuela as Guaidó holds press conference in Caracas." *Netblocks*. URL: https://netblocks.org/reports/streaming-services-restricted-in-venezuela-as-guaido-holds-press-conference-in-caracas-xyMGQGAZ

Netblocks. (2019d). "Youtube and online services restricted in Venezuela as Guaidó speaks from Guatire. *Netblocks.* URL: https://netblocks.org/reports/youtube-and-online-services-restricted-in-venezuela-as-guaido-speaks-from-guatire-zA4zDlyR

Netblocks. (2019e). "Youtube and online services restricted in Venezuela as Guaidó tours Los Teques, Miranda." *Netblocks* URL: https://netblocks.org/reports/youtube- and- online- services- restricted- in- venezuela- as-guaido-tours-los-teques-miranda-QAd2qPyl

Netblocks. (2019f). "Youtube and Periscope disrupted in Venezuela during national assembly live stream." *Netblocks* URL: https://netblocks.org/reports/youtube-and-periscope-disrupted-in-venezuela-during-national-assembly-live-stream-JBQxZbAo

Payne, C. L., & Abouharb, M. R. (2016). "The international covenant on civil and political rights and the strategic shift to forced disappearance." *Journal of Human Rights*, 15 (2), 163– 188.

Pemstein, D., Marquardt, K. L., Tzelgov, E., Wang, Y.-t., Medzihorsky, J., Krusell, J., Miri, F., & von Römer., J. (2025). "The v-dem measurement model: Latent variable analysis for cross-national andcross-temporal expert-coded data.V-Dem Working Paper, (21).

Poe, S. C. (2004). *Understanding human rights violations*. Ashgate.

Rejali, D. (2007). *Torture and democracy*. Princeton University Press.

Ritter, E. H. (2013). "Policy disputes, political survival, and the onset of severity of state repression." *Journal of Conflict Resolution*, 58 (1), 143–168.

Ritter, E. H., & Conrad, C. R. (2016). "Preventing and responding to dissent: The observational challenges of explaining strategic repression." *American Political Science Review*, 110 (1), 85–99.

Sequera, V., & Guanipa, M. (2024). "Venezuela launches investigation against opposition leaders amid protest crackdown." *Reuters* URL: https://www.reuters.com/world/americas/maduro-security-forces-round-up-venezuelans-involved-protests-operation-knock-2024-08-05/

Shelton, T. (2025). "Opinion – Mapping Atlanta's camera network and surveillance strategy" *Atlanta press collective.* URL: https://atlpresscollective.com/2025/06/10/atlanta-surveillance-camera-network/

The Times of India. (2021). "Lakhimpur Kheri violence: Supreme court extends interim bail to Ashish Mishrea." *The Times of India.* URL: https://timesofindia.indiatimes.com/india/latest-news-lakhimpur-kheri-violence-supreme-court-extends-interim-bail-to-ashish-mishra/articleshow/107619399.cms

The World Bank. (2021a). Gross domestic product. *The World Bank.* URL: http://data.worldbank.org/indicator/NY.GDP.MKTP.CD

The World Bank. (2021b). Percentage of individuals using the internet. *The World Bank*. URL: http://data.worldbank.org/indicator/IT.NET.USER.ZS

The World Bank. (2021c). Total population. *The World Bank*. URL: http://data.worldbank.org/indicator/sp.pop.totl

UNHCR. (2025). "Emergency appeal: Venezuela situation." *United Nations Office of the High Commissioner for Refugees*. URL: https://www.unhcr.org/emergencies/venezuela-situation

United States Department of State. (2024). "2023 country reports on human rights practices: Mozambique." *United States Department of State*. URL: https://www.state.gov/reports/2023-country-reports-on-human-rights-practices/mozambique/

US Department of State, Bureau of Western Affairs. (2019). "Venezuela: A democratic crisis." *United States Department of State*. URL: https://2017-2021.state.gov/a-democratic-crisis-in-venezuela/

CHAPTER 4:

DIGITAL RIGHTS AND LEGITIMATION: HOW GOVERNMENT STRATEGIES OF DERIVING LEGITIMACY IMPACT DIGITAL REPRESSION[9]

[9] LaVelle, Meridith. To be submitted to a peer review journal.

Abstract

What explains a government's willingness to violate digital rights? Traditional explanations of state violations of human rights, especially civil and political rights, are often rooted in theories of repression, principle-agent models, and agency loss. One alternative way to approach this question centers on the ways in which a chief-executive justifies its claim to power: legitimation strategies. This article argues that leaders who derive their rule using personalist means, rather than rational-legal, are more willing to support policies and engage in practices that erode the enjoyment of digital other related human rights. Personalist leaders are more likely to violate these rights for three key reasons: full digital rights enjoyment allows for holding leaders accountable; information asymmetries existing between the ruling elites and opposition members pose a threat to leaders; and weakened digital privacy means politically excluded out-groups are more at risk for being targeted for being threats to national identify. Using a series of ordinary least squares regressions, the result demonstrate that empowerment rights and digital repression generally erode under personalist rule, but privacy rights violations are not impacted by personalists.

Introduction

Authoritarians and other far right populist governments have chipped away at the progress of democratization since the 1990s (Idea International, 2025; Levitsky & Way, 2020; Varieties of Democracy, 2025). With this, various institutions used to uphold liberal democratic norms have also been increasingly neutralized and attacked by various nationalist far right leaders and supporters who aim to exclude those who pose a threat to national identity. Political, social, economic, and cultural forms of exclusion have been far reaching across dozens of multiple contexts: queer communities in

Egypt (US Department of State, 2024), women's rights activists in Iran (Amnesty International, 2025b; UN News, 2024), people of color, immigrants and undocumented individuals in the United States (Amnesty International, 2025a, 2025c; Human Rights Measurement Initiative, 2024c), political critics in Venezuela (Alarcón, 2024; Amnesty International, 2024; Sequera & Guanipa, 2024), Muslims and other non-Hindu groups in India (Council on Foreign Relations, 2024; Human Rights Measurement Initiative, 2024b; Human Rights Watch, 2024), among countless other examples. Varieties of Democracy's Democracy Report provides comprehensive statistical insights into just how far these trends have come, providing evidence to suggest that liberal democracies are now the least common regime type in the world, with only 24 countries maintaining this status. Meanwhile, nearly 72% of the world lives in autocracies, levels which haven't been seen since 1972 (Varieties of Democracy, 2025). The report also provide evidence pointing to autocratization happening at a greater rate across all regions in the world, with the highest concentration of this trend in sub-Saharan Africa and Eastern Europe countries.

Another key insight from the report cited the role of censorship as a key facilitator in the decline of democracies (Varieties of Democracy, 2025). While censorship in and of itself is hardly a new tactic used by authoritarian regimes, more modern approaches are being used by government to silence critics, media, academics, opposition members, civil society, intellectuals and artists among others who challenge the government's will and its policies: digital technologies. Throughout the cases mentioned above, digital components were and still are being used to target individuals' enjoyment of human rights more broadly. In particular, governments are using various forms of digital repression, especially surveillance, censorship, and content moderation, to target challengers who are simply trying to enjoy their various empowerment rights. This grouping of rights is composed of the right to freedom of opinion and expression, political participation, freedom of religion, and the right to assembly and association, which lends to civil society's ability to persist.

The primary goal of this article is to continue building on certain theoretical mechanisms that have been recently linked to explanations of why states engage in human rights abuses. Historically, human rights scholars have explained state sanctioned political violence and subsequent violations of human rights abuses using theories of repression and (Davenport, 2007; Hill & Jones, 2014; Moore, 1998; Moore & Welch, 2015; Poe, 2004; Poe & Tate, 1994; Ritter & Conrad, 2016). Comprised of threat and institutional arguments, theories of repressive state violence have produced a rich and ongoing literature. Much of this research is dedicated to understanding how real or imagined threats to regime tenure influence leaders to respond with violence (among other policy options) in a contentious political environment. Moreover, some strands of this literature are also dedicated to understanding the institutional mechanisms of democracies that are designed to prevent human rights abuses, particularly physical integrity rights abuses. Related, principal-agent theory has also been utilized to help explain human rights abuses through the lens of state capacity and agency loss. Assuming governments are able to effectively screen, hire, train, monitor, reward/punish, and compensate their agents, state leaders should be able to delegate their preferences to agents and agents will carry out these orders. On the other hand, when these conditions are not met, agency loss - or the inability or unwillingness for state agents to carry out order from the executive - may occur (Butler et al., 2007; Mitchell, 2004).

Recent work by Bagwell, Rains, and LaVelle (2023) has sought to extend the framework of principle-agent arguments to provide a more holistic theoretical approach to explaining motivations of a state and its agents to engage in human rights abuses. In the study, the authors explore how legitimation strategies factor into state decisions to carry out abuses towards outgroups within a particular nation, specifically in terms of physical integrity rights. The authors find that states with executives in power who derive their legitimacy through personalism are more likely to have worsened respect for this group of rights. However, this dissertation project has contended that

state preferences to reduce outside threats to leadership tenure should influence leaders to reduce overall levels of repressive violence towards domestic challengers and instead are more likely to utilize other means to engage in more targeted repression. By doing this, overall levels of state-sanctioned repressive violence are reduced, and in turn, this may stave off negative consequences from the international community and others invested in human rights conditions on the ground. As such, how might various forms of legitimation strategies impact empowerment and digital rights more broadly? Building off Bagwell, Rains, and LaVelle (2023), this article contends that leaders who derive their legitimacy to rule through personalist means (i.e., personality or other characteristics of that individual lend legitimacy to their rule) are more likely to engage in empowerment rights and other digital rights violations.

The article will proceed as follows: the first section will briefly review the literatures on legitimacy and motivations for governments to repress. Then, the next section will present the core theoretical argument: personalist leaders are more likely to engage in empowerment rights violations and digital rights violations because these types of rights present individuals the channels to critique, express and widely share negative opinions of, organize against, and hold the government accountable. Moreover, wider access to technology by governments allows for greater surveillance capabilities to keep tabs and collect information on individuals deemed particularly threatening to a regime. Given leader preferences for minimizing both domestic and international risks to continued maintaining of power, personalist leaders are instead expected to use these tools to streamline violence with the goal of reducing overall levels of physical integrity rights abuses. Finally, given that personalist leaders derive their legitimacy on the basis that they are the one true leader fit to rule "the people." This perception should mean that those who are as being part of the out-group in a state with a personalist leader are more likely to experience rights violations. Following the presentation of the theoretical arguments and hypotheses, the following section will present the research design.

A discussion of the results will be followed by concluding remarks that will include future work and policy prescriptions.

Background

Motivations for State Violations of Human Rights

Since the end of WWII and the aftermath of the Holocaust, the international human rights legal regime has grown to include the establishment of the United Nations, the drafting and adoption of the Universal Declaration of Human Rights, and dozens of legally binding and non-binding human rights treaties, conventions, protocols, and other relevant documents. The International Covenant on Civil and Political Rights (ICCPR) (and its optional protocols), followed by the International Covenant on Economic, Social, and Cultural Rights (ICESCR) entered into force in 1976 for states who had signed and ratified the documents, making governments party to the treaties legally obligated to respect, protect, and fulfill the obligations contained within the texts. Subsequent conventions continued to be drafted and adopted by UN member states, zeroing in on codifying rights protections for individuals that have been historically vulnerable: women, children, migrant workers and their families, people with disabilities, and racial minorities, among others. Treaties contained accountability and reporting mechanisms, special courts were established to try war crimes and other atrocities, and liberal-democratic norms that underpinned human rights enjoyment continued to diffuse throughout the 1990s. Yet, human rights abuses persisted in the face of the legal regime that sought to mitigate abuses. Moreover, the very events that these measures sought to prevent -- genocide and mass atrocities -- continued throughout this era and persist today, covering not only more widely known cases such as Rwanda, Bosnia, Cambodia, Gaza, Myanmar, and Ukraine, but also Timor Leste, South Sudan, Cameroon, Central African Republic, Tigray, the Yezidis in Iraq, among others (US Holocaust Memorial Museum, n.d.).

Political scientists have spent decades evaluating why governments choose to violate human rights, producing a variety of explanations. The "Law of Coercive Responsiveness" purports that when there is some sort of threat facing a particular regime, challenging the status quo often leads to repressive action by the government and its agents to quell threats (Davenport, 2007). Further, democratic institutions increase the cost of repression given that those who repress can be voted out while simultaneously providing institutionalized, legal mechanisms to engage in non-violent dissent. (ibid). More specifically, judicial independence and access to fair trials signal that checks on executive power can weaken executive overreach when it comes to repressive state violence (Hill & Jones, 2014; Keith et al., 2009; Powell & Staton, 2009). Other key domestic factors that tend to predict when a government is more likely to engage in violent repression include youth bulges (Davenport, 2007; Hill & Jones, 2014), economic factors (e.g., higher GDP, creditworthiness, oil rents, compliance with structural adjustment programs) (Clay & Digiuseppe, 2017; Davenport, 2007; DeMeritt & Young, 2013; Hill & Jones, 2014; Moore & Welch, 2015), and satisfied electorates (de Mesquita et al., 2003).

Two key theories primarily underpin explanations of why states and their agents abuse human rights: principle-agent theories and decision-making models. Principle-agent explanations of human rights abuses posits that principles, or delegators, give orders to agents, or delegatees. When applying this theory of delegation to the human rights context, delegation comes about for one of two reasons. First, motivations of the power held by the chief executive and other regime elites can lead to principles delegating to state agents to target opponents of the government. Similarly, principles can also delegate agents to target individuals who are perceived to be on the "wrong side of politics" (Mitchell, 2004). An important facet to highlight here is that the principal is not the one who is carrying out orders to commit violence against targets. Because agents are the ones carrying out violence, and not principles, this means that conditions may arise where agent's preferences are

not aligned with their principles, and as a result can lead to agency loss. When agency loss occurs, this can result in more human rights abuses when agent opt to shirk on their orders from the principles (Butler et al., 2007; Johansson & Sarwari, 2017). This may occur for several reasons: greed, survival, coercion from other groups, multiple-principal problems. These issues are often further exacerbated when state capacity, or the willingness and/or ability of a state to carry out policy and govern (Englehart, 2009), is weak. When government officials are unable to effectively monitor, compensate, or punish its agents, agency loss is more likely to occur as agents are less incentivized to act in line with principal orders (ibid).

The other primary theoretical explanation as to why governments violate human rights is the decision-making model. Rooted in political survival, this argument contends that leaders are rational and want to remain in power. As such, when executives or other regime elites are facing either real or perceived threats to their tenure, they will act in ways to minimize threats relative to their own political strength. To achieve these goals, leaders have a variety of policy options to counter threats, one of which being violent repression. Using a cost-benefit analysis, leaders will opt for policy options that will maximize their desired outcomes (Mason, 2008; Poe, 2004). While other policy options, such as accommodation, co-optation, requesting foreign aid, etc. are available, these options often tend to be perceived as more financially costly compared to repression. Further, limited state capacity and government access to resources can constrain the abilities of governments to accommodate demands of a populace, which in turn may lead some regimes to opting for repression to counter challengers who want leaders ousted from their offices (Englehart, 2009).

Preventing Human Rights Abuses

Knowing that governments often have varying degrees of motivation to engage in human rights abuses, what prevents governments from carrying out these violations? Many attribute

democracy as the primary means to prevent human rights abuses, but more specifically physical integrity rights abuses (Davenport, 2007; Davenport & Armstrong, 2004; Hill & Jones, 2014; Moore & Welch, 2015; Poe & Tate, 1994). However, there are more specific features of domestic democratic institutions that are often attributed to tempering violent state human rights abuses. In particular, domestic legal institutions should be independent from executive (or other) interference and be able to enforce both domestic and international human rights obligations to all individuals within a particular state (Powell & Staton, 2009). In turn, this means that to enforce domestic and international human rights obligations, domestic judiciaries also must be free from state interference when holding violators accountable. This speaks to a broader necessary feature of democracies that help to mitigation human rights violations: separation of powers and civil liberties (Davenport, 2007). To be truly independent would mean that a state's judiciary system would be able to hold even those within the executive accountable, which is crucial given that the executive is often the chief principal whose will may be to carry out violence against those that they deem a threat, illegitimate, or otherwise function counter to the will of the ruling government (Moore & Welch, 2015).

Those who challenge the state are less likely to be deemed as illegitimate or a threat in democracies where institutionalized forms of dissent are regularly respected. This isn't always the case, as many newer democracies that have yet to consolidate still may perceive any challenge as a threat (Davenport, 2007). Further, most democratic governments view violent dissent as wholly illegitimate (Greogory, 2009; Moore & Welch, 2015). In terms of ``legitimate dissent'', the most common form of institutionalized dissent in democratic contexts is through elections and broader empowerment rights. Here, individuals can simply challenge leadership tenure through voting out those who violate human rights or go against the will of the people. This also encompasses the ability of individuals to freely express, articulate, and share their political preferences, be it policy or

candidates. While many electoral systems are in place across a variety of democracies, Cingranelli & Filippov (2010) find that the specific combination of proportional representative systems with small district magnitude, and open list systems are most conducive for human rights outcomes. This particular system provides greater representativeness of domestic interests while simultaneously making elected officials more directly beholden to their constituents through a high district magnitude configuration. Other critical forms of institutionalized dissent include protesting, free speech and the ability to criticize public officials and/or policies, petitioning, among other actions that are often codified constitutionally.

Other key forms to safeguard human rights enjoyment center on other domestic and international accountability mechanisms. Domestic forms include the ability of civil society actors to document and share evidence of human rights abuses freely as well as critique other government injustices and the establishment of National Human Rights Institutions (NHRIs). Civil society organizations that focus on human rights, or human rights organizations (HROs), typically include some component of accountability via documenting and sharing information on human rights abuses whether the perpetrator was a state agent or private citizen. Even in the case of reporting on private human rights violations, the state is still obligated to ensure that perpetrators are held accountable. By not holding violators accountable, domestic legal systems fail to meet their obligations to uphold international human rights standards. Further, HROs often work with other like-minded organizations to extend their network and reach to educate, provide awareness, and uphold accountability for human rights in the domestic space. National Human Rights Institutes, on the other hand, are a different type of domestic institution that are established within a state and has a state goal to uphold, protect, and improve human rights at all levels within the country in which it operates (Carver, 2010; Moore & Welch, 2015).

At the international level, naming and shaming campaigns designed to call attention to human rights abuses and shame violators for engaging in these acts has been one common strategy for decades to minimize abuses in their tracks. Domestic civil society working on the ground to document, verify, and share abuses to broader audiences (e.g., other human rights stakeholders throughout the country, INGOs, IOs, and westerns governments) discuss some international accountability mechanisms + risks that incentivize HR compliance then wrap it up.

Legitimacy and Where it Comes From

One longstanding thread of political science literature that has often helped explain autocratic behavior is rooted in legitimacy. Weber (1978) conceptualizes legitimacy as having two primary components: the ways in which rulers claim their right to rule and how domestic populaces justify the leader's rule. This goes beyond simple obedience by those being ruled through material gains or fear of sanctions (Tannenberg et al., 2020; Weber, 1978). The ways in which leaders derive this rule, as originally conceptualized by Weber (1978) included three primary sources: rational-legal, traditional, and charismatic. Rational-legal forms of leader legitimation tend to be sourced from institutions, laws (or other legal norms), or other "right" policies that have already been established (Brunkert & von Soest, 2023; Tannenberg et al., 2020; Weber, 1978). Traditional legitimation, on the other hand, is rooted more in long-standing, sacred practices and customs where leaders rely on these types of institutions to claim their rule (Weber, 1978). As Tannenberg at al. (2020) note, these forms of legitimation incorporate strong elements of obedience to customary practices whereby the leader in power derives justification to rule through hierarchies and subordinates within society where these such social ladders are reinforced through deep-seed loyalty to the ruler. Finally, Weber's third classification of legitimation comes from charismatic rule. Here, these types of rulers derive their rule from the idea that these rulers possess "the exceptional sanctity of heroic qualities

or exemplary character of a person" (Weber, 341), and these qualities make this individual the most "ordained" to rule (Tannenberg et al., 2020; Weber, 1978). Since Weber's initial classification of forms of legitimacy to rule, other scholars have revised these classifications to capture more updated versions of how leaders today engage in these processes. This article utilizes the typology developed by Tannenberg et al. (2019), which still relies heavily on Weber's initial conceptualizations. While they maintain the typologies of rational-legal and charismatic, Tannenberg et al. (2019) integrates the work of David Easton (1965; 1975) to develop additional categories: performance and ideological. Easton initially conceptualized these forms of legitimacy as "diffuse" and specific", or acceptance of rule based on some sort of political meaning and "quid pro quo for the fulfilment of demands" respectively (Easton 1965: 268). Instead, Tannenberg et al. (2020) re-imagines diffuse as ideological legitimacy, or those who justify their claim to rule through political or societal ideology. These types of legitimation can center on political or economic ideology, such as nationalism or communism, as well as religious ideologies. Specific legitimation, on the other hand, focuses more on what the performance of rulers themselves. This is primarily rooted in a leader being able to legitimize their rule through their performance, or how the leader has been able to deliver on promises and governance outcomes more broadly. Finally, rather than continue to employ the term "charismatic" rule, Tannenberg et al. (2020) uses the term personalism to describe the type of rule where individuals rely on exceptional characteristics to legitimize their rule. Of note here is the authors' linking of populism to personalism. Through extensive validity testing, Tannenberg et al. (2020) finds strong evidence to suggest that populism and personalism have strong conceptual overlap. Given the rise in democratic backsliding, often attributed to the rise of the far right through populist means, this classification is useful in studying not only the ways in which leaders may combine and shift their legitimation strategies. In turn, evaluating how these strategies may be utilized by rulers to

relate with their populace will undoubtedly have implications on technology and its role in facilitating legitimation.

Theoretical Argument

What is the relationship between legitimation strategies and human rights outcomes, especially when it comes to digital rights and digital repression? Bagwell, Rains, and LaVelle (2023) found evidence to suggest that leaders who derive their legitimacy through personalist means are more likely to rely on their own unique characteristics rather than other means, namely institutions, to justify engaging in greater physical integrity rights abuses. Where institutions exist to enshrine, protect, and most notably hold violators of human rights accountable, personalist leaders are less inclined to activate or manipulate these accountability mechanisms. Rather, leaders may work to weaken these mechanisms, if necessary, while simultaneously signaling to their constituencies their disregard for human rights. Supporters, in turn, may also share preferences that human rights may pose a threat to the nation. Rejali's (2009) "civic discipline" model, which holds that there is a shared agreement among the chief executive, the state's security apparatus, and the public that the state will protect the people. If both the personalist executive and the public view human rights norms as threat to the nation, then there may be a permissive attitude of the leader to allow state security forces and even private citizens to engage in physical integrity rights abuses with impunity, especially when these preferences align. Crucial to the argument, supporters do not necessarily have to view human rights violations positively. Rather, engaging in abuses to achieve security is the underlying mechanism tying together passive abuses, personalist rule, weakening or ignoring institutions of accountability, and the "civic discipline" model.

While these mechanisms may apply to some forms of digital repression, the nature of enjoying one's digital rights may not play into the same mechanisms detailed above among the state,

its agents, and individuals' abilities to enjoy their physical integrity rights. This is particularly the case for more extreme versions of digital repression where private actors or firms are necessary to carry out digital repression. One such example involves internet shutdowns. While internet shutdowns are considered to be one of the most extreme policy options a state has at its disposal, engaging in these responses should be difficult as an agent of the state. Likely, executives themselves would be the ones to hold the ultimate power in utilizing this option, and as such would not likely be included in this theoretical framework. Further, while this could be made easier in countries where the state owns internet service providers (ISPs), the executive is assumed to have the ultimate authority when it comes to this drastic measure. Typically, there are more likely to be other forms of digital repression that occur leading up to engaging in internet shutdowns, especially ones where state agents would have more discretion to engage in such violations.

Many digital rights and forms of digital repression tend to center on another set of human rights: empowerment rights. Using the Human Rights Measurement Initiative's definition, empowerment rights refer to any rights that provide the ability of people to express themselves free and fully participate in public life (Human Rights Measurement Initiative, 2024a). Empowerment rights include rights such as the ability to engage in political participation, freedom of opinion and expression, the right to free speech, the right to peaceful assembly, freedom of religion and belief, and right to association. The enjoyment by individuals and legal obligations of state governments to respect, protect, and fulfil these rights extends into digital spaces. What has been increasingly termed as digital rights are typically the ways in which various human rights translate into digital spaces. Full digital empowerment rights enjoyment implicitly means that individuals are free to fully realize and share their full identities, to openly express themselves in digital spaces, may interact with other individuals without concern of government inference or retaliation. Digital empowerment rights

enjoyment also means that individuals have equitable access to information and scientific innovations.

Given the relationship between personalist leaders and institutions of accountability, there are reasons to believe that full enjoyment of empowerment rights pose a particular risk to these types of leaders. First, empowerment rights complement accountability mechanisms in place to hold violators accountable. In democracies, these rights function as institutionalized pathways for challenging and calling out state leaders who engage in behaviors that are counter to human rights and democratic institutions more broadly. In other words, empowerment rights often function as means to engage in legal dissent, both at the individual and collective levels. For example, the ability for one to participate in politics inherently means that an individual would be able to cast a vote against opposition, run against opposition, or campaign against opposition party members. Further, for individuals to fully enjoy their rights to assembly and association means that people can establish new political parties, organize campaign rallies, or hold peaceful demonstrations or protests to oppose politicians in power to send a message with the goal of changing some kind of policy or action of the state. To be able to effectively carry out any of these actions, the right to freedom of opinion and expression must be respected for all individuals within a given state. Further, journalists must be able to enjoy freedom of expression to report on potential government corruption, scandals, or demonstrations against a ruling government to not only inform citizens of what may be happening within their own governments, but also to bolster any movements that may align with democratic ideals.

To synthesize how personalist leadership erodes digital and physical rights enjoyment, the theoretical framework centers on three key actors and groups: personalist leaders, state agents who are beholden to the preferences of the leader, and individuals living within a particular country. When the leader's preference is to curtail mechanisms that would limit their own powers, the leader

will work to disrupt or hallow out accountability institutions as well as other channels designed to maintain checks on the executive's power. State agents, in turn, will likely be directed to carry out these orders from their principle, the chief executive. In maintaining the principal agent framework, executives and other elected officials are seen as beholden to those that elected them to power, which in makes the head of state accountable to its supporter base. Where principles don't uphold the will of its base, voters can utilize elections to hold leaders accountable and vote them out of office (Cingranelli & Filippov, 2010; Cingranelli et al., 2014). Where elected officials are voted into office based on protecting the "real" people of "the nation", electorates may vote in executives who share these preferences, regardless of these preferences including direct human rights violations. While voter bases may not explicitly request that leaders order agents to directly carry out violence against individuals within a particular state, their preferences of protecting "the nation" may involve actions on behalf of the state to carry out human rights abuses to reflect this will of a population.

Extending this framework to empowerment rights requires rethinking how institutions of accountability differ as well as how each of these groups interact with said institutions. For executives who lean more personalist, this means directing agents to counter modes of expressing dissent, as these channels for dissent are likely viewed by personalists as illegitimate due to critics utilizing these institutional channels that the personalist also does not view as legitimate to weaken the leader's power. Further, online spaces offer the abilities for those who oppose elected officials to have an instantaneous and far-reaching impact when sharing opinions or expressing negative views on said leader. The ability to engage in free speech online that criticizes the leader of a state may reach others who may have previously held positive views of a leader, or it can lead to individuals organizing in online spaces to find ways to legitimately counter the regime. In turn, this can lead to quicker development of organizations to work to challenge the state when not having to rely on

meeting in person but rather instantly reach broader audiences to elicit support for peaceful state challenges.

The space for state agents to get involved in digital empowerment rights is quite large compared to blatant physical state violence against perceived challengers. In digital spaces, state agents can, often anonymously, target those who seek to organize challenges or even just criticize the state leader. This is often done through surveilling online activity, harassing individuals online, or even making anonymous threats of violence against individuals, journalists, human rights defenders, and others. Broader, more concerted state efforts to reduce digital empowerment rights extend to state-sanctioned censorship, whereby individuals who engage in open criticism of political elite's online face potential threats of fines or arrests, which in turn fosters self-censorship of regime critics. This can include both directly messaging online critics with threats, posting threatening messages publicly, or even seeking out individuals who work for organizations that may be critical of the leader and their policies to engage in more targeted threats. Related, when ISPs or private online firms share preferences with the executive on protecting the nation at whatever cost, content moderation is another avenue through which state agents can surveil those online who engage in discourse that critiques the chief executive and their will. Conversely, those who have been targeted by either agents or private citizens online may experience a lack of accountability when reporting threats, harassment, and offline violence by perpetrators who support a personalist leader.

Other efforts that state agents can utilize include mis- or disinformation campaigns to stifle the spread of information about regime abuses or to create confusion or distrust of information disseminated online. In these cases, state agents can utilize some of the previously addressed response options, such as censorship and content moderation, and drive online content through spreading falsehoods about information pertaining to state abuses, flood the internet with other false news stories with the purpose of distracting from state violations of human rights, or disseminating

content that reiterates the views of the executive. In some states, such as Türkiye for example, there are laws on the books that are alleged to reduce the spread of mis- and disinformation, but often these policies aren't used against state agents these purposes. Instead, these policies are often weaponized against online platforms themselves and target civil society organizations, journalists, and other human rights defenders to threaten or impose heavy fines and jail sentences, often under the auspices of criticisms against the state or pro-human rights information as posing a national threat. Further, such policies often create further environments of censorship, which in turns limits the ability for individuals to engage in freedom of speech and expression.

Law enforcement aren't the only state agents that can intervene when it comes to empowerment rights enjoyment. Again, when agent preferences align with a personalist leader, particularly when it comes to bureaucrats, these preferences can trickle down into decision making that may impact empowerment rights in other ways. For example, when individuals or groups apply for permits for protests, bureaucrats may use their discretion to outright reject, impose fees, or create further hurdles for organized groups to receive permits. Other state officials, such as legislators whose preferences align with executives, may work to draft policies that create further obstacles for groups to organize protests. Law enforcement may also feel emboldened by shared preferences of a chief executive to engage in violence against protest participants with expected impunity. Law enforcement could also be more willing to overlook violence against protesters by private citizens when protesters are rallying for policies that counter the preferences of the executive and/or involve individuals perceived to not be included within “the nation" in which the chief executive privileges. Similar bureaucratic hurdles may be imposed on groups seeking to form new opposition political parties, especially when viewed as posing a real challenge to the ruling regime.

Bureaucratic and legislative hurdles may pave the way for individuals to rightfully engage in all facets of their right to political participation, specifically voting. When these groups share

preferences with leaders who oppose groups considered as outsiders to "the nation" and have the political capital to work to consolidate power on behalf of the executive, greater possibilities for voter disenfranchisement may arise. For example, at the time of this writing, the US legislature has introduced a bill titled ``The SAVE Act", which claims to target undocumented immigrants from voting, but would work to disenfranchise women, people of lower socioeconomic status, people of color, and transgender individuals. This policy reflects the chief executive's preference of consolidating political power among wealthy, white men whose beliefs align with those in power and taking away political participation from groups that have traditionally been excluded as being part of the "American people." In contexts where social hierarchical structures have been systemized, these dynamics are likely to be highly pronounced.

Finally, personalist regimes with state agents who reflect the preferences of the leaders will likely engage in many of these policies through a violation of privacy rights. Like empowerment rights, for one to fully enjoy their right to privacy means that individuals will be able to fully express who they are - especially outside of public settings. This means that individuals should not be forced to engage in self-censorship in terms of their identity, affiliations, beliefs, etc. In finding out which individuals or groups take particular issues with personalist leadership, state agents are likely to have at their discretion the ability to surveil those who challenge the ruling elites or who do not conform to the identity that comprises "the nation." In this regard, state agents have more covert pathways to target these groups in online spaces. Reports of various ways in which state agents have gone about this have ranged from law enforcement monitoring and catfishing gay men on Grindr with targeted individuals being subsequently arrested (Bureau of Democracy & Labor, 2023); Serbia has increasingly been utilizing surveillance against civil society members by using both Pegasus and Android's NoviSpy spyware (International, 2024), among numerous others.

Where personalists are vocal about the "the nation" and the "real" people who comprise it, these beliefs may signal to state agents who they should be monitoring as to not threaten national identity. Further, as directives such as these are shared across various principle-agent relationships, environments of impunity may arise. Particularly when considering physical versus digital surveillance, the ability for law enforcement to engage in digital surveillance provides significantly more covert pathways to obtain information on targets that otherwise could be revealed when relying on more physical forms of surveillance. This is increasingly more often the case as private firms, such as NSO Group, Paragon, Google, and dozens of others develop and sell malicious surveillance software to governments across the globe, both to target individuals and for military purposes. Weak regulations likely work in conjunction with state monitoring apparatuses that ensure agents follow principles' orders, where accountability mechanisms designed to curtail agents', extra-legal surveillance are inherently weakened.

However, these mechanisms also speak to the ability for agents to streamline future targeted violence. Having broader access to digital surveillance technology should mitigate indiscriminate violence that has historically been used to gather information when information asymmetries exist between the state and citizens. Rather than needing to rely on informant networks, torturing individuals who may or may not have information on particular targets, or civilian reporting, surveillance technologies not only streamline more targeted forms of repression, but they do also through substitution effects whereby state agents no longer need to engage in costlier methods to acquiring information through violence. Instead, other rights (i.e., privacy rights) are instead violated to expedite action against individuals that they state has deemed a threat.

In combining the ways in which state agents can and do utilize digital technologies and spaces to violate the rights of individuals, this inherently means that digital repression in these contexts ought to be more frequent compared to regimes where legitimacy is derived through

rational-legal means. Whereas those who derive legitimacy through rational-legal mechanisms are more likely to respect the rule of law and utilize legal channels to go after perpetrators of digital repression, personalist leaders should instead be expected to justify the use of digital repression so long as these actions support those who the leader claims to rule. The mechanisms detailed throughout this section translate cleanly into how state agents can more frequently and with impunity target individuals' empowerment rights in digital spaces. As such, I propose the following hypotheses:

Hypothesis 1: *Countries with personalist leaders are more likely to violate empowerment rights.*

Hypothesis 2: *Countries with personalist leaders are more likely to engage in privacy rights violations.*

Hypothesis 3*: Countries with personalist leaders are more likely to engage in forms of digital repression compared to states whose leaders derive rule through rational-legal means.*

Methodology

This study relies on a series of both ordinary logistic and ordinary least squares regression models. In terms of sample, the empirical analysis includes 202 countries for the years 2000-2022 where standard errors are clustered at the country level. To address issues with correlation and endogeneity, all independent variables are lagged one year. The unit of analysis is the country-year.

Dependent Variables

To test the series of hypotheses proposed, this study relies on multiple dependent variables: the rights to assembly and association, freedom of speech, electoral self-determination, non-governmental organization (NGO) freedom, and religious freedom from the CIRIGHTs data (Mark, Cingranelli, & Filippov, 2024). Each right is measured as an ordered categorical variable using scale

of 0-2, where scores of 0 indicate widespread abuses of the right and scores of 2 indicate lower levels of rights abuses. These indicators reflect the practices of governments, meaning that scores that countries receive each year are reflective of a government's actual violations this set of rights. To measure privacy rights, this study relies on the Varieties of Democracy's (V-Dem) *v2smpricon* variable, which captures the degree to which governments have established legal frameworks to protect internet users' privacy and data (Coppedge et al., 2025). This measure was converted from a categorical measure to an interval scale of -4 to 4 using a Bayesian measurement model. Finally, the variable for digital repression is an index comprised of six V-Dem indicators: privacy rights (*v2smprivcon*), government internet shutdowns in practice, *(v2smgovshut)* government internet censorship effort (*v2meceneft*), political party hate speech (*v2smpolhate*), and government dissemination of false information domestic (*v2smgovdom).* The index was developed using factor analysis with a scale of -2.7 to 1.3, where lower values indicate greater environments of digital repression and higher values reflect lower levels of digital repression. These measures were chosen because conceptually, these five areas comprise the five key means through which governments engage in digital repression. This is not to say this is an exhaustive list, but privacy rights, internet shutdowns, censorship/filtering, hate speech/harassment, and government mis- and disinformation campaigns have become increasingly salient when addressing issues of campaigns of state repression using digital means.

Independent Variables

This study assesses the ways in which leaders derive their rule, and as such, the primary independent variables of interest focus on leaders who derive their legitimacy to rule through personalist means and through rational-legal means. In keeping with the work of Tannenberg et al. (2019; 2020), this study will utilize their measures. Again, personalist leaders are those who derive

their rule as those who are "endowed with extraordinary personal characteristics and/or leadership skills" (ibid). For those who derive their rule through rational-legal means, these individuals primarily rely on the institutional legal mechanisms through which they were brought to power (i.e., elections) and govern through the institutions that provide and support executive powers (ibid). These measures were originally coded as ordinal measures but have been converted into an interval measure using a Bayesian item response theory approach, which are scaled from -3.2 to 3.5 where higher values indicate greater levels of personalism or rational legitimation.

Finally, the analysis controls for certain factors that may impact human rights outcomes. First, analysis includes a measure to account for democracy. Rather than including a measure of democracy itself, this research opts to include a variable on judicial constraints on the executive. First, as Hill (2016) finds, there should be concern for scholars who include overarching measures of democracy in analysis that also include human rights outcomes given the conceptual overlap between democracy and human rights. As such, the study chooses to use judicial constraints on the executive instead to avoid these potential modelling issues. This measure, which also comes from V-Dem, captures the degree to which an executive respects the country's constitution, laws, courts, and whether courts can function independently from the executive. This is an index comprised of five constituent variables: executive respects constitution, compliance with judiciary, compliance with high courts, and high court independence, and lower Court independence. Again, V-Dem developed this indicator through developing an index using Bayesian factor analysis. This is an interval variable ranging 0-1, where lower values indicate less respect for judicial constraints on the executive and high values greater respect towards judicial constraints. Given historical ties between democracy and human rights, it would be irresponsible to omit evaluating this relationship.

The study also accounts for the presence of conflict. Relying on the UCDP/PRIO data, this study utilizes the data to develop a count of ongoing conflicts that a country may be enduring,

including both civil and international conflict (Gleditsch et al., 2002). The study also accounts for GDP to capture state capacity as well as population.

Results

The results published in Table 4.1 below provide details of the empirical analysis that tests how personalism, rational-legal legitimation, and other covariates impact empowerment rights enjoyment. The models explore the effects of leaders who derive their legitimacy through personalist or rational-legal means across the rights to association, freedom of speech, electoral self-determination, NGO freedom, and religious freedom. Further, the results provide robust standard errors, clustering at the country levels, and includes lags across all independent variables to avoid issues with correlation and endogeneity.

Table 4.1 presents the regression output for models 1-5, demonstrating strong support across all empowerment rights underlying Hypothesis 1: compared to their rational legal counterparts, personalists are more likely to violate the rights to association and peaceful assembly, freedom of speech, electoral self-determination, non-governmental organizational freedom, and religious freedom. A one standard deviation change in personalism leads to a 0.09 decrease in right to assembly and association, a 0.10 decrease in freedom of speech, a 0.10 decrease in electoral self-determination, a 0.05 decrease in NGO freedom, and a 0.05 decrease in religious freedom.

For the most part, leaders who derive their legitimacy through rational-legal means tend to better respect each of the empowerment rights of interest (excluding electoral self-determination), but the results for rational-legal leaders are not significant across any of the outcomes of interest. Concerning control variables, these generally perform according to expectation except for GDP per capita, which frequently has a negative relationship with freedom of speech, electoral self-

Table 4.1: Regression Results for Empowerment Rights Models [10]

	Dependent Variables				
	(1) Association/ Assembly	(2) Speech	(3) Electoral S-D	(4) NGO Freedom	(5) Religious Freedom
Personalism	-0.043***	-0.050***	-0.049***	-0.023**	-0.024**
	(0.011)	(0.009)	(0.010)	(0.009)	(0.010)
Rational Legal	0.012	0.001	-0.002	0.009	0.015
	(0.014)	(0.013)	(0.014)	(0.013)	(0.014)
Judicial Constraints	0.407***	0.414***	0.505***	0.390***	0.324***
	(0.060)	(0.050)	(0.062)	(0.054)	(0.065)
Conflict	-0.028	-0.037*	-0.016	-0.044***	-0.061***
	(0.018)	(0.020)	(0.021)	(0.015)	(0.019)
GDP (logged)	0.005	-0.006	-0.005	0.004	-0.035***
	(0.008)	(0.007)	(0.008)	(0.008)	(0.008)
Population (logged)	-0.043***	-0.018*	-0.001	-0.030***	-0.000
	(0.011)	(0.010)	(0.011)	(-0.010)	(0.012)
Association	0.603***				
	(0.021)				
Speech		0.592***			
		(0.020)			
Electoral Self-Determination			0.606***		
			(0.021)		
NGO Freedom				0.788***	
				(-0.017)	
Religious Freedom					0.676***
					(0.019)
Constant	0.753***	0.555***	0.291**	0.505***	1.016***
	(0.156)	(0.131)	(0.132)	(0.117)	(0.155)
N	3,621	3,628	3,628	3,680	3,642
R-Squared	0.643	0.647	0.664	0.814	0.626

**** p<.001, ** p<0.01, *p<0.05*

determination, and religious freedom.

Regarding Models 6 and 7, Table 4.2 includes the regression output for hypotheses two and three, which contend that personalist leaders are most likely to engage in privacy rights violations as well as digital repression, respectively. Counter to expectations, there is no meaningful relationship

[10] All independent variables are lagged one year

Table 4.2: Regression Results for Privacy Rights and Digital Repression Models

	Dependent Variables	
	(1) Privacy Rights	(2) Digital Repression
Personalism	-0.003	-0.005***
	(0.002)	(0.002)
Rational Legal	0.002	-0.000
	(0.003)	(0.003)
Judicial Constraints	0.037**	-0.034***
	(0.015)	(0.013)
Conflict	-0.002	0.006
	(0.004)	(0.005)
GDP (logged)	-0.003*	0.002
	(0.002)	(0.001)
Population (logged)	0.001	0.002
	(0.002)	(0.002)
Privacy Rights	0.985***	
	(0.003)	
Digital Repression		0.977***
		(0.005)
Constant	(0.023)	-0.050***
	(0.0229)	(0.019)
N	3,633	3,731
R-Squared	0.984	0.983

**** p<.001, ** p<0.01, *p<0.05*

between privacy rights violation and legitimation strategies. While personalism and rational-legal legitimation perform in the expected directions (negative and positive, respectively), there is no statistical significance for either strategy of legitimation in terms of degree of legal privacy rights protections within a given country. Given this lack of evidence, hypothesis 2 should be rejected based on the current empirical findings. For Model 7, which tests the effect of legitimation strategy on digital repression more broadly, the results indicate that personalists are more likely to engage in campaigns of digital repression, which include policies pertaining to surveillance and privacy,

internet shutdowns, censorship and filtering, harassment/threats, and mis- and disinformation by governments. For a unit increase in personalism, there is 0.005 unit decrease in the digital repression index. Lower values on the digital repression index reflect greater levels of digital repression, so this relationship is statically significant in the expected direction. Alternatively, for a one standard deviation increase in personalism, there is an expected unit decrease in digital repression of 0.002. Although these results seem small, this is three times the average change produce from the overall sample in the regression output. The results demonstrate that while we must reject hypothesis two, there is evidence to suggest that personalist leaders are more likely compared to rational legal leaders to use digital repression against their populace.

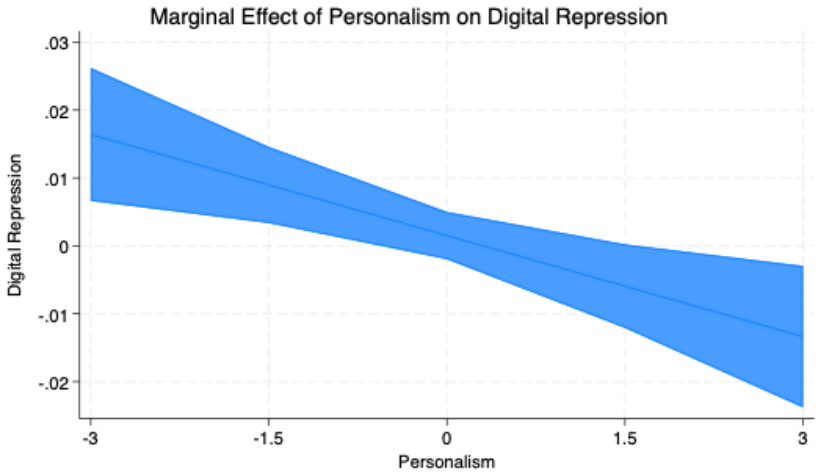

Figure 4.3: Marginal effect of personalism on digital repression

Figure 4.3 above provides data visualization of the overall effect of personalism on digital repression. As the figure demonstrates, as leaders increase in overall levels of personalism, there is a statistically negative relationship with digital repression. To reiterate, lower levels of digital repression in the data represent greater degrees of digital repression, where higher values reflect environments with less digital repression. In other words, leaders who are less personalist are less

likely to resort to digital repression, but leaders who are more personalist are more likely to engage in digital repression.

Discussion

The results from the regression analysis lends support to many of the theoretical arguments presented earlier in the article. Regarding the theoretical arguments presented for hypothesis one, which contended that personalism will erode empowerment rights protections, the evidence supports the theoretical claims. As leaders increasingly rely on some form of unique characteristic of theirs rather than other channels of legitimacy (legal institutions), empowerment rights respect diminishes. Of the five empowerment rights tested, the results were consistent across the entire group. As personalists come to and consolidate power, those who peacefully assemble to challenge the legitimacy of a personalists' rule are likely to be seen as a direct threat to their position of power. Freedom of speech and electoral self-determination work together with this context. Those who peacefully come together and challenge personalist leaders, particularly in large groups, online, at the ballot-box, and in other spaces to which individuals may express institutionalized dissent against leaders, these spaces will likely come under scrutiny by personalists. By closing spaces for expression from social movements, NGOs, religious groups, and other organizations operating to criticize and challenge personalist leaders, these individuals can continue to consolidate their rule without continued challenges. Regarding religious groups, this also lends to the theoretical argument that if members of religious groups are considered as an out-group in a particular nation, then their abilities to enjoy their right to religious freedom will be diminished. To restrict the enjoyment of these rights, personalists are more inclined to rely on gutting institutions that operate to document and maintain accountability of individuals within a state who violate human rights, particularly state agents. These results are consistent with the findings of (Bagwell et al., 2023), which also argue that

personalists tend to seek ways to gut and hallow out domestic accountability mechanisms for human rights while simultaneously relying on state agents to continue carrying out the will of the executive, in line with principle-agent arguments. Further, this bolsters the claims and results from (Bagwell et al., 2023), in that the authors contend that these institutions of accountability function to hold state violators accountable, in turn resulting in the government wanting to halt any unwanted narratives from the public (ibid, 7). By finding consistent and strong support that personalist leaders work to erode empowerment rights, particularly assembly and association, freedom of speech, and NGO freedom, these results strengthen those arguments and lend further support to the overarching claim that personalist leaders tend to weaken human rights protections and enjoyment overall.

Regarding the digital components of the argument, one point should be evident: empowerment rights are also largely enjoyed in digital spaces. As such, finding evidence to support the claim that empowerment rights enjoyment become more vulnerable under personalist leadership should inherently be the first step in exploring the relationship between leadership legitimation strategies and digital human rights. Surprisingly, this study did not find evidence to support the argument that personalist rule will have a negative impact on privacy rights. One possible explanation is that privacy rights, especially governed in online spaces, are generally lacking across the globe. Privacy rights are often protected in some areas sectors such as healthcare, financial and education, but as is often the case, policymaking on topics that quickly evolve often mean that the laws have not caught up to other areas. Expansion of artificial intelligence, development, evolution, and rapid diffusion of surveillance technology, weak transparency mechanisms, and government motivations to hide unlawful privacy rights all play into massive gaps in effective privacy policies. In turn, this means that drafting passage of relevant policies - even under non-personalist regimes - are lacking.

Another possible explanation could be that the rise in national security concerns since 9/11 have led to policymakers and governments across the globe to preference the expansion of state surveillance practices for the purpose of preventing terrorism, reducing crime, and for other law enforcement purposes over providing strong privacy protections for individuals living within a given border. There is an extensive literature that argues that in the face of national crises (e.g., terrorism, other crises), citizens often prefer governments to engage in securitization of the state at the expense of various civil rights (Huddy et al., 2005; Piazza, 2023). Pairing this explanation with various crises that have occurred since, including the 2008 housing crash, the Covid-19 pandemic, various conflicts and subsequent migration, some parties have utilized some of these crises to justify further expansions into privacy rights violations to improve national security outcomes. For example, several countries have been recently integrating AI and other invasive policies towards immigrants and other visitors coming into borders of foreign states. Some tactics include requiring foreign nationals to submit to biometric data collection, providing social media account information, and even scanning contents on personal devices. In these contexts, not only have relevant policies been lagging, but some leaders and political parties tend to have the propensity to take advantage of certain crises to justify invasive data collection practices in the name of national security.

Although privacy rights on their own do not have a statistically significant relationship with personalists, digital repression more broadly does. The results demonstrate that personalists tend to perform worse on a set of rights that comprise digital repression. The rights that comprise the digital repression index centered on internet shutdowns, privacy, censorship and filtering, government harassment and threats, and government programs of mis- and disinformation. While this study was more interested in digital repression, future work will need to further investigate how various types of legitimation strategies impact the constituent components that comprise this index, including how ideological and traditional forms of legitimacy.

Conclusion

This study sought to address the question of how legitimation strategies, namely personalism and rational-legal, impact digital rights, particularly empowerment rights, privacy rights, and digital repression more broadly. Through employment a series of ordinary least square models, the results provided evidence to suggest that leaders who derive their legitimacy through personalist means tend to produce negative outcomes for empowerment rights enjoyment. Personalism - those who derive their legitimacy to rule through their own unique characteristics - leads to a deterioration of freedom to engage in peaceful assembly and association, speech, electoral self-determination, NGO freedom, and religious freedom. Empowerment rights, which are increasingly expressed in online spaces, are a key mechanism through which a populace can openly engage in various forms of dissent and criticism of a state's leader. Those seeking to peacefully protest and criticize a personalist leader inherently call attention to various policies, especially those that infringe on human rights enjoyment. Moreover, through these institutionalized mechanisms of dissent function to hold leaders accountable via calling attention to injustices carried out on personalist leadership. NGOs, too, work to hold human rights violators accountable through the documentation and sharing of information on human rights violations, education individuals on human rights, and working with relevant stakeholders in a given state to improve human rights outcomes. Finally, religious freedom, which may also function to hold personalist leaders accountable, may also diminish under attack when leaders who rule for a particular "people" may also view religious "outsiders" as a threat to their rule and broader national identity. Empowerment rights, across the board, function as institutionalized mechanisms of dissent, which inherently are viewed by personalists as illegitimate as these mechanisms challenge their power and have nothing to do with their own legitimacy to rule within a state. Because these also function in various ways as checks on power, personalists will

work to reduce accountability structures that may temper their rule, in turn, reducing empowerment rights enjoyment.

Although there was no evidence to demonstrate a relationship between privacy rights and personalist rule, there was evidence pointing towards a strong relationship between increasing personalist rule and greater degrees of digital repression. In this study, digital repression included the following five components: privacy rights, internet shutdowns, censorship and content filtering, political hate speech and harassment, and domestic government-led campaigns of mis- and disinformation. Each mechanism within the index used within this study has strong theoretical links to why personalists may rely more heavily on digital repression as a policy tools. While privacy rights on their own did not have a statistically significant relationship with personalism, it did as a component of the digital rights index.

Other questions remain on exploring the links between legitimation strategies and digital rights/repression. First, while one goal of this study was to establish baseline relationship between two of the predominate forms of legitimation, there is reason to believe that leaders may be characterized as relying on more than one form of legitimation to justify their rule. As such, exploring these typologies on much more depth is warranted to continue expanding on our understanding of the relationships between legitimation and human rights enjoyment more broadly. Additionally, given the lack of evidence supporting hypothesis two - the relationship between legitimation strategies and privacy rights - more work needs to be done to better understand the relationship between privacy rights and legitimation.

References

Alarón, Á. (2024). "Venezuela's many means of surveillance and control." Access Now URL: https://www.accessnow.org/the-many-means-of-surveillance-and-control-in-venezuela/

Amnesty International. (2024). "Venezuela: Tech companies set dangerous precedent with app for reporting anti-government protesters." Amnesty International. URL: https://www.amnesty.org/en/latest/news/2024/08/venezuela-tech-companies-set-dangerous-precedent-with-app-for-reporting-anti-government-protesters/

Amnesty International. (2025a). "The human cost of the repressive cooperation between the us and El Salvador." Amnesty International. URL: https://www.amnesty.org/en/latest/news/2025/04/la-cooperacion-represiva-entre-eeuu-y-el-salvador/

Amnesty International. (2025b). "Iran: Authorities target women's rights activists with arbitrary arrest, flogging and death penalty." Amnesty International URL: https://www.amnesty.org/en/latest/news/2025/03/iran-authorities-target-womens-rights-activists-with-arbitrary-arrest-flogging-and-death-penalty/

Amnesty International. (2024). "Serbia: "a digital prison": Surveillance and the suppression of civil society in Serbia." Amnesty International. URL: https://www.amnesty.org/en/documents/eur70/8813/2024/en/

Amnesty International. (2025c). "USA: Deployment of national guard to Los Angelas in response to ICE raids is dangerous." Amnesty International. URL: https://www.amnesty.org/en/latest/news/2025/06/usa-response-to-ice-raids-is-dangerous/

Bagwell, S., Rains, M., & LaVelle, M. (2023). "Of one's own making: Leadership legitimation strategy and human rights." Journal of Conflict Resolution, 68 (10), 1994–2018. https://doi.org/https://doi.org/10.1177/00220027231220006

Brunkert, L., & von Soest, C. (2023). "Praising the leader: Personalist legitimation strategies and the deterioration of executive constraints." Democratization, 30 (3), 419–439.

Bureau of Democracy, Human Rights, & Labor. (2023). "2023 country reports on human rights practices: Egypt." United States Department of State URL: https://www.state.gov/reports/2023- country-reports-on-human-rights-practices/egypt/

Butler, C. K., Gluch, T., & Mitchell, N. J. (2007). "Security forces and sexual violence: A cross-national analysis of a principal-agent arguments." Journal of Peace Research, 44 (6), 669–687.

Carver, R. J. (2010). "A new answer to an old question: National human rights institutions and the domestication of international law." Human Rights Law Review, 10 (1), 1–32.

Cingranelli, D., Fajardo-Heyward, P., & Filippov, M. (2014). "Principals, agents and human rights." British Journal of Political Science, 44 (3), 605–30.

Cingranelli, D., & Filippov, M. (2010). "Electoral rules and incentives to protect human rights." The Journal of Politics, 72 (1), 243–57.

Clay, K. C., & Digiuseppe, M. R. (2017)." The physical consequences of fiscal flexibility: Sovereign credit and physical integrity rights." British Journal of Political Science, 47 (4), 783–807.

Coppedge, M., Gerring, J., Knutsen, C. H., Lindberg, S. I., Teorell, J., Altman, D., Angiolillo, F., Bernhard, M., Cornell, A., Fish, M. S., Fox, L., Gastaldi, L., Gjerløw, H., Glynn, A., God, A. G., Grahn, S.,Hicken, A., Kinzelbach, K., Krusell, J., Ziblatt., D. (2025). "V-dem codebook v15 varieties of democracy (v-dem) project." Varieties of Democracy. https://doi.org/https://doi.org/10.23696/vdemds25

Council on Foreign Relations. (2024). "India's Muslims: An increasingly marginalized population." Council on Foreign Relations URL: https://www.cfr.org/backgrounder/india-muslims-marginalized-population-bjp-modi

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

Davenport, C., & Armstrong, D. A. (2004). "Democracy and the violation of human rights: A statistical analysis from 1976 to 1996." American Journal of Political Science, 48 (3), 538–554.

de Mesquita, B. B., Smith, A., Siverson, R. M., & Morrow, J. D. (2003). The Logic of Political Survival. MIT Press.

DeMeritt, J. H. R., & Young, J. K. (2013). "A political economy of human rights: Oil, natural gas, and state incentives to repress." Conflict Management and Peace Science, 30 (2), 99–120.

Englehart, N. A. (2009). "State capacity, state failure, and human rights." Journal of Peace Research, 46 (2),163–180.

Gleditsch, N. P., Wallensteen, P., Eriksson, M., Sollenberg, M., & Strand., H. (2002). "Armed conflict 1946-2001: A new dataset." Journal of Peace Research, 39 (5), 615–37.

Greogory, P. R. (2009). Terror by quota: State security from Lenin to Stalin (An archival Study). Yale University Press.

Hill, D. W., & Jones, Z. M. (2014). "An empirical evaluation of explanations for state repression." American Political Science Review, 108 (3), 661–687.

Huddy, L., Feldman, S., Taber, C., & Lahav, G. (2005). "Threat, anxiety, and support of antiterrorism policies." American Journal of Political Science, 49 (3), 593–608.

Human Rights Measurement Initiative. (2024). Empowerment. URL: https://rightstracker.org/metric/empowerment

Human Rights Measurement Initiative. (2024a). "India - safety from the state." Human Rights Measurement Initiative URL: https://rightstracker.org/country/IND?tab=report-physint

Human Rights Measurement Initiative. (2024b). "United States – safety from the state." Human Rights Measurement Initiative. URL: https://rightstracker.org/country/USA?tab=report-physint

Human Rights Watch. (2024). "India: Increased violence, harassment against minorities." Human Rights Watch. URL: https://www.hrw.org/news/2025/01/16/india-increased-violence-harassment-against-minorities

Idea International. (2025). "The Global State of Democracy 2024." Idea International, URL: https://www.idea.int/gsod/2024/

Johansson, K., & Sarwari, M. (2017). "Sexual violence and biased military interventions in civil conflict." Conflict Management and Peace Science, 36 (5), 469–493.

Keith, L. C., Neil, C. T., & Poe, S. C. (2009). "Is the law a mere parchment barrier to human rights abuse?" The Journal of Politics, 71 (62), 644–60.

Levitsky, S., & Way, L. (2020). "The new competitive authoritarianism." Journal of Democracy, 30 (1), 51–65.

Mason, T. D. (2008). Caught in the Crossfire: Revolution, Repression, and the Rational Peasant. Rowman Littlefield Publishers, Inc.

Mitchell, N. J. (2004). Agents of Atrocity: Leaders, Followers, and the Violation of Human Rights in Civil War. Palgrave Macmillian.

Moore, W. H. (1998). "Repression and dissent: Substitution, context and timing." American Journal of Political Science, 42 (3), 16–42.

Moore, W. H., & Welch, R. M. (2015). "Why do governments abuse human rights?" Emerging Trends, 1–16.

Piazza, J. (2023). "Fear of terrorism and support for non-democratic rule in democracies." International Interactions, 49 (4), 587–611.

Poe, S. C. (2004). Understanding human rights violations. Ashgate.

Poe, S. C., & Tate, C. N. (1994). Repression of human rights to personal integrity in the 1980s: A global analysis. American Political Science Review, 88 (4), 853–872.

Powell, E. J., & Staton, J. K. (2009). Domestic judicial institutions and human rights treaty violation. International Studies Quarterly, 53 (1), 149–174.

Ritter, E. H., & Conrad, C. R. (2016). Preventing and responding to dissent: The observational challenges of explaining strategic repression. American Political Science Review, 110 (1), 85–99.

Sequera, V., & Guanipa, M. (2024). "Venezuela launches investigation against opposition leaders amid protest crackdown." Reuters, URL: https://www.reuters.com/world/americas/maduro-security-forces-round-up-venezuelans-involved-protests-operation-knock-2024-08-05/

Mark, S., Cingranelli, D., & Filippov, M. (2024). "Cirights: Quantifying respect for all human rights." Human Rights Quarterly, 46 (2), 264–286.

Tannenberg, M., Bernhard, M., Gerschewski, J., Lührmann, A., & von Soest, C. (2020). "Claiming the right to rule: Regime legitimation strategies from 1900 to 2019." European Political Science Review, 13 (1),77–94. https://doi.org/https://doi.org/10.1017/S1755773920000363

UN News. (2024). "Iran: Repression of women 'intensifying', two years on from mass protests." United Nations News, URL: https://news.un.org/en/story/2024/09/1154306

US Department of State. (2024). "2023 country reports on human rights practices: Egypt." United States Department of State, URL: https://www.state.gov/reports/2023-country-reports-on-human-rights-practices/egypt/

US Holocaust Memorial Museum. (n.d.). "Country case studies." US Holocaust Memorial Museum, URL: https://www.ushmm.org/genocide-prevention/countries

Varieties of Democracy. (2025). "Democracy report 2025: 25 years of autocratization - democracy trumped?" Varieties of Democracy, URL: https://v-dem.net/documents/61/v-dem-dr 2025 lowres v2.pdf

Weber, M. (1978). Economy and society: An outline of interpretive sociology. University of California Press.

Conclusion: Revisiting Motivations, Key Findings, and Future Work

This dissertation focused on improving collective understandings of the relationships between digital technologies, government repression involving digital technologies, and how human rights (including digital rights) have been impacted during the latter parts of the information era. Digital repression, or the ways in which governments rely on technology to facilitate repression, has been increasingly on the rise. These strategies carried out by governments all over have shifted the trajectory of how repression has been traditionally carried out. With global data demonstrating a clear pattern that democratic deficits are spreading, the result has been a rise in authoritarianism, illiberalism, and extreme populism. Through having rapidly evolving technology, these hardline, often nationalist, leaders have more expedient tools to carry out campaigns of human rights violation than ever.

Chapter 2, which first explored the relationship between mass mobilization, transnational shaming, state capacity, with internet shutdowns, found substantial evidence to support the theoretical propositions asserted. First, mass mobilization, which refers to non-violent protests, demonstrations, and other peaceful dissent events, does have a statistically significant relationship with internet shutdowns. As these movements grow in number and participation, these elements attract attention from the state, which has incentives to hide information surrounding the protests. For one, to have a global audience witness increasing levels of dissatisfaction with a government, could be perceived as weakness on the part of the ruling government. To be able to have higher degrees of mass mobilization implies that there must be institutionalized channels to legally engage in dissent, which means some level of democracy exists within a mobilizing context. However, even smaller demonstrations can attract the attention of outside observers, being enough to trigger state-

sanctioned shutdowns to varying degrees. When including the role of transnational advocacy network shaming, which typically involves publicizing political violence carried out by a state and its agents, there is also evidence to suggest that this relationship matters: as more attention is being drawn to human rights abuse by offending states, this could lead to other undesirable outcomes for repressing regimes. For both situations, there is motivation for governments to shut down the internet or block other communication services and apps. When considering how TAN shaming and mass mobilization may interact to elicit government responses of shutdowns, there is also evidence of a relationship established. Specifically, when mass mobilizations are gaining traction but haven't reached their maximum levels of frequency or support, an increase in TAN shaming has a significant effect on the rate of internet shutdowns ordered by a government. Regarding state capacity, it is argued that states with the ability to carry out policy and govern should have a strong bearing on carrying out internet and other telecoms shutdowns when faced with a thriving civil society. The role of civil society – regardless of ability to overcome collective actions problems and mobilize – is still crucial to documenting, monitoring, educating, and engaging in community outreach across various types of human rights issues. The results from the negative binomial model indicate that there is a conditional relationship: when state capacity is lower (i.e., governments are unable to effectively govern, carry out effective policy, and in turn do not have the infrastructure or capabilities to ensure that citizens are protections against human rights abuses), and civil society is thriving, governments are more inclined to rely on internet shutdowns. However, as state capacity increases and the ability of civil society to flourish decreases, so does the rate of internet shutdowns ordered by political elites. Finally, the study also evaluated the argument that governments that have previously relied on internet shutdowns will do so again. The results suggest that governments that have used a shutdown within the previous six months are more likely to do so again. This is also a key finding in

that there are crucial short-term impacts of internet and other telecommunication shutdowns that can necessarily be studied at a country-year level.

Chapter 3 continued to explore the role of internet shutdowns by asking how governments decide between competing campaigns of digital repression. The main motivation for the chapter centers on the idea that governments clearly rely on another key form of digital repression: surveillance and monitoring. However, in contexts where internet shutdowns are used frequently, relying on surveillance approaches when the internet is not available could pose issues with governments who seek out individuals they deem threats to a regime. The article approached this question through integrating to core strands of literature: the repression-dissent literature, specifically the dynamics of substitution and complementarity, and the growing literature on digital technology in political violence. Substitution is the idea that governments, when faced with political contention, have multiple ways in which they can respond to continued dissent. Governments may try one strategy or a set of tactics to address demands and find that they will have to alter their response. When government swap out one response option for another, this is referred to as substitution. Complementary would mean that governments add in another repression or other policy response to "complement" ongoing methods of addressing discontent. The main arguments presented within this chapter are the following: where demands are widespread, mobilization is growing and widespread, governments are more inclined to rely on surveillance-based approaching, surveilling and collecting information on individuals who the regimes perceive as a threat or opposition. In turn, when governments rely on surveillance-based approaches to engage in targeted repression, this reduces the overall appearance of violent repression. Reducing this overall image was a key focus of Chapter 3 where governments have incentives to reduce the appearance of or hide mass violence. Alternatively, if governments are faced with situational, sporadic opposition movements they may opt for a swifter response: internet shutdowns. Here, governments can shut

off the internet and make it to where information on violent repression is difficult to share beyond the specific area to outside audiences. With the internet shutdown, the regime having control over information flows, and the ability to hide evidence of mass violence, this could lead to greater levels of human rights abuses. While initial results pointed to evidence that may have supported two of the four hypotheses, other statistics from the two sets of SUR models provide evidence that better modelling needs to be carried out in a future study as the main assumptions of the model, correlated error terms between the models, was unsubstantiated. Despite the poor fit of the model, the results for the hypothesis on greater mobilization leading to more surveillance were consistent with other findings within this dissertation project that evaluate mass mobilization's relationship with other forms of digital repression. Additionally, evidence here suggests that at certain levels of mass mobilization and internet shutdowns, governments do carry out greater levels of human rights abuses. While counter to the expectations of the argument, the results also point to and interactive effect between mass mobilization and surveillance on violent repression: as mass mobilization and surveillance (of social media) both increase, so does the probability that violent human rights abuses will be carried out by the state. While there is certainly much more work to be done on this topic, one key take away from this chapter was the need for qualitative approaches to parse out how these strategies are substituted and complemented over time. While detailing the case of Venezuela throughout the chapter, there may be an argument for approaching this type of study from a sequencing angle. In other words, through analyzing this case, there is reason to believe that internet shutdowns may be an early digital strategy for some states, and over time they adopt other surveillance type approaches as well as become more targeted with internet shutdowns and other reduced-connectivity events.

The final chapter of the dissertation shifts focus to the evaluating the type of leaders that are most likely to use digital repression. Authoritarians all over are increasingly prone to using digital

means to repress, but this chapter explores this question through the lens of legitimation, or the ways in which leaders derive the legitimacy of their rule. The study ties in the relationship between empowerment rights as digital rights, privacy rights, and digital repression, on one hand, and how two key types of legitimation may impact this group of rights: rational legal legitimation and personalist legitimation. Leaders who derive their legitimacy through rational-legal means are those who are elected to office through legal and normalized means. This is typically the way in which democratically elected officials are elected, assuming that elections are free, free, regular, and competitive. Personalists may come to power through elections or other institutional means, but that is not how they derive their legitimacy. Typically, these leaders rely on their own merits, characteristics, or other traits that they believe deem them to be a "true" leader – the leader that is the only one who can lead a government. These leaders are more likely to ignore, neutralize, or destroy institutions that would hold them accountable for their behavior, which again, they justify through their own unique characteristics as being the most effective way to rule a country. For both types of legitimation, it is important to note that not only do the leaders themselves have to find these methods legitimate, but so do their populaces.

Regarding empowerment rights, the motivation for including these types of rights is that many of these rights underpin the enjoyment of these rights online: freedom of opinion and expression, right to political participation, assembly and association, and freedom of religion. Without government's fulfilling their obligations to respect, protect, and fulfil these rights, being able to fully express someone's thoughts, which are often exercised in online/digital spaces, then digital rights would largely take a hit. Digital rights are the human rights as expressed, enjoyed, and protected in digital spaces.

In tying the two together, personalist leaders often campaign on being the best suited person to rule a country, especially for the "real people" of that country. This means that those who do not

fit into these definitions are often excluded and marginalized, often including minority ethnic, racial, and religious groups, women, LGBTIA+ individuals, unions, people with disabilities, civil society and other human rights defenders, watchdogs, among others. These individuals, who the leader may also see as a threat to their power, also often become targets of the regime. The leader may send signals to their agents to monitor government critics, those who threaten the "national identity". One key area that this impacts in these contexts is empowerment rights. When individuals are increasingly excluded from political, social, economic, and cultural spheres, it is not uncommon, especially in more democratic regimes, to express discontent and criticize the government and their policies. Moreover, assembling protests to send messages of disapproval and to make demands of the government because increasingly popular to demand change to personalist status quo.

Given that personalists would see these acts as a challenge to what they perceive as their legitimate rule, personalists should be more likely to go after empowerment rights and privacy rights to deter and quash dissent. Further, given the continued expansion of digital repression, it was argued in Chapter 4 that personalist leaders, for the reasons above, should be more inclined to use digital repression as part of their response to domestic challenges. The results of the OLS model point to evidence consistent with these arguments: personalist leaders are more likely, compared to rational-legal leaders, to violate the rights to assembly and association, freedom of speech, right to electoral self-determination, NGO freedom, and religious freedom. Moreover, they are more likely to engage in digital repression. The results did not provide evidence to support the claim that personalist leaders are more likely than rational-legal leaders to violate privacy rights. While this was a surprising finding, more work needs to be done to fully understand why.

This dissertation sought to contribute to the literatures on human rights, digital rights, digital repression, and political violence. The literatures on digital rights and digital repression are rapidly growing literatures, there is much more to be studied. While this one project helps contribute to our

collective knowledge on these topics, it has also illuminated more meaningful ways to approach digital repression. One consistent challenge throughout these studies is data availability. When conducting studies on privacy rights, it is apparent that there is limited data available on privacy rights in general. These gaps are even more glaring when measuring practices on how governments violate privacy practices. One clear avenue is to urge other scholars in the field to continue working on the issues of privacy rights and government surveillance and how we can develop valid measures on these concepts.

Outside of the vast data limitations, this project also contributes the message that a shift towards the sequencing of campaigns of digital repression occur. These tactics don't happen in a vacuum – there are clear dynamics and constraints, both internally and abroad, that factor in a governments' decision making of how to maximize its preference through digital means. From some of the case studies included, there seemed to be a pattern of lower-level uses of surveillance, shifts to internet and telecommunications shutdowns, and then a shift to widespread surveillance and monitoring with targeted violence. This could explain the lack of evidence to support some of the claims throughout this dissertation, namely that surveillance and reduced connectivity aren't necessarily substitutions of one another but rather can work complement one another to produce outcomes reflecting a government's preference.

This project has also produced several policy implications. First, while outside of the scope of the dissertation, there is a clear need for stronger, more meaningful private rights protections. Having strong monitoring mechanisms to institutionalize respect for privacy rights is a clear need. It is likely that governments everywhere violate peoples' rights to privacy. Having strong laws to protect privacy rights and effective domestic judicial institutions to enforce these policies are crucial for the enjoyment of privacy rights. And although the right to privacy is codified in the International Covenant on Civil and Political Rights, the monitoring and enforcement mechanisms behind the

treaty have clearly not been enough. Strong, domestic policies are crucial. Governments who work to protect the privacy of individuals within their borders must continue or start to engage with digital rights civil society organizations, ethical technologists, and legal firms that focus on privacy. Moreover, while strong privacy policies may be condemned by tech firms, governments that are serious about wanting to ensure privacy rights for all must give preference to the people within its borders rather than corporate profits.

Regarding internet shutdowns, one trend that has become evident is that governments who utilize internet shutdowns and other communications disruptions have gradually transitioned from using more national level blackouts to more targeted, local disruptions. While many governments that are repeat offenders of internet shutdowns have relied on national or regional level shutdowns, states such as India and Myanmar have shifted to utilizing more targeted, village or township level internet shutdowns. More attention needs to be given to governments who weaponize communications technologies in these ways, as well as other international telecommunications firms from outside countries that choose to operate within the borders of a highly repressive country.

Finally, policy makers should consider developing legal protections to prevent governments from using internet shutdowns as a policy option, whether a state has previously used internet shutdowns or other telecoms disruptions, if it seems to be at risk for doing so, or if it has never utilized one. As has been discussed in earlier chapters, democratic backsliding has been a global trend for years now and working to prevent this type of unilateral control via policy, executive orders, threats or other coercion carried out by regime elites against telecom companies and ISPs, or other forms of corruptions that could influence communication or social media companies to comply shutdown, monitoring, or censorship requests. Having effective policies on the books with an effective judiciary could prevent this from being a broader global trend.

There is an incredible amount of work to be done on the intersection of digital technologies, human rights, and political violence. This dissertation is rooted in the dire need for strong domestic institutions to hold governments accountable with digital abuses. However, the reality is that many states are still lagging on codifying or updating domestic laws surrounding digital repression. Concerning privacy, most states have a long road ahead to implementing policies that will protect citizens from government monitoring and surveillance, capitalizing off selling data, removal of personal data in unwanted online spaces, doxxing, scraping data to train AI systems, and so much more. Compounding this issue is the lack of digital literacy. There are countless cases throughout the world where individuals simply don't have access to knowledge or how digital technologies, privacy rights violations, among other challenges can impact them or their communities. The is also real need to provide education on how digital technologies can be used and abused by governments and other relevant actors to harm individuals, groups, communities, and clearly entire countries. Through expanding efforts to reach rural areas, hard to reach groups, and start educating people on the risks of government digital abuse, this can empower more people to come together and make the demands for governments everywhere to engage in meaningful, human rights-centered change.