5-2020

Flipping the Kill-Switch: Why Governments Shut Down the Internet

Elizabeth Sutterlin

Flipping the Kill-Switch: Why Governments Shut Down the Internet

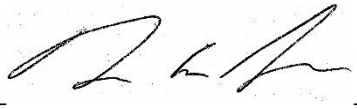
A thesis submitted in partial fulfillment of the requirement
for the degree of Bachelor of Arts in International Relations from
The College of William and Mary

by

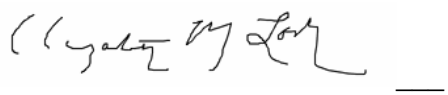
Elizabeth K. Sutterlin

Accepted for _____Honors_____
(Honors)

_____
Philip Roessler, Director



_____
Dennis Smith



_____
Elizabeth Losh

Williamsburg, VA
May 5, 2020

Table of Contents

Acknowledgments

First, I would like to thank Professor Roessler for his advice and support throughout this project. The shape of this thesis has changed significantly since its inception in the fall, and it would not have been possible to pivot this project successfully without his support.

I want to thank the other members of my committee for their support and feedback on this project as well. This remote semester has certainly changed a lot of things, but I can't overstate how much I appreciate your willingness to see this thesis in a new format.

I would also like to thank Peter Micek and the rest of his team at AccessNow for sharing their dataset with me. The information they compile on internet shutdowns globally made this thesis possible, but more importantly, their organization and the #KeepItOn campaign are doing incredible work bringing the truth to light about digital repression and refusing to allow online activists to be silenced.

I also want to give a big thank-you to Steven for his help troubleshooting (and to some extent teaching) Stata, as well as his help and advice on general econometrics questions. I am so grateful for your patience and willingness to lend a helping hand whenever I needed it. If not for you, I would probably still be getting error messages and browsing Stata online help forums for answers to very basic questions.

I am also eternally grateful to Liz Rosen for the huge amount of help, feedback, and support she has provided to me throughout this whole project! Liz, your comments always challenge me to improve my work and that has made this work so much better than it would have been otherwise. I always looked forward to our weekly meetings in front of The Daily Grind, both as a way to keep me honest and actually make progress each week, as well as just an opportunity to catch up with a great friend.

I can't express just how grateful I also am for the entirety of the PIPS family. This thesis grew out of my project last year, and it was thanks to the other fellows and the incredible mentors I had through PIPS that I was encouraged to explore my interests and really dive in to studies of technology and international security. The research experiences I've had throughout my four years at William & Mary have enriched my life in countless ways, and I have PIPS to thank for that.

Finally, I would like to thank the rest of my family and friends for supporting me throughout this process. This thesis has been many months and cups of coffee in the making, and the support and love I received whenever I doubted myself was what got me through to this point, many pages later. A special thank you goes to my parents for the time and space needed to make the final push of this project in the midst of a global pandemic.

Grandmom, I'm sad you won't be able to read this thesis cover to cover, but the way your face would light up whenever I talked about my project this year made me so happy. It gave me the drive to keep going. I love and miss you.

Abstract

In the last decade, governments have begun more frequently cutting internet and mobile services as a response to real or potential threats. Both democratic and autocratic regimes use internet shutdowns to maintain security and suppress dissent. Why do governments intentionally shut down the internet? This paper focuses on complete blackouts of online communications, known as "kill-switch" shutdowns, and examines the factors that contribute to a regime's choice to enact such extreme measures. Using a mixed-methods analysis, this paper evaluates multiple potential causes of internet shutdowns. Results from both cross-national, quantitative analysis and qualitative process tracing present several findings. First, government internet shutdowns follow a strong path dependency: once a government enacts a shutdown, the chances they will do so again are high. Second, there is surprisingly no apparent link between violent protest and internet shutdowns. This thesis finds strong support, on the other hand, for violent conflict and competitive elections as factors that lead governments to shut down internet services. Finally, this paper finds a negative relationship between U.S. foreign assistance and internet shutdowns in the data, suggesting that greater linkages with the West may be a way to curb government-mandated internet shutdowns in the future.

1. Introduction

On January 27th, 2011, in response to widespread anti-government protest, Egypt's internet went dark. Activists and journalists who had documented the protests in the center of Cairo and received worldwide support through Twitter lost the ability to connect and communicate. The internet had not been censored; it had been cut entirely. This was not the first time a country had cut off internet services in response to political unrest. Shutdowns of this kind had occurred in Nepal in 2005 and Myanmar in 2007. But Egypt's response to the Arab Spring marked the first time the world had closely watched a revolution organized and executed online, and it was in this context that the world watched a government quickly and effectively snuff out a mode of communication and mobilization.

Since 2011, governments across the world have used internet "kill-switch" tactics to try to dampen protests, silence political opposition, and undercut armed rebellions. Despite this rapid growth in government-mandated internet shutdowns, there is little scholarly consensus on why and when governments shut down the internet. This paper aims to address these questions. The answers to these questions are of great importance as the internet continues to play a central role in the social, economic, and political lives of people around the world. In addition to implications for human rights and free speech, internet shutdowns can also have debilitating economic effects, especially with growing dependence on digital technology for global trade, services, and financial transactions. Internet shutdowns threaten democratization and harm governance, but the economic fallout poses its own threat to sustainable development as shutdowns become more commonplace.[1]

[1] Tonderayi Mukeredzi, "Uproar over Internet Shutdowns: Governments Cite Incitements to Violence, Exam Cheating, and Hate Speech," *Africa Renewal: Africa Section of the UN Department of Public Information, August – November 2017*, August 21, 2017, https://www.jpanafrican.org/docs/vol10no10/10.10-3-Mukeredzi.pdf

Despite a 2015 United Nations declaration that established Internet kill-switch shutdowns as violations of international human rights law, even in times of conflict,[2] governments have not refrained from continuing to use them to curb protests and prevent opposition coordination around elections. In the last decade, a growing number of states, autocracies and democracies alike, have opted to conduct internet shutdowns instead of or in addition to internet filtering (content censorship) tactics. Only one internet kill-switch shutdown was recorded in 2011, but that number had risen to 173 by 2019.[3] Table 1 on the following page provides an overview of countries that have enacted shutdowns in these years. Given the growing popularity of internet shutdowns as a policy option, as one scholar puts it, "today's extreme case may become tomorrow's typical case—or be surpassed by a more repressive regime intent on testing the effectiveness of frequent information blackouts."[4]

I argue in this thesis that certain factors may affect the willingness of governments to carry out a kill-switch shutdown, including conflict, protests, proximity to elections, population demographics, internet infrastructure, and international linkages with the United States. I first test these hypotheses through OLS regressions using a novel and detailed dataset of internet shutdowns from Access Now, an NGO that tracks internet censorship.[5] I find ongoing armed conflict to be the strongest predictor of an internet shutdown in all my models; however, the occurrence of violent protest had surprisingly little effect. Competitive elections are associated with a higher *number* of internet shutdowns, but do not necessarily make them more likely to

---

[2] United Nations Office of the High Commissioner of Human Rights, "Joint Declaration on Freedom of Expression and responses to conflict situations," *United Nations Office of the High Commissioner of Human Rights*, May 4, 2015, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=15921&Lang__ID=E

[3] Deji Bryce Olukotun and Peter Micek, "Shutdown Tracker Optimization Project (STOP) Dataset," *Access Now and the #KeepItOn Coalition*, Accessed February 2020.

[4] Jan Rydzak, "The Digital Dilemma in War and Peace: Determinants of Digital Network Shutdown in Non-Democracies," *Under review*, 2018.

[5] Olukotun and Micek, "Shutdown Tracker Optimization Project (STOP) Dataset," 2020

Table 1. List of countries that have enacted kill-switch shutdowns by year.

Country/Year	2011	2012	2013	2014	2015	2016	2017	2018	2019
Algeria					X		X		X
Bahrain						X			
Bangladesh						X			X
Benin									X
Cameroon							X		X
Chad								X	
China									X
Cote D'Ivoire								X	
Democratic					X		X	X	X
Republic of Congo									
Ecuador									X
Egypt	X					X			
Equatorial Guinea							X		
Ethiopia						X		X	X
Gabon									X
Gambia						X			
India		X	X	X	X	X	X	X	X
Indonesia									X
Iran									X
Iraq					X	X		X	X
Liberia									X
Malawi									X
Malaysia					X				
Mauritania									X
Myanmar									X
Nicaragua								X	
Niger					X				
North Korea					X	X			
Pakistan						X	X	X	X
Philippines					X		X		
Republic of Congo					X				
Russia									X
Sierra Leone								X	
South Korea								X	
Sudan			X						X
Syria		X				X	X	X	X
Tajikistan									X
Togo					X				
Turkey						X			
Uganda						X			
Venezuela				X					
Yemen								X	X
Zimbabwe									X

occur. Conversely, while foreign aid from the United States makes shutdowns less likely in this sample, more foreign assistance does not appear to decrease the number of shutdowns for states already using them. Building from the cross-national analysis, I then turn to qualitative evidence to better understand the dynamic relationship conflict, protest, and prior competitive elections have on governments use of kill-switch shutdowns.

My thesis contributes to the study of digital repression in two important ways. First, it advances the most systematic analysis to date of the determinants of kill-switch internet shutdowns over the last decade. Earlier scholars have studied internet shutdowns from 1985 to 2011, but this thesis updates the body of scholarship on cross-national internet shutdowns by using Access Now's dataset.[6] This data is likely to bring new insights to the fore for two main reasons: first, because of the turning point for government-mandated internet shutdowns that occurred as the world watched Egypt go dark in 2011, and second, because of the explosion in internet and mobile phone access that has swept across the world in the last decade. At the start of the 2010s, the internet was still primarily a luxury of the developed world, but increasingly affordable cellular technology has made the internet was accessible to billions more people. Many low-income countries that previously lacked the infrastructure for fixed-line internet connections have 'leapfrogged' their way into twenty-first century technology, and this mobile phone revolution has doubtlessly changed the dynamics of online political behavior, popular mobilization, and governmental digital repression. This paper presents an updated study of internet shutdowns, utilizing data that is more representative of today's global internet repression situation. Second, while Jan Rydzak's cross-national study has pushed the envelope for studies of internet censorship, it has only examined determinants of network shutdowns in non-

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

democracies. In the last decade, democratic states like India have become some of the most frequent regimes to shut off the internet for their citizens. Expanding the cross-national analysis to include democratic states will likely yield important new insights to the body of literature on internet censorship and repression.

Second, this paper informs scholarship on the nexus between armed conflict and emerging information and communications technologies (ICTs). The strong connection between conflict and internet shutdowns is shown in case studies to be in part due to the ability of non-state actors to utilize the internet to mobilize for violent collective action. Shutdowns are shown to be a potent tool for reducing the ability of armed actors to communicate with each other and with an online audience. In states facing armed rebellions, internet shutdowns can also prevent the spread of information online that could threaten the political survival of the ruling regime. Finally, this paper also makes contributions to scholarly knowledge of repression more generally. Understanding why states are not utilizing internet kill-switch shutdowns in response to violent protest when we might expect them to opens further questions for scholars who examine contemporary dissent and repression.

The rest of the thesis is as follows. After surveying the existing literature on internet shutdowns and the body of literature on international internet censorship, I situate the place of this study and its importance for bringing the study of internet kill-switch shutdowns into the present. Building off the extant literature, I present a theory of factors that might motivate governments to disconnect the internet and develop hypotheses for the relationships I expect to see between each of my independent variables and internet shutdowns. The paper then utilizes a mixed-methods approach to evaluate these hypotheses, moving from a large-N, cross-national analysis using OLS regression to small-n process tracing of the causal pathways in several cases.

The paper concludes with the implications of this work and avenues for future research.

2. Conceptualizing Internet Shutdowns

Internet kill-switch shutdowns are one of several potential tools that governments can use to control the flow of information online. This section reviews relevant literature on approaches states have taken to using information and communication technology (ICT) alongside societies. I then highlight the unique nature of kill-switch shutdowns and discuss why this form of internet censorship has become more common over time.

2.1 The Digital Repression Toolkit

Before delving into the body of knowledge on state restrictions on ICT, it is important to conceptualize the practice of internet shutdowns vis-à-vis other tactics that governments use to restrict access to ICT. To define internet shutdowns, I adopt a definition commonly employed by other scholars in the field: "an intentional and complete disruption of fixed-line or mobile Internet, ordered pursuant to the authority of the state, that renders the Internet inaccessible or unusable for a specific population, often to exert control over the flow of information."[7] In particular, I focus on what are known as "kill-switch shutdowns," in which the government turns off the entire internet—that is, blocks all access to fixed-line or mobile internet services, rather than blocking certain websites or applications or merely slowing down internet speeds.

Internet shutdowns can be distinguished from other forms of digital government censorship. States have pursued a number of tactics to block access to information and suppress dissent online. Wilson argues that the choices states make about internet control are contingent

[7] Rajat Kathuria et al., "The Anatomy of an Internet Blackout: Measuring the Economic Impact of Internet Shutdowns in India," *Indian Council for Research on International Economic Relations*, April 2018, https://thinkasia.org/bitstream/handle/11540/8248/Anatomy_of_an_Internet_Blackout.pdf?sequence=1. Ben Wagner, "Understanding Internet Shutdowns: A Case Study from Pakistan," *International Journal of Communication* 12(2018), 3917–3938, https://ijoc.org/index.php/ijoc/article/view/8545/2465

on both the state's internet infrastructure, as well as the tech-savviness of the regime seeking to control it.[8] Wilson lays out a menu of options that states wishing to control their country's internet can undertake, organized as three main approaches that each take aim at a different part of the internet: attacking individual "nodes", controlling the network, and controlling the application layer. Governments with a very high level of technological capacity can attack 'nodes' by utilizing viruses, spyware, and malware to track and control individual users. The United Arab Emirates, for example, passed legislation banning encryption of BlackBerry messages in 2011, allowing it to intercept personal messages between individuals and small businesses.[9] States without access or ability to track individuals with sophisticated technology can 'control the network' instead. This approach entails a cruder set of tactics, including internet shutdowns, that rely on control of the physical infrastructures that enable connectivity (such as internet cables or cell phone towers) to police online behavior. This approach requires less sophistication, but it can also be more easily circumvented by citizens if a government does not make a shutdown far enough 'upstream,' or high enough on the hierarchy of physical infrastructure. Finally, controlling the application layer is another technically sophisticated method of control, also known as customized malware or 'man-in-the-middle attacks.' Tunisia, Egypt, and Iran have used this approach to gain access to personal email and social media accounts to screen anti-regime messages and gather intelligence.[10] These kinds of surveillance and attacks require much more sophistication and a higher level of internet fluency than other approaches. For regimes with weaker IT capabilities, domain name system (DNS) blocking of

[8] Steven Lloyd Wilson, "How to control the Internet: Comparative political implications of the internet's engineering," *First Monday*, Volume 20, Number 2:2 (February 2015), http://dx.doi.org/10.5210/fm.v20i2.5228
[9] Josh Halliday, "UAE to tighten Blackberry restrictions," *The Guardian*, April 18, 2011, https://www.theguardian.com/technology/2011/apr/18/uae-blackberry-emails-secure
[10] Wilson, "How to Control the Internet," 2015.

specific websites or attacks on the internet infrastructure itself (i.e. a kill switch shutdown) are much more feasible.[11]

While this theoretical framework is useful for conceptualizing the components of the internet that governments can target, a continuum of other actions and policy options exist for governments seeking to control access to or content on the internet. Some scholars have drawn a contrast between regime control of the internet and regime activism on the internet. While regime control of the internet uses the tools of online repression, the latter entails governments and their agents employing—rather than blocking—social media and online resources to spread pro-regime messaging and misinformation that undermines political opposition and civil society.[12] Gunitsky builds on this work and develops a qualitative framework for how non-democratic regimes in particular use social media. He argues that social media serves a four-fold purpose for autocratic governments seeking to pursue regime activism and boost their legitimacy: (1) counter-mobilization, (2) discourse framing, (3) preference divulgence, and (4) elite coordination. These tactics work especially well when governments can "crowd-out" civil society dissent and discourse that occurs online.[13] For example, while China aggressively censors certain political content, such as calls for multiparty politics, not all online protest is taken down. "Protest within the bounds of the established political framework," Gunitsky writes, "can be used by party moderates as ideological ammunition against communist hard-liners."[14] The internet has also allowed state interests to masquerade as non-state actors when they participate in public

[11] The domain name system (DNS) is the database that provides names for network resources and connects them to IP addresses. For more information on its development and role in internet infrastructure, see J. Klensin, "Role of the Domain Name System," Network Working Group, Paper 3467. The Internet Society. 2003. https://tools.ietf.org/html/rfc3467. Also see: Wilson, 2015.
[12] Sheena Greitens, "Authoritarianism Online: What Can We Learn from the Internet in Non-Democracies?" *Political Science & Politics*, 2013.
[13] Seva Gunitsky, "Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability," *Perspectives on Politics* 13, no. 1 (2015): 42–54, doi:10.1017/S1537592714003120.
[14] Gunitsky, "Corrupting the Cyber-Commons," 2015.

discourse, using social media to join public discussion and shape discourse online.[15]

Several scholars have established that that attacks on internet infrastructure (such as kill-switch shutdowns) are more common among regimes with lower technological capacity. Rydzak argues that governments turn to increasingly advanced surveillance and censorship methods rather than simple internet shutdowns as they develop greater technological literacy. He cites video filtering and private armies of trolls that can be hired to report and remove undesirable content as tactics that are harder to track than simple shutdowns.[16] Zittrain et al. study internet censorship and content filtering around geopolitical conflicts, and identify internet shutdowns as an extreme option from a menu of internet censorship techniques. Kathuria et al. identified online counter-speech as an alternative to internet shutdowns in India that required a higher level of capacity and digital literacy.[17] Other scholars have also identified "throttling" as another tactic used by governments short of a full internet shutdown, by which a regime deliberately slows down internet connection speeds in public spaces and private residences.[18]

2.2 Kill-Switch Shutdowns

With so many options available to governments seeking to control their state's internet, the question arises: what makes internet shutdowns different from any of these other choices? In his article on the subject, Wagner makes a case for considering internet shutdowns as a unique phenomenon, distinct from other forms of internet control and censorship. He argues that shutdowns are more closely related to human rights violations and threats to democracy than

---

[15] Jonathan Zittrain et al,, "The Shifting Landscape of Global Internet Censorship," *Berkman Klein Center Research Publication* No. 2017-4; Harvard Public Law Working Paper No. 17-38, June 1, 2017, http://dx.doi.org/10.2139/ssrn.2993485

[16] Jan Rydzak, "The Digital Dilemma in War and Peace," 2018.

[17] Rajat Kathuria et al., "The Anatomy of an Internet Blackout," 2018.

[18] Ramesh Subramanian, "The Growth of Global Internet Censorship and Circumvention: A Survey," *Communications of the International Information Management Association (CIIMA)*, Volume 11, Issue 2, 2011, http://dx.doi.org/10.2139/ssrn.2032098.

other forms of internet control and censorship, as shutdowns not only take away communication and organization tools from protestors in times of crisis, but they also deprive surrounding society from accessing basic services in many cases.[19] Rydzak agrees that shutdowns deserve separate consideration, and writes that "in societies with a rapidly growing digital user base, network shutdowns should be the most basic, crudest form of maintaining control over the wired populace […] they are palpable, their effects are immediate, and they are a direct response (rather than a preemptive measure) to perceived threats."[20]

Existing literature has also studied the physical and political infrastructure of the internet that makes it possible for governments to carry out internet shutdowns. Although we often think of the internet as a decentralized web of connections, the physical infrastructure of network cables is both highly centralized and inherently hierarchical. A comparative study of internet infrastructure and government shutdowns in Egypt, Syria, and Libya found that a more highly centralized internet infrastructure rendered it easier to control and more vulnerable to shutdowns.[21] Egypt and Syria each had only one internet gateway, owned by a government monopoly, which made it simple for autocratic governments to order shutdowns. Libya, on the other hand, had infrastructure spread further apart geographically, which kept it outside government control and thus up and running during the country's civil war.[22] Other scholars have corroborated these findings, suggesting that internet shutoffs are easier to conduct in small countries, where there are fewer internet service providers (ISPs) to coordinate.[23]

Some scholars have contended that the development and global spread of secure

---

[19] Ben Wagner, "Understanding Internet Shutdowns," 2018.
[20] Jan Rydzak, "The Digital Dilemma in War and Peace," 2018.
[21] Warigia Bowman and L. Jean Camp, "Protecting the Internet from Dictators: Technical and Policy Solutions to Ensure Online Freedoms," *The Innovation Journal: The Public Sector Innovation Journal*, 18(1), 2013, article 3, http://www.ljean.com/files/Dictators.pdf.
[22] Ibid.
[23] Ramesh Subramanian, "The Growth of Global Internet Censorship and Circumvention," 2011.

protocols (https://, rather than http://) for internet connection has pushed some states towards internet shutdowns over milder forms of internet censorship. Prior to the expansion of secure protocols, Zittrain et al. write, censors were able to block individual webpages on websites like Wikipedia, rather than blocking access to the entire site. That ability is limited on sites that use HTTPS, which leaves internet censors with an all-or-nothing choice: to allow or block everything on a website.[24]

3. Theory and Hypotheses

This section develops a theory of why governments choose to enact costly internet shutdowns in the face of societies' dramatically higher mobilizational capacity since the spread of the internet worldwide. Given that this thesis is the first use of a novel dataset for a systematic analysis of the causes of internet shutdowns, I seek to test the effects of multiple independent variables on the likelihood of internet shutdowns. I begin with the factors that have been established as determinants by studies of earlier internet shutdowns, and then move into the factors I expect will have an effect on the likelihood of shutdowns based on my theory. I operationalize my variables in Section 4.

3.1 The Logic of Internet Shutdowns

Internet kill-switch shutdowns are one of a variety of tools at a regime's disposal as it seeks to achieve central policy goals. This paper assumes that states are rational actors whose policy goals revolve around maximizing their chances of political survival. This end goal is no different in democratic or autocratic regimes. In order to maintain power and achieve political survival, a government must successfully maintain security, grow the economy, and avoid mass unrest that threatens the legitimacy of the regime. Where transitions of power are less regular and

[24] Jonathan Zittrain et al., "The Shifting Landscape of Global Internet Censorship," 2017.

less institutionalized (in autocracies), this last goal is even more important because mass unrest could lead to uprising or revolution.

The rapid spread of ICT over the last decade has revolutionized the realm of state-society interaction. The Internet, mobile phones, and social media platforms have drastically raised the ability of societies to mobilize for both non-violent and violent collective action.[25] While generally autocratic regimes are more concerned with non-violent mobilization and protest that could threaten legitimacy, both autocracies and democracies alike are challenged to countermobilize against violent collective action and threats to security that are organized and carried out with the help of the internet.

The potential for digital communication platforms to increase dissent is widely documented in scholarly debates. In his book on the subject, James Fielder lays out the ways in which internet access can threaten authoritarian states through distance, decentralization, and interaction. He cites the ability to communicate cheaply and instantaneously over long distances as a huge boon to mobilization that puts autocrats on edge. He also describes how the decentralized flows of information that the internet enables are harder for states to control than earlier technology like television and radio. Thirdly, because of the interactive nature of the internet, users can be both producers and consumers of information and build trust through communities online.[26] In the earlier days of the internet, this mainly took the form of message boards and forums, and has now been replaced with networks and groups on large social media platforms. Each of these characteristics of online communications have the ability to increase dissent in authoritarian states. Facing this threat to regime survival, governments may be

---

[25] Clay Shirky, *Here Comes Everybody: The Power of Organizing Without Organizations*, Penguin Random House, 2008.

[26] James Fielder, "The Internet and Dissent in Authoritarian States" in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, *Taylor & Francis,* April 19, 2016.

motivated to shut down the internet at times of high protest mobilization to maintain control.

This theory, and many scholars of internet censorship and shutdowns, build on Christian Davenport's study of repression and the 'repression-dissent nexus:' as a regime faces real or potential threats to its hold on power or the status quo, the likelihood of repression grows.[27] Scholars have identified the growth in internet and mobile penetration as a clear challenge to the status quo: unilateral state control over the flow of citizens' information. Leberknight et al. argue that this development will compel regimes that have histories of repression to react against the rise of online communication and mobilization however possible.[28] Existing cross-national studies seem to provide support for this theory, and find that broad 'manipulation' of internet access to be more prevalent in autocracies.[29] Other scholars have further built on this theory and introduced other possible dynamics at play, like Kedzie's concept of a 'dictator's dilemma,' in which a regime may face social anger and increased mobilization regardless of its choice: to allow dissent on a free internet or by removing access to previously used forms of communication for a technologically-savvy populace.[30]

There is a growing body of literature on how social media and other online communication may lead to increased intergroup distrust and violence. Many of the characteristics that make digital communications (particularly mobile internet access) a powerful tool for activism and nonviolent mobilization have also contributed to its use in collective mob

---

[27] Christian Davenport, "State Repression and Political Order," *Annual Review of Political Science*, 10, 2007, pp.1-23, https://www.annualreviews.org/doi/abs/10.1146/annurev.polisci.10.101405.143216

[28] Christopher S. Leberknight, Mung Chiang and Felix Ming Fai Wong, "A Taxonomy of Censors and Anti-Censors Part II: Anti-Censorship Technologies," *International Journal of E-Politics (IJEP)* 3 (2012): 4, accessed (April 26, 2020), doi:10.4018/jep.2012100102

[29] Ronald Deibert et al., "Measuring Global Internet Filtering," in *Access Denied: The Practice and Policy of Global Internet Filtering*, MITP, 2008, pp.5-27.
P.N. Howard, S.D. Agarwal, and M.M. Hussain, "When do states disconnect their digital networks?" 2011.

[30] Christopher Kedzie. *Communication and Democracy: Coincident Revolutions and the Emergent Dictators*. Santa Monica, CA: RAND Corporation, 1997. https://www.rand.org/pubs/rgs_dissertations/RGSD127.html.

violence in a number of countries. The speed and frequency of mobile communications, mass forwarding functions on mobile platforms, and the social structure of social media and peer-to-peer messaging apps all make them potent tools for fostering violence and unrest.[31] ICTs do not only have the potential to facilitate online rumor-based violence. Because they lower coordination costs, access to the internet has been shown to increase the risk of conflict in Africa.[32] Access to mobile phone technology and internet services among previously unconnected populations has grown exponentially in the last decade, and with it, so has the risk of conflict outbreaks.

Perhaps the most common reason cited by governments who have chosen to enact internet shutdowns are concerns for safety and security. Where localized shutdowns have become a common pre-emptive tool for preventing mobilization, governments often justify their action with the risk of violent collective action. Many officials have cited the spread of misinformation online as necessitating a shutdown before it leads to violence.[33] Mukeredzi identifies violence prevention as a key factor in government decisions to carry out internet shutdowns in Africa, as does Rydzak in his study of internet shutdowns in Indian states.[34] Freyburd and Garbe find that election violence made internet shutdowns more likely to occur in their survey of sub-Saharan Africa, especially when ISP majority ownership rests in the hands of the state in authoritarian regimes.[35]

---

[31] Elizabeth Sutterlin, "Mob Violence, Mobile Phones: Private Messaging and the Future of Peacekeeping," *The Project on International Peace and Security*, 2019.
[32] Jan Pierskalla and Florian Hollenbach, "Technology and Collective Action: The Effect of Cell Phone Coverage on Political Violence in Africa," *American Political Science Review* 107:2 (2013), pp.207-224, doi:10.1017/S0003055413000075.
[33] Tonderayi Mukeredzi, "Uproar over Internet Shutdowns," 2017. Jan Rydzak, "Of Blackouts and Bandhs: The Strategy and Structure of Disconnected Protest in India." *Stanford University Working Paper*. February 7, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3330413
[34] Mukeredzi, "Uproar over Internet Shutdowns," 2017. Jan Rydzak, "Of Blackouts and Bandhs," 2019.
[35] Tina Freyburg and Lisa Garbe, "Blocking the Bottleneck: Internet Shutdowns and Ownership at Election Times in Sub-Saharan Africa," *International Journal of Communication* 12, 2018, pp. 3896-3916.

The goals of maintaining security and suppressing dissent are often interrelated. More than one potential cause can often be identified in a government's choice to carry out a shutdown. Scholars have noted the difficulty of distinguishing between legitimate efforts to maintain security and public safety and efforts to suppress dissent and mobilization. In his case study of shutdowns in Pakistan, Wagner puts it well: "Many of the shutdowns occur in the context of political rallies, elections, and public assemblies. Although there are clear security risks associated with such events, it remains an open question: What is being secured, and from whom?"[36]

Regardless of regime intentions, internet shutdowns serve as a policy tool that governments select as a means of maintaining security and suppressing dissent in the face of a population with this new, much higher mobilizational capacity. But what leads a state to select kill-switch shutdowns, rather than other forms of online censorship, tactics of digital repression, or offline policies? I argue that a state's choice to enact an internet shutdown is based on the perceived costs and benefits of the shutdown, as well as the state's capacity to make use of other policy tools.

Shutting down all internet services, even in a small geographic area, is incredibly disruptive and costly. There are economic costs—businesses and people that cannot carry out day to day transactions without access to mobile money or other digital financial services—as well as social and political costs. Domestic opposition politicians and digital rights watchdog NGOs can often come down hard on governments that enact repressive internet policy, and frequent shutdowns can erode public trust in government. However, if the perceived benefits of shutting down the internet are large enough (if the threat addressed with a shutdown represents a

[36] Wagner, 2018.

huge challenge to political survival), a regime may still select to enact a full shutdown. Part of that cost-benefit analysis is also a state's capacity to make use of other policy tools to address the threats it faces (whether security threats or mass uprisings.) Not all states have the technological capacity to employ sophisticated online surveillance of citizens or rebel groups. And for many, the costs of deploying state security forces to respond to threats of violent collective action may be much higher than shutting down the internet for a few hours or days to prevent the spread of misinformation or the coordination of violent attacks.

The following section uses this theoretical framework to introduce possible determinants of internet shutdowns: factors that increase or decrease shutdown costs, increase or decrease shutdown benefits, or increase or decrease a state's capacity to use other policy tools to respond to events that threaten a regime's political survival.

3.2 Determinants of Internet Shutdowns

Having surveyed the state of academic literature to better understand what internet shutdowns are, how they are implemented, why governments enact them, I turn to factors identified in the extant literature that contribute to a state's choice to shut down the internet. As mentioned earlier in this paper, given the relative newness of this phenomenon, the body of literature is still small, and few papers have delved into identifying the broad determinants of internet shutdowns.

When considering internet shutdowns, this paper focuses specifically on kill-switch shutdowns, and does not consider other types of internet censorship and repression (i.e. throttling of internet speeds or specific platform-based DNS blocking) that are widely used by governments seeking to control the flow of online information. There are several reasons for this choice. First, as mentioned earlier, full internet network shutdowns represent one of the crudest

and most immediately felt choices about internet access that a government can make. As discussed in the literature review, other scholars have argued that kill-switch shutdowns deserve special treatment because of these qualitative differences. One other reason to consider these shutdowns uniquely from other forms of internet control is for reduced noise in the dependent variables. Many states have enacted blocks at some time or another for varying social, cultural, or religious reasons (i.e. bans on online gambling and pornography). The reasons behind blocking specific websites, mobile apps, or other internet activity can vary country to country, just as the platforms in question that are being blocked will vary widely. Because kill-switch shutdowns are both so extreme and so crude, the states that implement them likely have more uniform motivations and expectations for what those shutdowns will achieve.

Narrowed down to kill-switch shutdowns, this paper looks at the effects of several independent variables on two dependent variables. First, I look simply at whether a kill-switch shutdown occurred in a given country-year. Second, I look at the effects on the number of kill-switch shutdowns that occurred in that country-year period. Looking at these as two different dependent variables is important, because while some countries only experience one shutdown around a large event in a year, there are some states where internet shutdowns have become a frequently used tool for controlling online speech. Reducing the variation in the data to a dummy variable obscures some of this, and so measuring both the presence of and the number of kill-switch shutdowns will yield important and meaningful results.

First, I examine the effects of regime type. Drawing on arguments from the literature, I expect that non-democracies and less democratic regimes will be more likely to implement internet shutdowns because they feel more threatened by the potential for greater mobilization and protest that internet services represent. The more autocratic a state is, the more likely it may

be to shut down the internet. However, as scholars have acknowledged variation within autocracies,[37] I also examine the effects of civil liberties. Civil liberties and media freedoms make internet shutdowns more politically costly to governments, as media can serve as a vehicle for expressing public disapproval or backlash against internet shutdowns. If a regime expects such backlash from independent media that could threaten its political survival, it will be less likely to employ internet shutdowns. In countries where traditional mass media is owned or controlled by the state, television, newspapers, and radio may not accurately portray political developments or provide media coverage of protests or opposition movements. Where this is the case, social media and online communications play and even more pivotal role as a space for citizen journalism and a public sphere not controlled by state authorities.[38] In that kind of environment, a regime might view online communications and social media as a threat to its information control. For this reason, I expect civil liberties to be negatively associated with internet shutdowns—the fewer civil liberties citizens and media have in a country, the more likely it is that a regime would shut down the internet.

Several scholars have found that internet penetration and internet shutdowns to be positively related.[39] In his groundbreaking cross-national analysis of internet shutdowns in non-democracies, Rydzak found that internet penetration was consistently positively associated with network shutdowns (i.e., that the more citizens use the internet, the more likely it is to be shut off by non-democratic regimes.) Additionally, his study finds tertiary education levels to be consistently positively correlated with network shutdowns, supporting the 'authoritarian anxiety'

[37] Tina Freyburg and Lisa Garbe, "Blocking the Bottleneck," 2018.
[38] Zeynep Tufecki, "New Media and the People-Powered Uprisings," *Technology Review,* 2011.
[39] Conor Sanchez, "The Link Between More Internet Access and Frequent Internet Shutdowns," *Net Politics Blog, The Council on Foreign Relations,* August 22, 2018, https://www.cfr.org/blog/link-between-more-internet-access-and-frequent-internet-shutdowns

hypothesis, in which non-democratic regimes fear an educated and connected population that is equipped to mobilize and drive collective action.[40] However, the paper also identifies the existence of a 'digital threshold,' past which online repression tapers off. Scholars looking specifically at India have observed fewer shutdowns in Indian cities with better developed digital infrastructure and higher levels of digital activity.[41] I expect this relationship to hold in my dataset of democracies as well as non-democracies—where there are few or no internet users, autocratic governments have no need to see the internet as a mobilizational threat. Additionally, if democracies are using internet shutdowns to address legitimate security concerns, their usage of internet shutdowns will also likely increase as the number of people using the internet rises, as a larger online population would likely lead to a larger number of threats to state security occurring online. As a larger portion of a country's population gets online, both the costs and the benefits of enacting shutdowns increase, but building on Rydzak's theory, I argue that the benefits rise more quickly than the costs. The higher the share of citizens who have access to the internet, the more shutdowns I expect to occur.

While the level of internet penetration in a country has been found to be positively related to government propensity to conduct an internet shutdown up to a certain point, the size of a country's digital economy would likely have a negative effect on the likelihood of shutdown. As more and more of a country's economy is dependent on the internet and technological sectors, and as the internet continues to revolutionize business operations in every sector of the economy, the economic costs of an internet shutdown grow, making it more costly for governments to enact them. Several scholars have attempted to measure the economic impacts of internet shutdowns, but there is still no universal measurement of the size of a digital economy. The

[40] Rydzak, 2018.
[41] Kathuria et al., 2018.

digital economy is often measured by looking at the relative size of a country's internet infrastructure.[42] I expect to find that the more established a country's internet infrastructure is (and thus the larger the digital share of its economy), the less likely its government will be to enact an internet shutdown, for concerns about the larger economic blowback of such a choice. As a country's internet infrastructure grows, so too does the state's technological capacity. In states with such well-established infrastructure, regimes will likely move away from crude internet shutdown tactics and towards more sophisticated methods of surveillance and content censorship, as the regime's ability to enact these more precise policies effectively increases.

Given that governments frequently cite security concerns and maintaining order around large events as reasons to implement shutdowns, I expect that the level of protest a country faces will play a role in whether it experiences a shutdown. As described in Section 3.1, high levels of protest, especially in an autocracy, can undermine the legitimacy of the government and threaten a regime's political survival. Internet shutdowns then become more attractive policy tools to counter protest as the severity of the threat (and thus the benefits of addressing it) increase. If a state experiences high levels of protest, the regime may view online communications as a tool of mobilization enabling those protests. If it is easier to cut off the internet than it is to address the grievances being protested, the government will be likely to choose an internet shutdown. I expect that this effect will be stronger for violent protests, as in the face of protest violence, the justification of internet shutdowns for security purposes becomes even greater. Cutting off the internet is generally cheaper in the short run than counter-mobilizing police or military forces to disperse violent protesters. For these reasons, I expect violent protests to make states more likely

[42] Organization of Economic Cooperation and Development, "Toolkit for Measuring the Digital Economy – Draft Version," *G20 Summit Argentina 2018*, November 2018, http://www.oecd.org/g20/summits/buenos-aires/G20-Toolkit-for-measuring-digital-economy.pdf

to shut down the internet.

Many scholars have noted the relationship between large youth populations (youth bulges) and government repression.[43] Not only are young people shown to be prone to mass mobilization and sensitive to socioeconomic grievances, but they are also the largest user base of online communications, and thus are both primed and prepared to use them to mobilize. Because of this greater mobilizational threat, a large youth population may increase the perceived benefits of enacting an internet shutdown, thus increasing the likelihood that a government will shut down the internet. This trend was especially visible during the Arab Spring, but it is unclear whether that relationship is broadly generalizable.[44] However, it is still possible that youth populations have affected internet shutdowns cross-nationally in the last decade as population demographics and internet repression dynamics have continued to evolve. Per this theory, I expect that a larger youth population will increase the likelihood that a country experiences a shutdown.

Internet shutdowns are often clustered around election times, especially in African states. Scholars and digital rights bloggers have theorized about a relationship between elections and internet shutdowns in electoral authoritarian regimes.[45] Incumbents have political motivations for shutting off internet services (such as preventing members of the opposition from organizing protests or reporting election irregularities), but may also use security concerns about election violence or fears of fake election results being spread online as justification for the shutdown. Although crude, shutdowns serve their purpose in helping regimes effectively maintain their hold

---

[43] R. Nordas and C. Davenport, "Fight the Youth: Youth Bulges and State Repression," *American Journal of Political Science*, 57: 926-940, 2013, doi:10.1111/ajps.12025

[44] Rydzak, 2018.

[45] Freyburg and Garbe, 2018. Sharon Anyango Odhiambo, "Fake News Dominates Ahead of Kenya's Elections," *Africa Up Close: a blog of the Africa Program at the Wilson Center,* August 4, 2017, https://africaupclose.wilsoncenter.org/fake-news-dominates-ahead-of-kenyas-elections/.

on power in the face of electoral competition.[46] Drawing on these theories, I expect that a regime will be more likely to enact an internet shutdown during an election year, as the potential benefits of an internet shutdown will be larger when a regime's political survival is at stake in the lead up to an election. I also expect that this effect will be stronger for competitive elections: if opposition parties are barred from contesting results, the incumbent regime will have no need to shut off internet services in election years to prevent protests over the results. A credible threat to survival will make governments more likely to enact an internet shutdown.

Scholarship on the relationship between conflict and internet shutdowns has had mixed results. Rydzak did not find support for the hypothesis that conflict can predict shutdowns—neither when measured in battle-deaths or on a scale of conflict magnitude, and questions the prevailing assumption that regimes tend to disrupt internet services and digital communication in times of war or violence.[47] This is inconsistent, however, with findings from Freyburg and Garbe who find that electoral violence plays an important role in the implementation of internet shutdowns in sub-Saharan Africa, though not a sufficient one on its own.[48] Rydzak does include the caveat, however, that "trouble in the neighborhood" (conflict in the surrounding region) could lead a regime to wage a "preemptive assault on the digital rights of citizens."[49] Based on my theory, I argue that conflict will raise the perceived benefits of an internet shutdown as governments seek to maintain security. State forces could enact internet shutdowns to disrupt the online communications (and thus the ability to mobilize) of armed insurgent groups, or to prevent the spread of information that could harm regime legitimacy. I expect that a higher level of conflict will lead to an increased likelihood of internet shutdowns.

---

[46] Freyburg and Garbe, 2018.
[47] Rydzak, 2018.
[48] Freyburg and Garbe, 2018.
[49] Rydzak, 2018.

I include GDP per capita as a control, as several other scholars in this field have done prior.[50] Poorer countries may not have the infrastructure to use more technologically sophisticated tactics than kill-switch shutdowns. I expect that wealthier states have the technological capacity to pursue other repressive tactics online, such as specific content filtering or surveillance. Because a higher GDP per capita raises the ability of a state to pursue other policy options, I expect an increase in GDP per capita to lead to a decrease in the likelihood of internet shutdowns.

Given that the United Nations has passed resolutions condemning the use of internet shutdowns, even in crisis and conflict situations as violations of human rights law,[51] and that several liberal Western democracies have declared their support for internet freedoms,[52] it is clear that international norms against internet shutdowns have been set. While it is unclear what specific penalties states would incur from international legal institutions for violating these norms, regime leaders likely do recognize that they run the risk of losing the support of a security guarantor, development assistance, or simply good standing within international institutions as a result of implementing internet shutdowns and other digitally repressive tactics. Drawing on Levitsky and Way's theory of linkage and leverage, I expect that regimes with fewer international linkages to countries that condemn shutdowns will be more likely to shut down the internet.[53] Governments with more international linkages to states that are committed to freedom

---

[50] Ibid.
[51] United Nations Office of the High Commissioner of Human Rights, "Joint Declaration on Freedom of Expression and responses to conflict situations," 2015.
[52] Hillary Clinton, "Internet Rights and Wrongs: choices and challenges in a networked world." *Remarks at George Washington University*. February 15, 2011. http://diritto-comunicazione.decesare.info/Hillary-Clinton_George-Washington-Univ_15_02_11.pdf.
[53] Levitsky and Way's 2006 paper presents a framework for understanding post-Cold War regime change that involves two dimensions: western 'leverage,' which is "the degree to which governments are vulnerable to external democratizing pressure," and linkage to the West, which is "the density of ties and cross border flows" (379). Those ties can be economic, diplomatic, social, or organizational, and the flows across borders can be of trade and investment, people, or communication (379). The authors found that international linkages encourage

of internet access will have more to lose in development aid, trade sanctions, and other international financial costs that raise the perceived costs of implementing shutdowns.

Finally, this paper also seeks to test the path dependency hypothesis. Cursory examination of the data on which countries have enacted shutdowns from 2011-2019 shows that there are few countries that only implemented a shutdown once. Most countries have either never shut down internet access or have done so frequently in the last decade. This suggests that a potential path dependency may impact government choices of shutdowns. It seems likely that once a regime has shut down the internet once, it is much more likely to continue using that tactic in the future. After states have enacted a shutdown, the costs they face from subsequent shutdowns might fall while the benefits remain the same: citizens who had initially been unhappy about internet outages could be convinced of the necessity of more shutdowns for security, or further repressed to prevent them from protesting later shutdowns. I expect that shutdowns in the past increase the likelihood of shutdowns in subsequent years.

4. Data and Methodology

I employ a mixed-methods approach to better understand which factors increase a government's use of internet shutdowns and why. After explaining the unique strengths of this methodology, I describe the data I use for my dependent and independent variables in detail and explain the process through which I settled on the specific regression models in this paper.

4.1 Mixed Methods Approach

This thesis utilizes a mixed-methods analytical approach to first identify cross-national

---

democratization, because they "raise the costs of autocratic abuses by increasing their international salience and the likelihood of external response, enhancing the power and prestige of opposition forces, and expanding the number of domestic actors with a political, economic, or professional stake in adhering to international norms." (379) For more information, see: Steven Levitsky and Lucan A. Way, "Linkage versus Leverage. Rethinking the International Dimension of Regime Change." *Comparative Politics* 38, no. 4 (2006): 379-400, doi:10.2307/20434008.

factors that contribute to internet shutdowns, and then to process-trace the mechanisms through which those factors may be influencing government choices to enact internet shutdowns. By employing this nested research deign, this paper draws on the strengths of both large-N and small-n analyses for making causal inferences. Because there are several possible explanations for governments' choices to enact internet shutdowns, I have chosen to begin with the larger, quantitative analysis to rule out explanations with little empirical support. I then move to the smaller, qualitative case study analysis for the explanatory variables that do find support, to examine the circumstances in which those variables are major determinants in a government's decision to shut down the internet.

I begin first with a cross-national analysis of internet shutdowns from 2011 to 2019 to identify potential factors that played a role in causing the shutdowns. The quantitative, large-N side of this methodology is important for several reasons. First, because so few quantitative studies of internet shutdowns have been conducted by scholars in the literature, there is a great deal of value in running regressions to identify statistical relationships that have yet to be documented or studied. The time period selected for this analysis is also important. The most recent large-N study of internet shutdowns uses data ending in 2011. As the demographics with internet access via both fixed-line and mobile connections have shifted drastically in the last decade, conducting a cross-national analysis of more recent data that more closely resembles today's reality is of great importance.

After analyzing relationships discovered and identified in the cross-national, quantitative analysis, I move to a case-study approach using the methodological framework put forward by Lieberman, in which "the small-n analysis should be used to answer the questions left open by

the large-N analysis."[54] This small-n study will examine just how the factors shown to be statistically correlated actually lead to shutdowns of the internet. As both available data and statistical methods for analyzing that data are limited, the small-n segment of this nested research design, by making use of select cases to understand causality, will also inform future research questions to be answered using both small and large-N approaches, based on how well the theory suggested by the quantitative analysis seems to have predicted real country cases.[55]

4.2 Dependent Variable

The unit of analysis for this paper is at the country-year level. There is some variation in the geographic scope of kill-switch shutdowns used by countries around the world; for example, in India, shutdowns are frequently executed at the local or regional levels of government, while in Ethiopia, shutdowns are more likely to come from the national government and impact a less localized population—in many cases, the entire country is included in the blackout. While there is certainly value in understanding why different countries enact shutdowns on different geographic and governmental levels, that question is outside the scope of this research. Based on previous work done by scholars in the literature, I do not suspect that the factors informing government's motivations to carry out a shutdown at a local, regional, or national level would be any different. By analyzing data at the country-year level, I am able to evaluate kill-switch shutdowns in the same way and compare more easily across countries. I selected the 193 countries in my dataset using the criteria of UN membership; non-internationally recognized states and observer states are not included.

For the quantitative portion of this research, I make use of AccessNow's database of

[54] Evan S. Lieberman, "Nested Analysis as a Mixed-Method Strategy for Comparative Research," *American Political Science Review* 99, no. 3 (2005): 435–52, doi:10.1017/S0003055405051762.
[55] Ibid.

internet shutdowns from their Shutdown Tracker Optimization Project (STOP). The earliest reports of shutdowns included in their dataset are from 2005, with occasional missing years. Their data is complete beginning in 2011 and is the most up-to-date dataset of internet shutdowns; at the time I requested access to their master database, it included shutdowns through all of 2019. Some samples of their data are available online, but access to their complete records was granted for academic purposes and is available upon request.

AccessNow's STOP dataset captures several forms of government internet censorship: kill-switch (referred to in their data as 'full network') shutdowns, bandwidth throttling, and platform-based blockages. It does not capture more sophisticated forms of internet censorship, such as cyberattacks against targeted individuals or the use of groups of online trolls to report content en masse for takedown of sensitive media. Because this research is limited in scope to the determinants of kill-switch shutdowns, I excluded all entries from the STOP dataset that were instances of bandwidth throttling or platform blockages. However, a full network shutdown of either the internet, mobile network service, or both simultaneously are all considered. Including the shutdown of mobile services alone (without the shutdown of fixed-line internet) under the definition of full network shutdowns is important. In much of the developing world, people's sole access to the internet is generally through cellular devices, because physical, fixed-line internet infrastructure is rare and prohibitively expensive.

Having identified the cases of full network shutdowns in the STOP dataset from 2011 - 2019, I used those entries to create two dependent variables for the cross-national portion of my analysis. First, I created a variable to count the number of kill-switch shutdowns that occurred in a given country-year, and then created a dummy variable to measure the presence of a kill-switch shutdown in a given country-year, where 1 indicates that a kill-switch shutdown occurred and a 0

means there was no shutdown.

I also utilized the STOP dataset from AccessNow to test the path dependency argument. I created lagged variables to evaluate what impact past kill-switch shutdowns had on the likelihood a government would enact one again. For this, I also created two variables: first, one that measured whether a country had ever experienced a shutdown prior to that year, and second, one that measured whether a country had experienced a shutdown in the year directly preceding a given year. One important note regarding the construction of these variables is that AccessNow's dataset did not include any entries from 2010. While it is possible that simply no shutdowns occurred that year, I did not feel that this was a safe assumption and did not want to erroneously code missing 2010 data as though there were no shutdowns if any had in reality occurred. For this reason, when I coded whether or not there had been a shutdown in the year immediately preceding a given country-year, I used Access Now's 2009 data, essentially skipping 2010 and treating 2009 as the year before 2011 to address this data problem.

4.3 Independent Variables

I measure press freedoms using Freedom House's civil liberties score. The Freedom House methodology is well-documented and widely utilized by scholars seeking to cross-nationally examine press and political freedoms. The civil liberties score is a measure of 15 questions grouped into four subcategories: freedom of expression and belief, associational and organizational rights, rule of law, and personal autonomy and individual rights.[56] Countries are

[56] Internet shutdowns are one of the many indicators Freedom House uses to construct their Civil Liberties scores. If these values were strong predictors of internet shutdowns, this would undercut that effect; however, my analysis found civil liberties scores and internet shutdowns to be empirically uncorrelated. Future iterations of this research should find alternative measures of repression and media freedoms that do not factor in internet restrictions at all. For more information on how those at Freedom House compiled their scores, see part D of: Freedom House, "Freedom in the World Methodology," *Freedom House*, Last accessed April 23, 2020, https://freedomhouse.org/reports/freedom-world/freedom-world-research-methodology.

scored from 1 to 7, with a higher score representing fewer press freedoms. I elected to use only the civil liberties score for each country-year in my dataset, rather than the full score, because I was less interested in capturing Freedom House's measures of political rights, and felt that the questions asked to determine a country's civil liberties score were more telling about the situation of informational and press freedoms in said country. As described in Section 3, I expected that this might have an effect different from simply the level of democracy or political freedom in a country.

For measures of regime type, I utilize each country's Polity scores from the Polity IV dataset. Countries are scored from -10 to 10, from least to most democratic. For countries in transition, I followed the standard described in the Polity user manual for converting countries with scores -66, -77, and -88 (representing foreign interruption, anarchy, and transition periods, respectively) to fit the conventional twenty-point scale for easier time series analysis.[57]

To measure protest, I used open access cross-national dataset of protest from the Mass Mobilization Project, which aggregates the number of protests in a country-year period.[58] The data captures every event in which more than 50 protestors publicly demonstrate against a government, and spans 162 countries from 1990 until 2018. Although not all 193 countries that I had initially hoped to examine are included in this data, this dataset was the most up-to-date, publicly available resource for analysis. The 31 countries not included in this data are primarily very small countries—most of the island nations in the Caribbean and the Pacific, for example. This dataset also disaggregates violent protests from the total number of protests that occurred in

[57] Monty G. Marshall, Tedd Robert Gurr, and Keith Jaggers, "Polity IV Project: Political Regime Characteristics and Transitions, 1800-2016. Dataset Users' Manual." *Center for Systemic Peace*, p.17, https://www.systemicpeace.org/inscr/p4manualv2016.pdf.

[58] Clark, David and Regan, Patrick, "Mass Mobilization Protest Data," *Harvard Dataverse V3*, 2016, https://doi.org/10.7910/DVN/HTTWYL.

a country-year period, which allows me to specifically test for the effects of violent protest.

I also draw my measure of a country's online population from World Bank indicators. Specifically, I look at their indicator of individuals using the internet as a percentage of the population, sourced from the International Telecommunications Union database. Internet users are defined as someone who has used the internet from any location in the last three months, whether from a computer, mobile phone, personal desktop assistants (PDAs), games machine, digital TV, or other device.[59] This data was available for all years through 2018.

My measurement of the size of a country's youth population also comes from World Bank data. More specifically, the population I was most interested in were those aged 15-19, because I expected that age group to be both the most technologically savvy and most inclined to protest. While the World Bank's publicly available data did not have a direct statistic for the size of a country's youth population aged 15-19, it does include the percentage of a population that is male and female, and the percentage of the male and female population that are aged 15-19.[60] I created my own measure of the percentage of the total population aged 15-19 by doing the following math for each observation in my dataset:

$$Youth\ population\ =\ [(\%\ male\ of\ total\ population\ *\ \%\ aged\ 15-19\ of\ male\ population)\ +$$
$$(\%\ female\ of\ total\ population\ *\ \%\ aged\ 15-19\ of\ female\ population)]\ /\ 100$$

My data on GDP per capita also came from the World Bank. I elected to use their measure of per capita GDP at purchasing power parity using current international dollars, from the last round conducted in 2011.[61]

---

[59] Despite being a clear metric of a country's online population, there is reason to suspect that these indicators might be underestimates, especially in African states with high mobile phone penetration and use of mobile money but few fixed line internet connections. For more information on how the data was collected, see: World Bank, "World Development Indicators," *World Bank Open Data*, https://data.worldbank.org/indicator/IT.NET.USER.ZS?view=chart

[60] World Bank, "World Development Indicators," *World Bank Open Data*.

[61] World Bank, "World Development Indicators," https://data.worldbank.org/indicator/NY.GDP.PCAP.PP.CD

I gathered data on the time until a country's next election from Princeton's Database of Political Institutions, which includes a variable for the years until the country's next national election, which includes both legislative and executive. Election years are coded as zeroes.[62] To create a dummy variable out of this, I counted a country's election years (zeroes in DPI's dataset) as a 1 and all non-election country-years as 0.

My measure of conflict came from UCDP/PRIO's Armed Conflict Dataset. I did not distinguish between interstate and intrastate conflicts, but I used their measure of conflict intensity to measure the level of conflict occurring in a given country and year. I coded a zero for the absence of conflict, a 1 for low level conflict (25-999 battle deaths), and a 2 for intense conflict (1000 or more battle deaths), following the scale described in the UCDP/PRIO codebook.[63]

My measure of competitive elections comes from V-Dem, the Varieties of Democracy dataset. I utilize their measure of national multiparty elections (v2elmulpar), an ordinal variable scaled from 0 to 4, where zero is the least competitive and 4 is the most competitive. The scores are based on respondents' answers to the question: "Was this national election multiparty?"[64] Because not every year is a national election year, I used this data to create a lagged variable that signals whether or not the country's most recent election was competitive. I also create a dummy variable for whether or not the country's last election was competitive, and to do that, I condense the data so that a score greater than equal to 3 for a given country-year is converted to a 1 (a previous competitive election), and all values less than 3 are converted to a 0 (a previous non-

---

[62] Carlos Scartascini, Cesi Cruz, and Phillip Keefer, "The Database of Political Institutions 2017 (DPI 2017)," *The Inter-American Development Bank*, https://publications.iadb.org/en/database-political-institutions-2017-dpi2017.
[63] Nils Gleditsch et al., "Armed Conflict 1946-2001: A New Dataset." *Journal of Peace Research* 39(5), 2002, p.5. https://ucdp.uu.se/downloads/ucdpprio/ucdp-prio-acd-191.pdf.
[64] Michael Coppedge et al., "V-Dem Codebook v9." *Varieties of Democracy (V-Dem) Project*. 2019.

competitive election). V-Dem describes a score of 3 on this variable to mean that "elections are multiparty in principle but either one main opposition party is prevented (de jure or de facto) from contesting, or conditions such as civil unrest (excluding natural disasters) prevent competition in a portion of the territory."[65] I chose this score as the cutoff point when constructing the dummy variable, as any country that could not meet these criteria for limited fairness did not have competitive enough elections to incite incumbents to use shutoffs to prevent mobilization or campaign organizing.

My measure of aid dependence on the United States was calculated using GDP statistics from the World Bank at constant 2015 US dollars and using reported statistics from the U.S. Agency for International Development (USAID). I use aid from the United States specifically rather than an institutional or other unilateral donor for two reasons. First, by only considering one source country for assistance, it is easier to compare apples to apples when looking at recipient aid to GDP ratios. Secondly, because of the strong stance of the United States on commitment to internet freedoms abroad[66] and the country's relative power as a norm and agenda-setter in the international system, I expect that figures on aid received from the US would accurately show the relationship between Western foreign assistance and internet shutdowns.[67]

As described in the theory section, measuring the size of the digital economy in dollars is nearly impossible. However, one proxy identified and recommended by the Organization for

---

[65] Ibid.
[66] Hillary Clinton, "Internet Rights and Wrongs," 2011.
[67] The Obama and Trump administrations have each taken very different approaches to American foreign assistance, both in the size of the budget and the issues prioritized. The Trump administration has overseen the U.S. retreat from leadership in international institutions and has generally harmed the image of the United States as a democracy promoter overseas. However, as my analysis only runs through 2019, it is somewhat too early to see the effects of changes made under the current administration since 2017. Many U.S. government programs that promote international internet freedom and condemn digital repression have remained in place across administrations. For more information on U.S. government internet freedom programs, see: U.S. Agency for Global Media, "USAGM launches independent internet freedom grantee," U.S. Agency for Global Media, November 25, 2019, https://www.usagm.gov/2019/11/25/usagm-launches-independent-internet-freedom-grantee/.

Economic Cooperation and Development (OECD) is a country's number of secure internet servers.[68] This measure gives an estimate of the size and development of a country's information and communications technology (ICT) infrastructure. The size of a country's ICT infrastructure is a good proxy for the relative importance of the digital sector in its economy. The World Bank's open source data include a measure of secure internet servers in a country per 1 million people annually. Their measure uses a raw number of secure internet servers (defined as distinct, publicly trusted TLS/SSL certificates).[69] The World Bank's data comes from Netcraft's Secure Server Survey, which "examines the use of encrypted transactions through extensive automated exploration, tallying the number of websites using HTTPS."[70] Where the certificate is valid for the hostname and has been issued from a publicly-trusted root, the geographic hosting location of the sites using that certificate are traced. The World Bank then divides that data by the mid-year population and multiplies it by one million to reach their measure.

4.4 Methodology

This paper utilizes OLS regression to empirically test the relationships between my independent variables and the likelihood of a kill-switch shutdown. After importing all necessary data into Stata, I created lagged variables for variables in my dataset where there were not yet published values for 2019, but their values were unlikely to have changed in just a year. These variables were the Polity scores, online population, youth population, conflict, secure internet

---

[68] OECD, 2018.

[69] TLS/SSL certificates are essentially what makes a website secure and gives it a secure protocol (HTTPS rather than just HTTP.) They serve to encrypt the information that is sent over the internet between the user's computer (the client) and the server hosting the websites that are visited, protecting sensitive information from potential theft or capture. These certificates are especially important for online transactions, in which sensitive financial information is communicated between servers and clients. For more information on how these certificates work, see Gruhn, Diana. https://www.entrustdatacard.com/blog/2019/march/ssl-certificates-101-why-do-i-need-an-ssl-tls-certificate.

[70] Netcraft is a British cybersecurity company that has been tracking the global use of TLS/SSL protocols for market research since 1996. For more information on their survey, see their website: https://www.netcraft.com/internet-data-mining/ssl-survey/.

servers per 1 million people, and GDP per capita. Prior to running any regressions, I ran a short test to check for high correlations between any of my independent variables that would have made including them all redundant. Through this process, I excluded some of the variables I had initially collected in my dataset and settled on twelve independent variables to test in my models. The collinearity tests for all variables can be found in Appendix A. Regime type (Polity scores) was dropped due to its high correlation with Freedom House scores. The general protest count variable was excluded as I expected violent protest to be more closely related to internet shutdowns, when governments have more incentive to shut down the internet to preserve security. I excluded the variable for the size of a country's online population due to its high correlation with youth population. I elected to include youth population instead, as I was also still capturing a related measure to internet use through the secure servers per million people variable. I also dropped the dummy variable for whether or not a country was in an election year, instead keeping the variable for the number of years until the next election. Finally, I also excluded the non-dummy variable for electoral competitiveness, instead choosing to focus on whether a country's last election met the cutoff described above to be considered competitive. Table 2 provides descriptive statistics for the variables I have selected.

While running different variations of regressions to test how consistent the effects of my independent variables were, I noticed that my model was extremely sensitive to India. This makes sense, in that India has carried out the most internet shutdowns in the world, and generally enacts them at a local, or even hyper-local level—rather than enacting one national-level shutdown, Indian officials might instead enact multiple shutdowns at the municipal level on the same day. For this reason, I selected four regression models for analysis in this paper. I evaluate the effects of my independent variables on both the presence of shutdowns for the world

Table 2. Mean values and standard deviations for both independent and dependent variables, rounded to four decimal places.

Variable	Mean Value	Standard Deviation
Presence of kill-switch shutdown	0.0420	0.2007
Number of kill-switch shutdowns	0.2343	3.4394
Media freedom	3.3057	1.9030
Prior shutdowns	0.1002	0.3003
Shutdown in the previous year	0.0300	0.1705
Violent protest	0.9717	2.5527
Percentage of population aged 15-19	8.4501	2.2978
Time to next election (years)	1.9780	1.4097
Secure internet servers (per million people)	2550.317	11445.58
Conflict	0.2065	0.4933
Last election competitiveness	3.3402	1.0413
GDP per capita (PPP)	17772.69	19043.47
U.S. foreign aid to GDP ratio	1.2334	5.5974
Year	2015	2.5827

(model 1) and without India (model 2), and on the number of kill-switch shutdowns for the world (model 3) and without India (model 4). The following section analyzes and discusses the results of these regressions.

5. Quantitative Analysis

The regressions shown in Table 3 show the coefficients, standard error, and level of significance for each of my independent variables. I have also included standardized coefficient plots to show visually the effects of my independent variables for each model. When looking at the signs for the coefficients on media freedom, it is important to note that since this analysis uses Freedom House scores, a higher number indicates a worse environment for free media. This variable did not have a statistically significant effect on the presence of shutdowns in either Model 1 or Model 2. However, worse civil liberties did have significant effects (at the 0.05 level) on the number of shutdowns that occurred in a country-year period in Models 3 and 4. Model 4 has a mean number of shutdowns of 0.23, and an expected positive coefficient, suggesting that

Table 3. Four regression models for analysis.

	(1) Presence,World	(2) Presence,no India	(3) Number,World	(4) Number,no India
Civil liberties	0.001	0.008	-0.187*	0.028*
	(0.006)	(0.006)	(0.088)	(0.013)
Prior shutdown	0.074**	0.068**	0.285	0.120*
	(0.025)	(0.023)	(0.342)	(0.051)
Shutdown in preceding year	0.152***	-0.012	5.500***	0.250**
	(0.042)	(0.043)	(0.576)	(0.092)
Violent protest	0.003	0.001	0.058	0.001
	(0.002)	(0.002)	(0.032)	(0.005)
Youth population (lag)	0.010*	0.009*	0.028	0.014
	(0.004)	(0.004)	(0.057)	(0.009)
Time to next election	0.001	0.001	0.028	-0.004
	(0.004)	(0.004)	(0.060)	(0.009)
Secure servers per million (lag)	-0.000	-0.000	-0.000	-0.000
	(0.000)	(0.000)	(0.000)	(0.000)
Armed conflict	0.093***	0.082***	0.360	0.119***
	(0.015)	(0.014)	(0.201)	(0.030)
Last election competitiveness	0.014	0.018	-0.063	0.062**
	(0.010)	(0.010)	(0.141)	(0.021)
GDP per capita, PPP (lag)	0.000	0.000	-0.000	0.000
	(0.000)	(0.000)	(0.000)	(0.000)
U.S. foreign aid to GDP ratio (lag)	-0.004**	-0.003*	-0.010	-0.004
	(0.001)	(0.001)	(0.019)	(0.003)
Year	0.009**	0.011***	0.047	0.020**
	(0.003)	(0.003)	(0.045)	(0.007)
Constant	-18.932**	-22.594***	-94.364	-39.747**
	(6.605)	(6.206)	(90.280)	(13.454)
Observations	924	917	924	917
R^2	0.157	0.109	0.160	0.105

Standard errors in parentheses

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

with all else equal, an increase in a country's civil liberties score by one standard deviation would lead to a 2.8 percentage point increase in shutdown number in a given year. Model 3, however, has a much larger negative coefficient; the same increase in civil liberty score *decreases* the number of shutdowns in a given year by 18.7 percentage points. These different results demonstrate just how sensitive the sample is to India, especially for the effects on the number of shutdowns. In Model 3, the sheer number of shutdowns India, a democracy with a relatively free and open media environment, carries out each year drags down the coefficient. This effect of India on the coefficient for the civil liberties score is visually clear when we

compare the standardized coefficient plots for these models in Figures 1 and 2 on the next page.

My models find a lot of support for the path dependency hypothesis. The data shows that governments that have used internet kill-switch shutdowns in the past frequently turn to them again as a tool for controlling the flow of information. The dummy for whether a country has ever experienced a kill-switch shutdown had a significant effect on the presence of shutdowns at the 0.01 level in Models 1 and 2, and had a significant effect on the number of shutdowns a country experienced at the 0.05 level in Model 4, where India was excluded. A prior shutdown increased the likelihood of another one by 7.4 points (a 176% change) in Model 1, and by 6.8 points (a 134% change) in Model 2. The Model 2 results tell us that for the prior shutdown variable, we can see that India is not completely driving the relationship. While prior shutdowns did not have a significant impact on the number of shutdowns when India was included (Model 3), excluding India for Model 4 revealed a larger positive coefficient at a lower level of statistical confidence: all else equal, prior shutdowns increases the number of shutdowns per country-year by 12 percentage points. Shutdowns in the preceding year also had significant positive relationships with kill-switch shutdowns in three models. In Model 1, a shutdown in the preceding year made the presence of a shutdown 15.2 percentage points more likely at the 0.001 confidence level. However, in Model 2 (with India excluded), shutdowns in the preceding year had no significant effect on shutdown presence. Differences between these two models can be compared visually in the standardized coefficient plots in Figures 3 and 4 on the following page. In Model 3, shutdowns in the preceding year led to an additional 5.5 internet shutdowns at the 0.001 confidence level. Referring back to Table 1, earlier in this paper, it is clear that India has had shutdowns in more consecutive years than just about every country, so it follows that the effect on shutdown number would be so strong in Model 3. However, with India excluded in

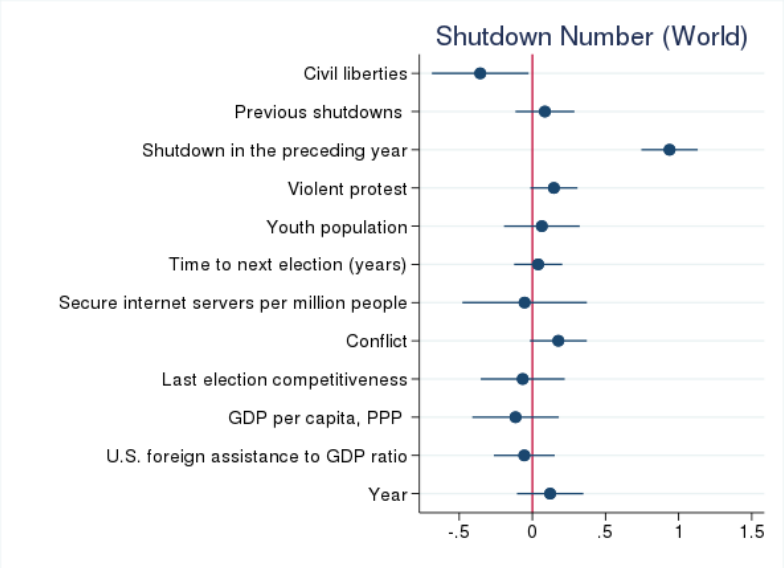


Figure 1. The standardized coefficient plot showing the effects of my independent variables on the number of kill-switch shutdowns in all countries (Model 3). All variables except conflict and violent protest are lagged to the previous year. All independent variables have been standardized with a mean of 0 and a standard deviation of 1 to determine their relative effects. The mean level of the number of KS shutdowns is 0.23 across country-years. The x-axis shows the relative increase in number of shutdowns.

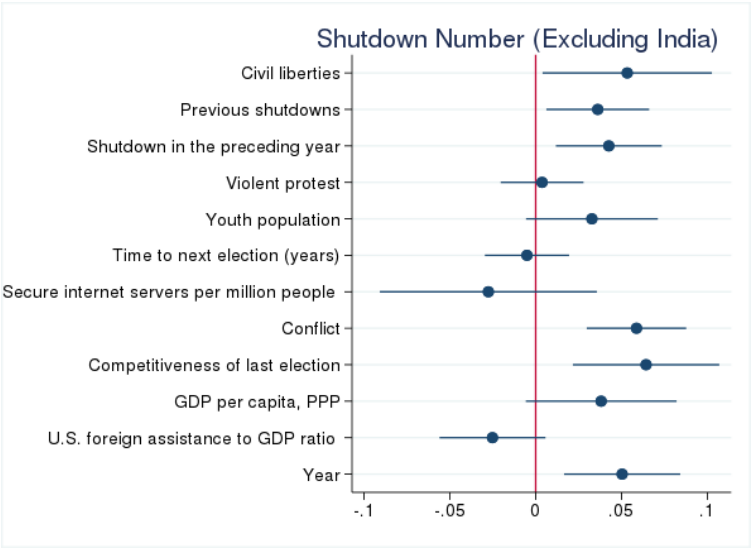


Figure 2. The standardized coefficient plots showing the effects of my independent variables on the number of kill-switch shutdowns in all countries except India (Model 4). All variables except conflict and violent protest are lagged to the previous year. All independent variables have been standardized with a mean of 0 and a standard deviation of 1 to determine their relative effects. The mean level of the number of KS shutdowns is 0.23 across country-years. The x-axis shows the relative increase in number of shutdowns.

Model 4, we see a more modest figure for most other country-years: a shutdown in the preceding year led to a 25 percentage point increase in the number of shutdowns at the 0.01 confidence level. There are several reasons this could be the case, but one reason could be that after governments have enacted a shutdown in a preceding year and have developed the technological and political ability to do so, they learn to not only enact a shutdown again, but to enact a higher number of shutdowns at a more local level, so as to accrue the political benefits of a shutdown without the high economic costs of cutting off a whole country's or region's internet. This has been the case with India, which explains the huge coefficient in Model 3.

One of the most interesting findings this data shows contradicts one of the hypotheses put forward earlier. Violent protest does not seem to be a strong predictor of internet shutdowns. Its coefficients in all four models are close to zero, and it is not statistically significant in any of them. This is quite surprising, given the expectation that states would use shutdowns to counter violent protest mobilization.

The youth bulge hypothesis does not find much support either. The relationship between the size of the youth population and the presence of internet shutdowns (Models 1 and 2) is statistically significant at the 0.05 level. In Model 1, an increase of 1 standard deviation in youth population increases the likelihood of a shutdown by 2.2 percentage points (a 52% increase), and in Model 2, without India, an increase of one standard deviation in youth population size increases shutdown likelihood by 2.1 points (or 57% more likely to occur.) In Models 3 and 4, I cannot reject the null hypothesis and assert that youth population has any effects on a higher number of shutdowns that are not due to random chance.

I also found no statistically significant effects from the time to a country's next election on the presence or number of internet shutdowns. The coefficients were both small and not

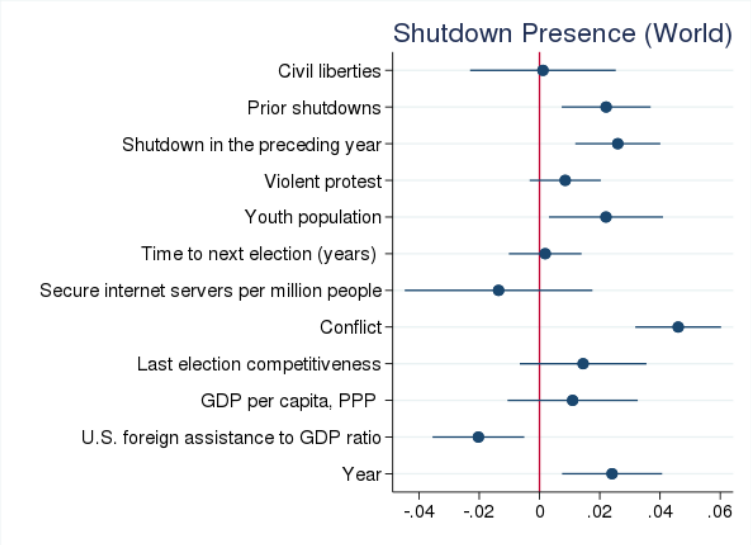


Figure 3. The standardized coefficient plot showing the effects of my independent variables on the presence of kill-switch shutdowns in all countries (Model 1). All variables except conflict and violent protest are lagged to the previous year. All independent variables are standardized with a mean of 0 and a standard deviation of 1 to determine their relative effects. The mean level of the presence of shutdowns is 0.042 (4.2%) across country-years. The x-axis shows the percentage point increase in the likelihood of a shutdown in a given year. Thus, all else being equal, conflict doubles the risk of shutdown (an increase of more than 0.04, or 4 percentage points).

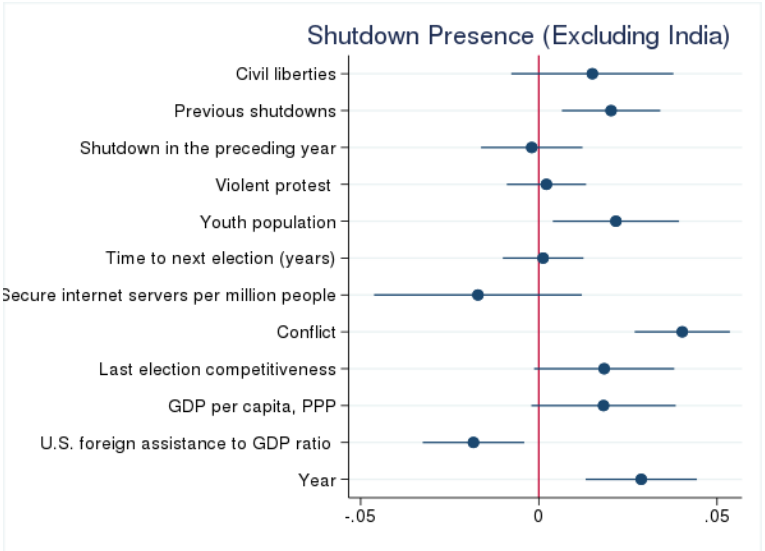


Figure 4. The standardized coefficient plot showing the effects of my independent variables on the presence of kill-switch shutdowns in all countries except India. All variables except conflict and violent protest are lagged to the previous year. All independent variables have been standardized with a mean of 0 and a standard deviation of 1 to determine their relative effects. The mean level of the presence of shutdowns without India is 0.037 (3.7%) across country-years. The x-axis shows the percentage point increase in the likelihood of a KS shutdown in a given year.

significant, so it is quite possible that these effects are only due to chance. Similarly, there was no strong relationship between the number of secure internet servers per million people and the presence or number of internet shutdowns. The variable was not significant in any of the models, so any relationship could still be the result of chance.

Conflict was one of the strongest predictors of shutdowns of all the variables in this analysis: it had significant effects at the 0.001 level in three of the four models. In Model 1, a one standard deviation increase in conflict intensity led to a 4.6 percentage point increase in the likelihood a shutdown would occur, all else equal. In Model 2, without India, a standard deviation increase in conflict intensity also led to a 4 percentage point increase in the likelihood of a shutdown. When looking at the effects of conflict on the number of shutdowns enacted in a given country year, I find a very strong (but not significant) effect in Model 3 when India is included. But in Model 4, where India is excluded, the effect of conflict is both strong and highly significant at the 0.001 confidence level. An increase in conflict intensity leads to an 11.9 percentage point increase in the number of shutdowns in Model 4.

Figures 1 and 2 above demonstrate how when examining the effects on the number of shutdowns, India does drive some of the relationship between conflict and the number of internet shutdowns. Without India, the relationship is weaker but highly statistically significant.

The competitiveness of a country's elections did not have a significant effect on the likelihood of a shutdown occurring in either Model 1 or Model 2, but it did have an impact on the number of internet shutdowns in countries other than India in Model 4. At the 0.01 confidence level, if a country's last election was competitive, it would have a 6.2 percentage point increase in the number of shutdowns it enacted. Comparing across models also shows us that when India is removed from the analysis, the coefficient is calculated with much less error.

The negative sign on the coefficient in Model 3 for this variable is another sign of how sensitive the data is to India, given the sheer number of shutdowns it carries out each year. The other three models support the hypothesis that governments have more of an incentive to shut down the internet around competitive elections, as a tactic to maintain an incumbent's grip on power. Where elections are less free and fair, and opposition parties are barred from contestation, incumbents have less reason to utilize shutdowns.

A country's GDP per capita had an incredibly weak and non-statistically significant relationship with shutdowns in all four models. However, the ratio of U.S. foreign aid a country receives to its GDP had statistically significant effects on the likelihood of shutdowns in Models 1 and 2. In Model 1, a one standard deviation increase in foreign aid led to a decrease in the likelihood of shutdowns by 2 percentage points (a 47% decrease), which was significant at the 0.01 confidence level. With India excluded, in Model 2, foreign aid increases led to a decrease in the likelihood of a shutdown by 1.8 percentage points (a 48% decrease), which was significant at the 0.05 confidence level. The ratio of U.S. foreign aid a country receives to its GDP had a significant negative effect on the likelihood of a kill-switch shutdown in Models 1 and 2, with and without India. This effect is slightly smaller but of less significance in Models 3 and 4, which measure the effects on the number of shutdowns enacted. This is one of this paper's more encouraging findings—there seems to be some possibility to use aid as leverage to encourage regimes to maintain a free and functioning internet for their citizens.

Finally, there is a statistically significant relationship between the year variable and both the presence and number of kill-switch shutdowns. In Models 1 and 2, an increase in the year leads to a 0.9 percentage point (24 %) and 1.1 (30%) percentage point increase in shutdown likelihood, respectively. In Model 1, this is at the 0.01 confidence level, and the 0.001 level in Model 2. In

Model 3, the effect on the number of internet shutdowns is not statistically significant, but when India is excluded in Model 4, each increase in the year variable leads to a 2 percentage point increase in the number of shutdowns that occur, at the 0.01 confidence level. These results support the time trend observed earlier in this paper: internet kill-switch shutdowns have become a much more popular tool for stifling the flow of online information in the last decade.

Because I include the same number of variables in each model, I opted to use the simple r-squared value rather than the adjusted r-squared. The low r-squared values in each of my four models suggests that there is a great deal of variation in the data that they do not explain. There is still much work to be done to determine factors that explain patterns in government internet shutdowns, but finding a lack of evidence for many variables motivated by prevailing theory of internet shutdowns is an important contribution. While this analysis also relies on relatively short panel data (eight years,) the panel is not too short to draw meaningful conclusions from the data that Access Now has collected. As this analysis only relies on random effects and does not look at fixed effects within countries, these findings cannot predict year by year changes in shutdown likelihood within country cases. This work builds a general model that seeks to explain why countries use shutdowns (or do not use shutdowns), rather than attempting to answer why a country does or does not use a shutdown year by year. Better and more available data might make such a project possible in the future.

Another limitation of this quantitative analysis stems from the necessity of using country-level data. Shutdowns occur on a variety of geographic scales and can be executed by everything from the national to municipal level depending on the country in question. Examining all of these kill-switch shutdowns as if they were the same is less realistic but gives a larger sample size and sufficient variation of government-mandated shutdowns. Many of my independent variables are

also only captured at the country level, which makes looking at the geographic scope of a shutdown difficult. Many scholars have already opined about the problems with reducing complex phenomena into simple indicators like Freedom House scores, and even the ethical issues that emerge when scholars try transforming the realities of armed conflict into neat data points and clear-cut categories.[71] By addressing the very real limitations of the data available for this thesis, this can hopefully serve as a starting point for further work into the causes of government internet censorship.

6. Qualitative Analysis

Having identified broad trends in the data on internet shutdowns in the cross-national analysis above, this section of the paper aims to engage in process-tracing to evaluate the mechanisms behind three factors that appear to impact a regime's choice to enact an internet shutdown. The three effects I focus on in this section are those of conflict, competitive elections, and violent protest.] I chose not to qualitatively examine the effects other two significant variables (shutdowns in prior years and the ratio of U.S. foreign assistance to GDP) for two reasons. First, while it is valuable to know that there is a path dependency for countries that implement internet shutdowns, that variable does not help to explain a country's first shutdown; in other words, which factors led a country to start enacting shutdowns in the first place. Systematically understanding which countries stick to shutdowns while others steer away from them is important, but outside the scope of this thesis. I chose not to discuss the effects of aid dependence on the U.S. because of the difficulty of determining a cutoff point for distinguishing between countries that were dependent enough on aid to be ideal case studies. Is there a certain

[71] Valery Tishkov, "Ethnic Conflicts in the Former USSR: The Use and Misuse of Typologies and Data," *Journal of Peace Research* 36, no, 5 (1999); 571-91.

dollar amount, or percentage of GDP, for U.S. assistance that will change the outcome of a shutdown, regardless of the sector to which that aid is allocated? Future iterations of this research could take a closer look at aid from different donors or donor types, as well as the sector to which aid is directed, to better isolate the effects of foreign aid dependence on shutdowns, but that question is currently outside of the scope of this thesis.

6.1 Internet Shutdowns for Conflict Prevention: Bangladesh and Chad

To select cases for this qualitative analysis, I returned to Access Now's dataset of shutdowns, and took note of all countries that experienced conflict that preceded a kill-switch shutdown. I did not take into account the severity of conflict when identifying the universe of cases here; any case with more than 25 battle deaths in a country-year period was included. This left me with 22 country-years. From that point, I ruled out cases where the conflict had preceded the shutdown by more than a year and was less likely to have had directly caused the shutdown. To isolate the potential confounding effects of other factors, I filtered out country-years that experienced violent protest to look strictly at the impact of conflict on the likelihood of shutdown. Two cases emerged from this process that highlight how armed conflict can motivate governments to carry out shutdowns: Bangladesh in 2016 and Chad in 2018. There are two causal pathways by which I would expect conflict to affect internet shutdowns. First, governments might use internet shutdowns to reduce the capacity of armed actors (insurgents or rebel groups) to mobilize against the state. Alternatively, a government might black out online communications if information about a conflict would affect regime legitimacy.

On August 2nd, 2016, the Bangladesh Telecommunications Regulatory Commission (BTRC) enacted a kill-switch internet shutdown in the business district of Dhaka for three and a

half hours as part of an "internet shutdown drill."[72] In addition to the temporary halt of internet services, mobile service providers also tested their abilities to stop voice calls during the drill. The month prior to the shutdown drill, on July 1st, 2016, armed gunmen had attacked a café in the area and killed 20 hostages before security forces were able to storm the building. Authorities had shut off internet to the café during the attack to prevent the perpetrators from communicating with the outside world, but the militants were still able to use SMS messages and phone calls to communicate. During and after the attack, images of the hostages were published by the Islamic State's news agency.[73] After the shutdown in in Dhaka, the chairman of the BTRC announced publicly that this was the first in a series of planned, short-term internet shutdown drills.[74] The drill was accompanied by the blockage of thirty-five news websites, some of which publish articles critical of the government in power.[75]

The Dhaka shutdown was not the first in Bangladesh. The country experienced a 75-minute full shutdown in 2015, which was followed by the blocking of several websites and social media platforms for four weeks.[76] But in the 2016 internet shutdown drills, the primary motivator seemed to be the ability of state security forces to effectively respond to terrorism threats; the BTRC tested whether state forces could still communicate while the internet was down in Dhaka's business district.[77] In the case of similar terrorist threats in the future, the BTRC hoped to use internet shutdowns to limit terrorists' ability to communicate and gain attention from other

---

[72] Zara Rahman, "Bangladesh Shuts Down the Internet, Then Orders Blocking of 35 News Websites," *Advox Global Voices,* August 5, 2016, https://advox.globalvoices.org/2016/08/05/bangladesh-shuts-down-the-internet-then-orders-blocking-of-35-news-websites/.
[73] Shamim Ahamed, "Bangladesh holds internet blackout drill to deal with emergencies like Dhaka terror attack," *bdnews24.com: Bangladesh's First Internet Newspaper,* August 2, 2016, http://bdnews24.com/bangladesh/2016/08/02/bangladesh-launches-internet-blackout-drill-for-emergencies-like-dhaka-attack.
[74] Zara Rahman, "Bangladesh Shuts Down the Internet," 2016.
[75] Ibid.
[76] Ibid.
[77] Ibid.

extremists online. The blockage of opposition news websites, while not an instance of a kill-switch shutdown, provides interesting insight to how states can use different repressive internet tactics in tandem to achieve policy goals. The censorship of certain online news sources may have been an attempt to prevent criticism of how the ruling party had handled the terrorist attack the month before, or to prevent discontent about internet shutdown drills that could lead to protest or other questions of regime legitimacy. Through the Bangladesh case, we can see the type of events—instances of terrorism in a country where political violence is not uncommon—that motivate governments to consider internet shutdowns as a tool for controlling the flow of information in crisis situations. The Bangladesh case is also more clear-cut than many instances of internet kill-switch shutdowns. Whereas some governments will often chalk up an intentional shutdown to technical difficulties, the government openly acknowledged the shutdown. The fact that it was a test demonstrates that the action was premeditated, and that the government was considering the utility of internet shutdowns as a future policy tool.

Next, I turn to Chad's 2018 internet kill-switch for another instance of a shutdown motivated by ongoing violent conflict. Chad faces a precarious security situation, with state forces spread thin fighting rebel groups, conducting counter-terrorism operations, and preventing further ethnic violence between tribes that have fought intermittently since the country gained independence.[78] The Chadian government is further stretched by the hundreds of thousands of refugees from neighboring Sudan and the Central African Republic who are vulnerable to violence, and in many cases, on the brink of starvation.[79] The country's executive branch is

[78] Aanu Adeoye, "Chadians feel 'anger, revolt' as they struggle without internet for one year," *CNN Marketplace Africa*, April 25, 2019, https://www.cnn.com/2019/04/24/africa/chad-internet-shutdown-intl/index.html. Lauren Ploch, "Instability and Humanitarian Conditions in Chad," *Congressional Research Service*, July 1, 2010. https://fas.org/sgp/crs/row/RS22798.pdf

[79] Lauren Ploch, "Instability and Humanitarian Conditions in Chad," 2010.

dominated by the Zaghawa ethnic group from the northeast, including the president, Idriss Deby, who has been in power since 1990.[80] The president's party, the Patriotic Salvation Movement (MPS), also exerts significant influence in Chad's legislature.

In March 2018, the Chadian government conducted a kill-switch shutdown after reforms were announced that would allow Deby to stay in power until 2033.[81] The political opposition had boycotted the conference where the constitutional reforms were announced. While access to the internet was restored shortly thereafter, social media platforms like WhatsApp, Twitter, Facebook, and Viber remained inaccessible for over a year. While there may have been reasons for the shutdown to prevent opposition protest, the director of Internet Without Borders, an organization that ran a campaign for freedom of information in Chad, claimed that the shutdown was to prevent the spread of video footage of conflict among the Zaghawa tribe on WhatsApp and other social media platforms.[82] While I was unable to locate the original video footage that many of the sources coming from Chad described, Francophone bloggers claimed that it contained footage of Salay Deby, the president's younger brother, insulting other prominent members of the Zaghawa group while praising the president and his MPS party.[83] Sources also claimed that rebel factions were particularly active online at this time, which may have contributed to the security concerns that Chad's government cited as the reason for the internet shutdown.

The political and economic control exerted by the Zaghawa and other northern ethnic groups has frustrated many in the southern part of the country that often explodes in instances of

---

[80] U.S. Department of State Overseas Security Advisory Council, "Chad 2019 Crime and Safety Report." *U.S. Department of State*, March 28, 2019, https://www.osac.gov/Country/Chad/Content/Detail/Report/35798eb8-0b8f-4d4c-ad91-15f4aebe2c4f

[81] Aanu Adeyoe, "Chadians feel 'anger, revolt'," 2019.

[82] Ibid.

[83] Ndengar Masbe, "Tchad: les rebelles meancent, Deby coupe l'Internet," Tchad Revolution, April 10, 2018, http://tchadrevolution.over-blog.com/2018/04/tchad-les-rebelles-menacent-deby-coupe-l-internet.html

conflict or violent demonstrations.[84] Given Chad's ongoing fights with rebel groups and history of coup attempts,[85] Deby and his government would thus have strong motivation to cut the internet and limit the spread of the leaked WhatsApp footage if it gave the impression of infighting within the ruling ethnic group. Such infighting could be quickly seized by opposition politicians, rebels planning a time to strike a blow to government forces, or leaders of underrepresented ethnic groups hoping to accumulate more political power by driving a wedge between leaders at a critical moment. Available evidence suggests that the Chadian government used a kill-switch shutdown to prevent the spread of information that would undermine the legitimacy of his regime in a conflict-prone environment, the second causal pathway through which conflict would affect internet shutdowns.

Very few people in Chad have internet access to begin with—according to the World Bank, only about 6.5% of Chadians use the internet.[86] But this case reinforces what other scholars of online repression have suggested: that governments recognize the Internet as a powerful, and potentially dangerous tool for mobilization even at low levels of penetration and usage.[87] Because of the nature of intrastate conflict and political risks (namely coup threats) in Chad, Deby and his associates did not need to fear that the whole country would see content online and revolt in an Arab Spring-style democratizing push. Even just a few political elites among the opposition or from marginalized ethnic groups seeing cracks in the coalition Deby has built over the last three decades would represent a huge political risk and an opening for rebel mobilization or a sudden coup.

---

[84] Arch Puddington, "Freedom in the World 2018," Freedom House, 2019, p. 192. https://freedomhouse.org/sites/default/files/2020-02/FreedomintheWorld2018COMPLETEBOOK_0.pdf
[85] U.S. Department of State Overseas Security Advisory Council, "Chad 2019 Crime and Safety Report," 2019.
[86] World Bank, *Data Bank*, 2020.
[87] Fielder, 2016.

Another interesting facet of the Chad case, however, is that it contradicts some expectations that emerge from the cross-national analysis above. As the presence of western foreign assistance seems to decrease the likelihood of an internet shutdown generally, it is curious that the Chadian government still utilizes kill-switch shutdowns and social media blocking as tools of digital repression, given its close security partnerships with France and the United States. While the relationship identified earlier provides us with reasons for optimism—perhaps aid can be used as leverage to encourage regimes to abandon repressive internet tactics—Chad's kill-switch shutdown and ensuing year-long social media censorship raises the question of whether the opposite is more likely to occur. Perhaps the imminent security threat Chad faces outweighs the influence of its Western security partners. Or perhaps because the United States needs its support to conduct counterterrorism operations, it is willing to turn a blind eye to the repression Deby and the rest of Chad's ruling regime carry out online, even when it violates democratic principles and international law.

6.2 The Null Effects of Protest on Internet Shutdowns: China and Tajikistan

To study the effects—or lack thereof—of violent protest on the likelihood of internet shutdowns more closely, I first excluded all country-years except for those in which there was (1) no shutdown, (2) at least one violent protest, and (3) no other violent conflict that could be a confounding factor or partial reason for the shutdown. This returned a large number of cases, as protests, even violent ones, frequently occur in stable democracies that do not respond with internet shutdowns. To further narrow my search for representative cases that could contribute to the theory about how protests fail to lead governments to internet shutdowns, I further excluded all country-year periods that had *not* had (4) a shutdown in the past. Not only did this help to isolate cases, but allowed me to gain further insight theoretically—why would a government that

had demonstrated itself willing to carry out internet shutdowns in the past not do so in subsequent years in the face of violent protests? Interestingly, the country-year periods that met all four of these criteria fit two 'archetypes:' states with both high and low technological literacy. To process-trace the pathway from violent protest to no shutdown, I selected one of each archetype for qualitative analysis: a state with high technological capacity, China, and Tajikistan, a state with low technological capacity.

China had enacted a kill-switch shutdown in Urumqi, the capital of Xinjiang province, in July 2009 in response to massive protests that devolved into ethnic riots, killing 193 people and injuring thousands more.[88] After Uighur citizens of the province clashed with riot police while protesting judicial discrimination, some rampaged and killed Han Chinese residents over several days. In turn, groups of Han vigilantes later attacked Uighurs in retribution.[89] The relative sizes of the losses on each side are disputed. The protests had been organized via text messages, phone calls, and the internet, according to Chinese authorities, who kept internet services out for ten months to prevent violence and protest from resurging.[90] However, since 2011, China has not carried out a single kill-switch shutdown, despite reports of multiple violent protests in each year from 2011 to 2017, many of which have taken place in Xinjiang province.[91]

One does not have to look far for reasons why crude kill-switch shutdowns are no longer the digital repression tool of choice for the Chinese Communist Party. China is a state with high technological capacity, and it has been able to develop sophisticated practices for censorship and control of online content. Much has been written about "the great firewall of China," the

---

[88] Chris Hogg, "China restores Xinjiang internet," *BBC News Shanghai*. May 14, 2010. http://news.bbc.co.uk/2/hi/asia-pacific/8682145.stm

[89] Edward Wong, "Rumbles on the Rim of China's Empire," *The New York Times Week in Review*, July 12, 2009, https://www.nytimes.com/2009/07/12/weekinreview/12wong.html

[90] Chris Hogg, "China restores Xinjiang internet," 2010.

[91] Olukotun and Micek, 2020. Clark, David and Regan, Patrick, "Mass Mobilization Protest Data,"2016.

draconian censorship laws that keep controversial content out by replacing many of the communication platforms owned by Western companies and used internationally with analogous Chinese ones: Weibo for Twitter, Baidu for Google, and many others.[92] Since Xi Jinping took office as president in 2012, China's government has not only invested in more sophisticated tools for internet filtering, but it has also employed up to two million people to monitor the Chinese internet and take down any content that challenges the Communist Party.[93]

Within Xinjiang province specifically, there is evidence of heavy censorship and surveillance online. In 2011 China introduced WeChat, which quickly became a popular and essential tool for communication across China, including in Xinjiang where a version in the local language was offered. One Uighur scholar stressed the brief moment of freedom that many felt as they became connected to others and could share their beliefs online like never before.[94] This included radical Islamist content, and although it constituted a small minority of content shared on WeChat, it led to swift crackdowns on the Uighur population. Starting around 2014, mentions of Islam or religion on the app could be flags to authorities for surveillance or arrest, as several bombings throughout China were attributed to Uighur militants.[95] In 2016, the regional government of Xinjiang passed stricter controls on online speech, including heavy fines for news websites and platforms that failed to remove false information, or content that mentioned ethnic conflict, terrorism, or violent extremism.[96] At the same time, 160,000 cameras were installed in

---

[92] Elizabeth Economy "The Great Firewall of China: Xi Jinping's Internet Shutdown," The Guardian, June 28, 2019, https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown
[93] Ibid.
[94] Rachel Harris and Aziz Isa, "Islam by Smartphone: the changing sounds of Uyghur religiosity," *Sounding Islam in China*, 2013, http://www.soundislamchina.org/?page_id=1277.
[95] Isobel Cockerell, "Inside China's Massive Surveillance Operation," *WIRED Backchannel*, May 9, 2019, https://www.wired.com/story/inside-chinas-massive-surveillance-operation/.
[96] Edward Wong, "Xinjiang, Tense China Region, Adopts Strict Internet Controls," *The New York Times*, December 10, 2016, https://www.nytimes.com/2016/12/10/world/asia/xinjiang-china-uighur-internet-controls.html.

the regional capital Urumqi, as both online and physical censorship developed in tandem.[97]

Scholars have contended that the huge increases in the size and sophistication of China's tactics to uphold the 'great firewall' have likely made crude internet kill-switch shutdowns obsolete.[98] In a state that has the knowledge and the financial resources to censor critics of the regime online without bearing the massive economic and social costs of blanket shutdowns, it is highly unlikely that the state would see a need to continue the kind of shutdown that occurred in 2009 in Xinjiang. One alternate explanation could be that other than isolated terrorist attacks, China has not seen a period of intense ethnic conflict in Urumqi or Xinjiang as intense as the 2009 riots since that time. While the exact reasons that mass violence has not erupted again are difficult to determine, it is quite possible that the extreme levels of both online and offline repression and surveillance have prevented any such mobilization of discontented Uighurs. While we lack the information to answer whether or not China would enact another full network shutdown again if faced with 2009 levels of extreme interethnic violence, this case highlights an interesting point: that governments willing and able to go to extremes of digital censorship and surveillance may be able to circumvent the situation in which a kill-switch shutdown would be deemed necessary.

Tajikistan, lacks the kind of financial and technological resources that China has been able to utilize instead of kill-switch shutdowns over the last decade. In addition to being one of the world's poorest states, Tajikistan has extremely low levels of internet penetration and technical literacy. This is partially a function of geography: as a landlocked country, Tajikistan has no direct access to the undersea cables that connect states and continents in a truly global

---

[97] James Leibold and Adrian Zenz, "Beijing's Eyes and Ears Grow Sharper in Xinjiang: The 24-7 Patrols of China's 'Convenience Police'," *Foreign Affairs Magazine*, December 23, 2016, https://www.foreignaffairs.com/articles/china/2016-12-23/beijings-eyes-and-ears-grow-sharper-xinjiang

[98] Rydzak, 2018. Zittrain et al., 2017.

internet network, and any extension of the nearest undersea cables (located in Pakistan) over land would have to pass through conflict-torn Afghanistan, which would leave a Tajik internet connection vulnerable to frequent physical line cuts and other attacks.[99] Despite low levels of internet access in the country, Tajikistan's government still enacted a kill-switch shutdown in 2006, timed around the 2006 presidential election in which incumbent Emomali Rahmonov won a third term.[100] The government acknowledged the shutdown and attempted to justify it in the name of quelling unrest and preserving order, but given the timing, attempts to restrict opposition coordination appears to be a more likely cause.[101] Tajikistan also did not fit the theoretical mold of a competitive election—Rahmonov won his third term with 75% of the vote, and Tajikistan's elections are far from free or fair. However, when faced with violent protests in 2012 and then again in 2014, the Tajik government did not carry out another kill-switch shutdown. In examining the Tajik case, the same question arises: why would a state that had used kill-switch internet shutdowns in the past not utilize the same tool of repression in the face of violent protest? Tajikistan does not have the resources, or even a large enough online population, to use tactics as sophisticated as China's.

Tajikistan, however, can still teach us something interesting about internet shutdowns and other internet censorship tactics. Reports from 2014 indicate that while the Tajik authorities did not institute a kill-switch shutdown as they had in 2006, they responded to the threat of violent protests organized by "Group 24" with other repressive internet tactics, namely, blocking

---

[99] Internet Society, "Tajikistan Internet Exchange Point Environment Assessment," *Internet Society*, June 2017, https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-Tajikistan-IXP-assessment.pdf.
[100] Stephanie Wang, "Pulling the Plug: A Technical Review of the Internet Shutdown in Burma," *Open Net Initiative, 2007, https://opennet.net/research/bulletins/013#_ftnref60*.
[101] Olukotun and Micek, 2020.

specific websites and online platforms regularly around times of major political events.[102] Oleg Salimov describes how opposition websites, online news sources, and social media were repeatedly blocked "before Tajikistan's parliamentary elections in the winter of 2010, during Tajikistan's military operation in the Autonomous region of Badakhshan in the summer of 2012, after the President's son Rustam Emomali's wedding in the spring of 2013, before the presidential election in the fall of 2013, and during political protests in Ukraine in the winter of 2014."[103] The blocking of social media platforms does not appear to have an anti-Western bias, as Tajik authorities also frequently block the Russian social media platform Vkontakte as well as Facebook and YouTube.[104]

In response to rumors of planned protest activity in the capital city Dushanbe on October 10, 2014, authorities in Tajikistan blocked the websites of local and international news outlets, opposition parties, as well as Facebook and Vkontakte on October 4th and did not allow access to the blocked sites again until October 11th. While the state telecommunications services denied responsibility for the blockages, the head of one of Tajikistan's ISPs, Asomiddin Atoev, claimed that the action was meant to prevent organized large-scale protests in Dushanbe.[105]

The shift in the internet censorship approach used by the government of Tajikistan between 2006 and 2014 reveals an important finding: a state does not have to be highly

---

[102] Oleg Salimov, "Tajikistan Blocks Radio Ozodi Website," *The Central Asia-Caucasus Analyst: a biweekly briefing on current affairs*, March 5, 2014, http://cacianalyst.org/publications/field-reports/item/12924-tajikistan-blocks-radio-ozodi-website.html.
[103] Oleg Salimov, "Tajikistan Blocks Radio Ozodi Website," 2014.
[104] Ibid.
[105] With this point, it is also important to remember the limitations of the dataset, and how they affect what we see. While in this case study, we still witness violent protests in 2014 Tajikistan, if government internet censorship (kill-switch or otherwise) had actually impeded planned protests, it would not have appeared as linked in the data. For more information, see: Oleg Salimov, "Tajikistan's Government Braces for Protests," *The Central Asia-Caucasus Analyst: a biweekly briefing on current affairs*, October 15, 2014, https://www.cacianalyst.org/publications/field-reports/item/13070-tajikistans-government-braces-for-protests.html.

technologically literate to move away from kill-switch shutdowns to other forms of internet control. Protest movements did not lead to the use of kill-switch shutdowns in Tajikistan, but they did lead to platform-based shutdowns and DNS blocking that the state enacted to try to hamper protest. This insight is critical, because it demonstrates that states do not need the same amount of wealth and technical sophistication as Xi Jinping's Communist Party to move past crude and extreme kill-switch shutdowns. If other forms of internet censorship are within the technical reach of a country as economically and technologically poor as Tajikistan, they are within the grasp of any regime looking to limit the spread of information online through means other than a full network shutdown.

These two cases demonstrating the null effects of violent protest on kill-switch shutdowns contribute some very interesting findings to our understanding of internet censorship. While violent protests do not seem to have led to many full network internet shutdowns in the last decade, China and Tajikistan illustrate that states with any level of technological literacy can easily use other digitally repressive tactics to respond to or pre-empt protest and dissent. The path dependency demonstrated previously in this paper still holds water, but these cases help us to better understand in what situations governments will turn to kill-switch shutdowns time and time again. For now, it seems like many regimes recognize the limited utility of full shutdowns when faced with violent protest but not ongoing armed conflict.

6.3 Competitive Elections and Internet Shutdowns: Sierra Leone 2018

Restricting analysis to cases where a kill-switch shutdown occurred in the presence of a competitive election, but without conflict or protest, filters out all cases but one: the internet shutdown that occurred on the night of Sierra Leone's 2018 runoff for the general election. The election's first round was held on March 7, 2018 and pitted the Sierra Leone People's Party's

(SLPP) Maada Bio against the All People's Congress's (APC) Samura Kamara. While the APC had been the ruling party up until 2018 (and the SLPP its main opposition), Kamara was not the incumbent—the former president Ernest Bai Koroma had served his two-term limit and stepped down. The APC maintained its parliamentary majority, taking 63 out of 132 seats, but no presidential candidate received the 55% of votes necessary for a clear victory in the initial election.[106] Bio and Kamara were separated by less than 15,000 votes and a runoff was scheduled for March 27, 2018.[107] The initial general election had already been fraught with accusations of ballot-tampering,[108] and the runoff was postponed to March 31 after further allegations of fraud and police harassment.[109]

Shortly after polling stations closed on March 31st (at around 10:15 PM), internet and mobile telephone access was restricted throughout Sierra Leone.[110] One internet censorship watchdog group corroborated reports of the shutdown, citing noticeable decreases in Google traffic statistics from Sierra Leone on Saturday, March 31.[111] The shutdown lasted nine hours, and services were reported to be restored around 7:30 in the morning on Sunday.[112] An election

---

[106] Eric Oteng, "Sierra Leone's ruling APC secures parliamentary majority with 63 seats," AfricaNews, March 20, 2018, https://www.africanews.com/2018/03/20/sierra-leone-s-ruling-apc-secures-parliamentary-majority-with-63-seats//.

[107] Abdul Rashid Thomas, "Sierra Leone 2018 elections – taking parliament and losing the presidency," *The Sierra Leone Telegraph*, December 11, 2017, http://www.thesierraleonetelegraph.com/sierra-leone-2018-elections-taking-parliament-and-losing-the-presidency/.

[108] Ahmed Idris, "Sierra Leone postpones runoff vote amid fraud allegations," *Al Jazeera*, March 27, 2018, https://www.aljazeera.com/news/2018/03/sierra-leone-postpones-runoff-vote-fraud-allegations-180327094425423.html

[109] Al Jazeera News, "Sierra Leone: Court puts break on presidential runoff," *Al Jazeera*, March 25, 2018, https://www.aljazeera.com/news/2018/03/sierra-leone-court-pauses-preparations-presidential-run-180324145356398.html.

[110] Sahara Reporters New York, "How Sierra Leonean Government Shut Down Internet, Telephone Services on Election Day," *Sahara Reporters*, April 1, 2018, http://saharareporters.com/2018/04/01/how-sierra-leonean-government-shut-down-internet-telephone-services-election-day.

[111] Abdur Rahman Alfa-Shaban, "Why Sierra Leone temporarily shut down internet after runoff vote," *Africa News*, April 1, 2018, https://www.africanews.com/2018/04/01/why-sierra-leone-temporarily-shutdown-internet-after-runoff-vote//. Maria Xynou et al., "Sierra Leone: Network disruptions amid 2018 runoff elections," *Open Observatory of Network Interference (OONI)*, April 5, 2018, https://ooni.org/post/sierra-leone-network-disruptions-2018-elections/.

[112] Sahara Reporters New York, "How Sierra Leonean Government Shut Down Internet," 2018.

monitoring group, Sierra Leone Decides, reported on Twitter after service returned that the shutdown had been to prevent the national electoral commission from sharing results with party affiliates as votes were counted.[113]

When early reports of the shutdown were published the following morning, the government had not yet made an official statement as to the reason for the shutdown, leaving reporters to theorize about the cause and look to past examples of internet shutdowns timed around elections in African states, namely in the Republic of Congo, Gambia, Chad, and Uganda.[114] Following the shutdown and the electoral victory of the SLPP's Maada Bio, the APC accused Sierra Leone's electoral commission of malpractice and election fraud due to the communications blackout, and the inability of electoral officials to communicate via internet or mobile services as runoff votes were being counted.[115]

The following day, April 2nd, 2018, Sierra Leone's national telecommunications regulatory body released a statement denying responsibility for the shutdown and emphasizing that the Sierra Leone Cable Company (SALCAB) is the entity that manages the country's physical internet cable infrastructure.[116] In its statement, the state telecommunications agency reported that SALCAB had traced the blackout to a problem with a physical submarine cable in Mauritania.[117] However, work from OONI found that while neighboring states that relied on the same submarine cables experienced outages of the internet on March 30th, 2018, the shutdowns on the night of March 31st were inconsistent and likely not caused by damage to physical

---

[113] Abdur Rahman Alfa-Shaban, "Why Sierra Leone temporarily shut down internet after runoff vote," 2018.
[114] Alfa-Shaban, 2018. Africa Freedom of Expression Exchange, "Sierra Leone Joins Global Trend: Shuts Down Internet and Mobile Services during Elections," *Africa Freedom of Expression Exchange*, April 2, 2018, https://www.africafex.org/digital-rights/sierra-leone-joins-global-trend-shuts-down-internet-and-mobile-services-during-elections__trashed.
[115] Sahara Reporters New York, 2018.
[116] Olusegun Ogundeji, "Internet shutdown as Sierra Leone votes," *ITWeb*, April 2, 2018, https://itweb.africa/content/rW1xLv59KZjvRk6m.
[117] Ibid.

undersea cables.[118] With other causes ruled out by the work of NGOs like OONI, and with repeated electoral irregularities reported by Sierra Leonians in 2018, there is reason to believe that the shutdown was premeditated.

As the government of Sierra Leone at no point took responsibility for the shutdown, it is difficult to assert without doubt that the internet shutdown was the result of a government order. Unlike other African regimes that have enacted internet shutdowns around the time of elections, Sierra Leone's government did not claim that it enacted the shutdown for reasons of national security. Neither presidential candidate was an incumbent in 2018, so an internet shutdown was not ordered by the incumbent president as a means of manipulating results to extend his term. The fact that the SLPP opposition candidate narrowly won the runoff vote is also curious—a situation in which the APC shut down the internet to manipulate results in their party's favor would be more clear cut.

While the country has come a long way since the end of its infamously bloody civil war in 2002, Sierra Leone's elections are still ordinarily marred by low-level violence and ethno-regional polarization. The APC has long drawn support from ethnic groups in the north and west, while the SLPP is popular among smaller groups in the south and east parts of the country. In 2007, then-incumbent Ahmad Kabbah threatened to call off the election due to violence, and candidates from both the APC and the SLPP accused the other of voter intimidation.[119]

The reasons why the government of Sierra Leone would carry out an internet shutdown, are unclear, but the reports suggest one potential compelling cause. With widespread reports of electoral regularities and a history of electoral violence between ethnic groups, the time between

---

[118] Maria Xynou et al., "Sierra Leone: network disruptions," 2018.
[119] Africa Research Institute, "Old Tricks, Young Guns: Elections and violence in Sierra Leone*," Africa Research Institute Briefing Note 1102*, April 2011, https://africaresearchinstitute.org/newsite/wp-content/uploads/2013/03/BN-1102-Old-Tricks-Young-Guns1.pdf.

the closing of polls and the announcement of the official result could have held significant danger. If one takes the word of the Sierra Leone Decides election monitoring group's word over that of the country's national telecommunications commission, then it is possible to see why the government would implement a shutdown to prevent the sharing of early results online as votes were counted. The credible threat of riots could motivate the incumbent government to shut off the internet during the vote count even if the APC was not altering ballots in their candidate's favor. Riots and other widespread violence occurred during Sierra Leone's 2007 election, and the greater access to ICTs in 2018 would allow rumors of early election results that could incite violence to spread much more quickly.[120] If their desire to protect citizens from possible violence outweighed their desire to see a fellow member of the APC party assume the presidency, President Komora's outgoing government may have chosen to shut down the internet without infringing on the NEC's ballot-counting.

Further, the case of Sierra Leone clarifies an important distinction that the quantitative data had obscured. Process tracing helps to more accurately pinpoint the timing and methods a government uses to enact a shutdown. The timing of this shutdown to occur while votes were being *counted* rather than *cast* in a close runoff election is a quite different strategy than the hypothesis I had initially expected to see: that states would use shutdowns before elections to limit the ability of opposition parties to mobilize. The fact that in this case, the blackout of internet only occurred after polls had closed, suggests that a different relationship between kill-switch shutdowns and competitive elections: that shutdowns may serve as a tool for obscuring electoral interference as well as countering mobilization and silencing dissent.

[120] While the percentage of Sierra Leone's population that uses the internet regularly still hovers around 10%, mobile phone subscriptions have skyrocketed from 12 per 100 people in 2007 to 88 per 100 people in 2018. (World Bank)

7. Conclusion

More and more governments have begun using kill-switch shutdowns to address misinformation, conflict, and unrest in the last decade. These shutdowns have debilitating social and economic costs and threaten human rights around the world. As internet kill-switch shutdowns become a popular policy tool in autocracies and democracies alike, it is crucial to better understand the factors that influence governments in their decision to shut down the internet in times of crisis. This thesis has presented several findings of interest: first, it confirms that there is a time trend at play in the spread of internet kill-switch shutdowns globally, and that a regime that uses internet shutdowns once is much more likely to do so again. Second, it suggests that while violent protest does not serve as a strong predictor of whether a government will shut down the internet, armed conflict makes intentional internet shutdowns much more likely. Competitive national elections also emerge as a likely cause for shutdowns, as incumbents have motivations to prevent oversight of election counting if opposition parties are allowed to contest. Finally, foreign assistance provided by the United States is associated with fewer internet shutdowns—while it is currently unclear if foreign aid is a direct cause of regimes' aversion to shutdowns, it suggests that the international community can play a role in setting norms against internet shutdowns and using international finance to encourage a more democratic and open internet internationally.

The implications of these findings are relevant for policymakers as well as academics. The potential to reduce internet shutdowns through linkage and leverage provides us with a cause for optimism. While this study did not separate out the effects of humanitarian aid from democratization assistance, funding that targets building democratic institutions and protecting media freedoms may help to mitigate the use of costly and extreme internet control tactics.

There are several steps that future researchers looking to understand the phenomenon of kill-switch shutdowns could take to build on this work. First, as mentioned in the methodology section, the inability to differentiate between shutdowns at different geographic scales is a major limitation of this paper, and future research should look to explore the potential different causes of shutdowns at varying local, regional, and national levels. Developing data tools to accurately measure the costs of an internet shutdown would also allow for a better understanding of the cost-benefit analysis that regimes are faced with when they consider whether or not to shut off the internet. Currently, scholars have an idea of what factors to consider in calculations in shutdown cost,[121] but disputes over how to define and measure a state's "digital economy" make it difficult to develop precise measures. As the internet now permeates almost all financial transactions and businesses, and not just those in the information technology sectors, accurately measuring the size of online economies around the world becomes both more complicated and more important. Another potential avenue for future research would be analyzing the extent of cross-border spread of internet shutdowns over time. Some scholars have argued that events outside a state's borders could influence its domestic internet censorship policies, whether those events are the existence of regional conflicts, or internet censorship practices by neighboring states that set an example for their effective use.[122] Others have noted the spread of internet shutdowns as a tactic for countermobilizing against conflict within cases over time.[123] Scholars looking to analyze kill-switch shutdowns in the future should consider the potential for cross-border spread of particular internet shutdown measures.

---

[121] Darrell M. West, "Internet shutdowns cost countries $2.4 billion last year," *Brookings Center for Technology Innovation*, October 2016. Kathuria et al., 2017. Abdi Latif Dahir, "Internet shutdowns continue to cost Africa's economies," data from *The Collaboration on International ICT Policy in East and Southern Africa*, *The Atlas*, 2018, https://theatlas.com/charts/S1LpT9ci-.

[122] Rydzak, 2018. Zittrain et al., 2017.

[123] Wagner, 2018. Kathuria et al., 2018.

Bibliography

Adeoye, Aanu. “Chadians feel ‘anger, revolt’ as they struggle without internet for one year.” *CNN Marketplace Africa*. April 25, 2019. https://www.cnn.com/2019/04/24/africa/chad-internet-shutdown-intl/index.html

Africa Research Institute. “Old Tricks, Young Guns: Elections and violence in Sierra Leone.” *Africa Research Institute Briefing Note 1102*. April 2011. https://africaresearchinstitute.org/newsite/wp-content/uploads/2013/03/BN-1102-Old-Tricks-Young-Guns1.pdf.

African Freedom of Expression Exchange. “Sierra Leone Joins Global Trend: Shuts Down Internet and Mobile Services During Elections.” *African Freedom of Expression Exchange*. April 2, 2018. https://www.africafex.org/digital-rights/sierra-leone-joins-global-trend-shuts-down-internet-and-mobile-services-during-elections__trashed

Ahamed, Shamim. “Bangladesh holds internet blackout drill to deal with emergencies like Dhaka terror attack.” *bdnews24.com: Bangladesh’s First Internet Newspaper.* August 2, 2016. http://bdnews24.com/bangladesh/2016/08/02/bangladesh-launches-internet-blackout-drill-for-emergencies-like-dhaka-attack

Alfa-Shaban, Abdur Rahman. “Why Sierra Leone temporarily shut down internet after runoff vote.” *Africa News*. April 1, 2018. https://www.africanews.com/2018/04/01/why-sierra-leone-temporarily-shutdown-internet-after-runoff-vote//

Al Jazeera News, “Sierra Leone: Court puts break on presidential runoff,” *Al Jazeera*, March 25, 2018, https://www.aljazeera.com/news/2018/03/sierra-leone-court-pauses-preparations-presidential-run-180324145356398.html.

Bowman, Warigia and Camp, L. Jean. “Protecting the Internet from Dictators: Technical and Policy Solutions to Ensure Online Freedoms.” *The Innovation Journal: The Public Sector Innovation Journal*, 18(1), 2013, article 3. http://www.ljean.com/files/Dictators.pdf

Clark, David and Regan, Patrick, "Mass Mobilization Protest Data." *Harvard Dataverse, V3*. 2018. https://doi.org/10.7910/DVN/HTTWYL.

Clinton, Hillary. “Internet Rights and Wrongs: choices and challenges in a networked world.” *Remarks at George Washington University*. February 15, 2011. http://diritto-comunicazione.decesare.info/Hillary-Clinton_George-Washington-Univ_15_02_11.pdf

Cockerell, Isobel. “Inside China’s Massive Surveillance Operation.” *WIRED Backchannel*. May 9, 2019. https://www.wired.com/story/inside-chinas-massive-surveillance-operation/

Coppedge, Michael et al. “V-Dem [Country-Year/Country-Date] Dataset v9” *Varieties of Democracy (V-Dem) Project*. 2019. https://doi.org/10.23696/vdemcy19.

Coppedge, Michael et al. “V-Dem Codebook v9.” *Varieties of Democracy (V-Dem) Project*. 2019.

Dahir, Abdi Latif. “Internet shutdowns continue to cost Africa’s economies.” data from *The Collaboration on International ICT Policy in East and Southern Africa*, *The Atlas*. 2018. https://theatlas.com/charts/S1LpT9ci-.

Davenport, Christian. “State Repression and Political Order.” *Annual Review of Political Science*, 10, 2007, pp.1-23. https://www.annualreviews.org/doi/abs/10.1146/annurev.polisci.10.101405.143216

Deibert, Ronald et al. "Measuring Global Internet Filtering," in *Access Denied: The Practice and Policy of Global Internet Filtering*. *MITP*. 2008. pp.5-27.

Economy, Elizabeth. “The Great Firewall of China: Xi Jin Ping’s internet shutdown.” *The Guardian.* June 29, 2018. https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown

Fielder, James. “The Internet and Dissent in Authoritarian States” in Conflict and Cooperation in Cyberspace: The Challenge to National Security. *Taylor & Francis.* April 19, 2016.

Freedom House. “Country and Territory Ratings and Statuses: 1973-2020.” *Freedom House.* Last accessed April 23, 2020. https://freedomhouse.org/report/freedom-world

Freedom House. “Freedom in the World Methodology.” *Freedom House*. Last accessed April 23, 2020. https://freedomhouse.org/reports/freedom-world/freedom-world-research-methodology

Freyburg, Tina and Garbe, Lisa. “Blocking the Bottleneck: Internet Shutdowns and Ownership at Election Times in Sub-Saharan Africa.” *International Journal of Communication* 12, 2018, pp. 3896-3916. https://www.alexandria.unisg.ch/255303/1/XXX_Bottleneck-Paper.pdf

Gleditsch, Nils Petter, Peter Wallensteen, Mikael Eriksson, Margareta Sollenberg, and Havard Strand. “Armed Conflict 1946-2001: A New Dataset.” *Journal of Peace Research* 39(5), 2002.

Greitens, Sheena. “Authoritarianism Online: What Can We Learn from the Internet in Non-Democracies?” *Political Science & Politics*, 2013.

Gruhn, Diana. “Why Do I Need an SSL/TLS Certificate?” *Entrust Datacard Blog*. March 5, 2019. https://www.entrustdatacard.com/blog/2019/march/ssl-certificates-101-why-do-i-need-an-ssl-tls-certificate.

Gunitsky, Seva. “Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability.” *Perspectives on Politics* 13, no. 1 (2015): 42–54. doi:10.1017/S1537592714003120.

Griffiths, James. “Democratic Republic of Congo internet shutdowns shows how Chinese internet censorship tactics are spreading.” *CNN*. January 2, 2019. https://edition.cnn.com/2019/01/02/africa/congo-internet-shutdown-china-intl/index.html

Halliday, Josh. “UAE to tighten Blackberry restrictions.” *The Guardian*. April 18, 2011. https://www.theguardian.com/technology/2011/apr/18/uae-blackberry-emails-secure

Harris, Rachel and Isa, Aziz. “Islam by Smartphone: the changing sounds of Uyghur religiosity.” *Sounding Islam in China*. 2013. http://www.soundislamchina.org/?page_id=1277

Hogg, Chris. “China restores Xinjiang internet.” *BBC News Shanghai*. May 14, 2010. http://news.bbc.co.uk/2/hi/asia-pacific/8682145.stm

Howard, P. N., Agarwal, S. D., & Hussain, M. M. (2011a). “The dictators’ digital dilemma: When do states disconnect their digital networks?” Retrieved from https://papers.ssrn.com/sol3/papers.cfm ?abstract_id=2568619

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

Human Rights Watch. “Myanmar: Internet Shutdown Risks Lives.” *Human Rights Watch*. June 28, 2019. https://www.hrw.org/news/2019/06/28/myanmar-internet-shutdown-risks-lives#

Idris, Ahmed. “Sierra Leone postpones runoff vote amid fraud allegations.” *Al Jazeera*. March 27, 2018. https://www.aljazeera.com/news/2018/03/sierra-leone-postpones-runoff-vote-fraud-allegations-180327094425423.html

Internet Society. “Tajikistan Internet Exchange Point Environment Assessment.” *Internet Society*. June 2017. https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-Tajikistan-IXP-assessment.pdf.

Kathuria, Rajat et al. “The Anatomy of an Internet Blackout: Measuring the Economic Impact of Internet Shutdowns in India.” *Indian Council for Research on International Economic Relations*. April 2018. https://think-asia.org/bitstream/handle/11540/8248/Anatomy_of_an_Internet_Blackout.pdf?sequence=1

Kedzie, Christopher. *Communication and Democracy: Coincident Revolutions and the Emergent Dictators*. Santa Monica, CA: RAND Corporation, 1997. https://www.rand.org/pubs/rgs_dissertations/RGSD127.html.

Klensin, J. “Network Working Group, Paper 3467: Role of the Domain Name System.” *The Internet Society*. 2003. https://tools.ietf.org/html/rfc3467

Leberknight, Christopher S., Mung Chiang and Felix Ming Fai Wong. "A Taxonomy of Censors and Anti-Censors Part II: Anti-Censorship Technologies," *International Journal of E-Politics (IJEP)* 3 (2012): 4, accessed (April 26, 2020), doi:10.4018/jep.2012100102

Leibold, James and Zenz, Adrian. “Beijing’s Eyes and Ears Grow Sharper in Xinjiang: The 24-7 Patrols of China’s ‘Convenience Police’.” *Foreign Affairs Magazine*. December 23, 2016. https://www.foreignaffairs.com/articles/china/2016-12-23/beijings-eyes-and-ears-grow-sharper-xinjiang

Levitsky, Steven, and Lucan A. Way. "Linkage versus Leverage. Rethinking the International Dimension of Regime Change." *Comparative Politics* 38, no. 4 (2006): 379-400. Accessed April 27, 2020. doi:10.2307/20434008.

Lieberman, Evan S. “Nested Analysis as a Mixed-Method Strategy for Comparative Research.” *American Political Science Review* 99, no. 3 (2005): 435–52. doi:10.1017/S0003055405051762.

Masbe, Ndengar. "Tchad: les rebelles meancent, Deby coupe l'Internet," *Tchad Revolution*, April 10, 2018, http://tchadrevolution.over-blog.com/2018/04/tchad-les-rebelles-menacent-deby-coupe-l-internet.html

Mukeredzi, Tonderayi. "Uproar over Internet Shutdowns: Governments Cite Incitements to Violence, Exam Cheating and Hate Speech." *Africa Renewal: Africa Section of the UN Department of Public Information, August – November 2017*. August 21, 2017. https://www.jpanafrican.org/docs/vol10no10/10.10-3-Mukeredzi.pdf

Nordås, R. and Davenport, C. "Fight the Youth: Youth Bulges and State Repression." *American Journal of Political Science*, 57: 926-940, 2013. doi:10.1111/ajps.12025

Odhiambo, Sharon Anyango. "Fake News Dominates Ahead of Kenya's Elections." *Africa Up Close: a blog of the Africa Program at the Wilson Center*. August 4, 2017. https://africaupclose.wilsoncenter.org/fake-news-dominates-ahead-of-kenyas-elections/

Organization of Economic Cooperation and Development. "Toolkit for Measuring the Digital Economy – Draft Verson." *G20 Summit Argentina 2018*. November 2018. http://www.oecd.org/g20/summits/buenos-aires/G20-Toolkit-for-measuring-digital-economy.pdf

Olukotun, Deji Bryce and Micek, Peter. "Shutdown Tracker Optimization Project (STOP) Dataset." *Access Now and the #KeepItOn Coalition*. Accessed February 2020.

Ogundeji, Olusegun. "Internet shutdown as Sierra Leone votes." *ITWeb*. April 2, 2018. https://itweb.africa/content/rW1xLv59KZjvRk6m

Eric Oteng. "Sierra Leone's ruling APC secures parliamentary majority with 63 seats." *Africa News*. March 20, 2018. https://www.africanews.com/2018/03/20/sierra-leone-s-ruling-apc-secures-parliamentary-majority-with-63-seats//.

Pemstein, Daniel et al. "The V-Dem Measurement Model: Latent Variable Analysis for Cross-National and Cross-Temporal Expert-Coded Data." *V-Dem Working Paper* No. 21. 4th edition. University of Gothenburg: Varieties of Democracy Institute. 2019.

Pettersson, Therese, Högbladh, Stina, and Öberg, Magunus. "Organized violence 1989-2018 and peace agreements." *Journal of Peace Research* 56(4). 2019.

Pierskalla, Jan H. and Hollenbach, Florian M. "Technology and Collective Action: The Effect of Cell Phone Coverage on Political Violence in Africa." *American Political Science Review* 107:2 (2013), pp.207-224. doi:10.1017/S0003055413000075

Ploch, Lauren. "Instability and Humanitarian Conditions in Chad," *Congressional Research Service*. July 1, 2010. https://fas.org/sgp/crs/row/RS22798.pdf

Puddington, Arch. "Freedom in the World 2018." Freedom House. 2019. p. 192. https://freedomhouse.org/sites/default/files/2020-02/FreedomintheWorld2018COMPLETEBOOK_0.pdf

Marshall, Monty G, Gurr, Tedd Robert, and Jaggers, Keith. “Polity IV Project: Political Regime Characteristics and Transitions, 1800-2016. Dataset Users’ Manual.” *Center for Systemic Peace*. https://www.systemicpeace.org/inscr/p4manualv2016.pdf

Rahman, Zara. “Bangladesh Shuts Down the Internet, Then Orders Blocking of 35 News Websites.” *Advox Global Voices*. August 5, 2016. https://advox.globalvoices.org/2016/08/05/bangladesh-shuts-down-the-internet-then-orders-blocking-of-35-news-websites/

Rydzak, Jan. “The Digital Dilemma in War and Peace: Determinants of Digital Network Shutdown in Non-Democracies.” *Under review.* 2018.

Rydzak, Jan. “Of Blackouts and Bandhs: The Strategy and Structure of Disconnected Protest in India.” Stanford University Working Paper. February 7, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3330413

Sahara Reporters New York. “How Sierra Leonean Government Shut Down Internet, Telephone Services on Election Day.” *Sahara Reporters*. April 1, 2018. http://saharareporters.com/2018/04/01/how-sierra-leonean-government-shut-down-internet-telephone-services-election-day

Salimov, Oleg. “Tajikistan Blocks Radio Ozodi Website.” *The Central Asia-Caucasus Analyst: A biweekly briefing on current affairs*. March 5, 2014. http://cacianalyst.org/publications/field-reports/item/12924-tajikistan-blocks-radio-ozodi-website.html

Salimov, Oleg. “Tajikistan’s Government Braces for Protests.” *The Central Asia-Caucasus Analyst: A biweekly briefing on current affairs*. October 15, 2014. http://cacianalyst.org/publications/field-reports/item/13070-tajikistans-government-braces-for-protests.html

Sanchez, Conor. “The Link Between More Internet Access and Frequent Internet Shutdowns.” *Net Politics Blog, The Council on Foreign Relations*. August 22, 2018. https://www.cfr.org/blog/link-between-more-internet-access-and-frequent-internet-shutdowns

Scartascini, Carlos, Cruz, Cesi, and Keefer, Phillip. The Database of Political Institutions 2017 (DPI 2017). *The Inter-American Development Bank*. https://publications.iadb.org/en/database-political-institutions-2017-dpi2017

Subramanian, Ramesh. “The Growth of Global Internet Censorship and Circumvention: A Survey.” *Communications of the International Information Management Association (CIIMA)*, Volume 11, Issue 2, 2011. (October 31, 2011). http://dx.doi.org/10.2139/ssrn.2032098

Sutterlin, Elizabeth. “Mob Violence, Mobile Phones: Private Messaging and the Future of Peacekeeping.” *The Project on International Peace and Security*. 2019.

Tishkov, Valery. “Ethnic Conflicts in the Former USSR: The Use and Misuse of Typologies and Data,” *Journal of Peace Research* 36, no, 5 (1999); 571-91.

Thomas, Abdul Rashid. “Sierra Leone 2018 elections – taking parliament and losing the presidency.” *The Sierra Leone Telegraph*. December 11, 2017. http://www.thesierraleonetelegraph.com/sierra-leone-2018-elections-taking-parliament-and-losing-the-presidency/

Tufecki, Zeynep. “New Media and the People-Powered Uprisings.” *Technology Review*. 2011.

United African Partnership for Democratic Change. “Chad Blocks Facebook Messenger and BBC.” *UAPDC Blog*. April 9, 2018. https://www.uapdc.com/new-blog/2018/4/9/chad-blocks-facebook-messenger-and-bbc

United Nations Office of the High Commissioner of Human Rights. “Joint Declaration on Freedom of Expression and responses to conflict situations.” *United Nations Office of the High Commissioner of Human Rights*. May 4, 2015. https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=15921&LangID=E

U.S. Agency for Global Media. “USAGM launches independent internet freedom grantee.” *U.S. Agency for Global Media*. November 25, 2019. https://www.usagm.gov/2019/11/25/usagm-launches-independent-internet-freedom-grantee/.

U.S. Agency for International Development. “Foreign Aid Explorer: The official record of U.S. foreign aid.” *U.S. Agency for International Development*. https://explorer.usaid.gov/data

U.S. Department of State Bureau of Democracy, Human Rights, and Labor. “2019 Country Reports on Human Rights Practices: Chad.” *U.S. Department of State*. 2019. https://www.state.gov/reports/2019-country-reports-on-human-rights-practices/chad/

U.S. Department of State Overseas Security Advisory Council. “Chad 2019 Crime and Safety Report.” *U.S. Department of State*. March 28, 2019. https://www.osac.gov/Country/Chad/Content/Detail/Report/35798eb8-0b8f-4d4c-ad91-15f4aebe2c4f

VPN Privacy Services. “Social media like WhatsApp, Facebook Messenger, and Viber have been blocked in Chad.” *Medium.com*. April 10, 2018. https://medium.com/@vpnprivacy.services/social-media-like-whatsapp-facebook-messenger-and-viber-have-been-blocked-in-chad-several-days-5703d4365950

Wagner, Ben. “Understanding Internet Shutdowns: A Case Study from Pakistan.” *International Journal of Communication* 12(2018), 3917–3938. https://ijoc.org/index.php/ijoc/article/view/8545/2465

Wang, Stephanie. “Pulling the Plug: A Technical Review of the Internet Shutdown in Burma,” *Open Net Initiative*. 2007. https://opennet.net/research/bulletins/013#_ftnref60.

West, Darrell M. “Internet shutdowns cost countries $2.4 billion last year.” *Brookings Center for Technology Innovation*. October 2016. http://witnessradio.org/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf

Wilson, Steven Lloyd. "How to control the Internet: Comparative political implications of the internet's engineering." *First Monday*, Volume 20, Number 2:2 (February 2015). http://dx.doi.org/10.5210/fm.v20i2.5228

Wong, Edward. "Rumbles on the Rim of China's Empire." *The New York Times Week in Review*. July 12, 2009. https://www.nytimes.com/2009/07/12/weekinreview/12wong.html

Wong, Edward. "Xinjiang, Tense China Region, Adopts Strict Internet Controls." *The New York Times*. December 10, 2016. https://www.nytimes.com/2016/12/10/world/asia/xinjiang-china-uighur-internet-controls.html.

World Bank. "World Development Indicators." *World Bank Data Bank.* https://data.worldbank.org/

Xynou, Maria et al. "Sierra Leone: Network disruptions amid 2018 runoff elections." *Open Observatory of Network Interference (OONI).* April 5, 2018. https://ooni.org/post/sierra-leone-network-disruptions-2018-elections/.

Zittrain, Jonathan et al. "The Shifting Landscape of Global Internet Censorship." *Berkman Klein Center Research Publication* No. 2017-4; Harvard Public Law Working Paper No. 17-38. June 1, 2017. http://dx.doi.org/10.2139/ssrn.2993485

Appendix A: Correlation Matrix for All Independent Variables

	Past Shutdown	Shutdown in the prior year	Media Freedom	Regime Type	Protest	Violent Protest	Online Population	Youth Population	Time to next election	Election year dummy	Last election comp.	Election comp. dummy	Lag GDP per capita	Lag conflict	Lag servers per mill.	Aid to GDP lag
Past shutdown	1.0000															
Shutdown in prior year	0.5284	1.0000														
Media freedom	0.3189	0.1241	1.0000													
Regime Type	-0.3182	-0.0693	-0.8178	1.0000												
Protest	0.0383	0.0191	-0.0128	0.0748	1.0000											
Violent Protest	0.0514	0.0532	0.0530	0.0219	0.8237	1.0000										
Online Population	-0.0972	-0.0962	-0.5977	0.3746	0.0248	-0.0841	1.0000									
Youth Population	0.0442	0.1058	0.5217	-0.2812	-0.0514	0.0506	-0.8368	1.0000								
Time to next election	0.0140	-0.0437	0.0587	-0.0367	-0.0031	-0.0038	-0.1244	0.0837	1.0000							
Election dummy	0.0307	0.0591	0.0324	-0.0395	0.0011	0.0001	0.0464	-0.0182	-0.6740	1.0000						
Last election comp.	-0.2159	-0.0035	-0.6619	0.7972	0.0167	0.0076	0.1900	-0.0931	-0.0290	-0.0289	1.0000					
Election comp. dummy	-0.2573	-0.0023	-0.5645	0.7017	-0.0142	-0.0106	0.0829	0.0229	-0.0226	-0.0064	0.8742	1.0000				
Lag GDP per capita	-0.1481	-0.0902	-0.5246	-0.2827	0.0201	-0.0780	0.8036	-0.7140	-0.0955	0.0413	0.1392	0.0577	1.0000			
Lag conflict	0.2596	0.2836	0.3819	-0.1929	0.0543	0.0382	-0.2240	0.2292	0.0033	0.0174	-0.1511	-0.2242	-0.2129	1.0000		
Lag servers per mill.	-0.0829	-0.0469	-0.2900	0.1780	-0.0238	-0.0704	0.3785	-0.3368	-0.0589	0.0092	0.1098	0.0630	0.4771	-0.1064	1.0000	
Aid to GDP lag	-0.0414	-0.0196	0.1845	-0.0968	-0.0073	0.0012	-0.2822	0.2760	0.0712	-0.0359	-0.1072	-0.0991	-0.2227	0.2167	-0.0750	1.0000