2018-12

DIGITAL REPRESSION AND CONFLICT VIOLENCE

Foote, Colin J.

Monterey, CA; Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

DIGITAL REPRESSION AND CONFLICT VIOLENCE

by

Colin J. Foote

December 2018

Thesis Advisor: Ryan Maness
Co-Advisor: T. Camber Warren

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2018	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE DIGITAL REPRESSION AND CONFLICT VIOLENCE			**5. FUNDING NUMBERS**
6. AUTHOR(S) Colin J. Foote			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

Digital repression of political speech gained prominence during the Arab Spring when governments acknowledged the power of networked collective action. The shutdown strategies that proliferated from the Arab Spring expanded around the globe. Now, almost a decade later, India leads the world in government-mandated digital repression. The rapid expansion of the internet and mobile penetration, combined with long-standing civil unrest, created a volatile issue within India. The use of strategic shutdowns by Indian authorities attempts to contain and reduce the conflict-related violence while limiting collateral economic damage. To investigate such efforts, this thesis examines patterns of civil violence across Indian states in the wake of digital repression events. This research employs both quantitative and qualitative approaches to analyze the relationship between violence and digital shutdowns using data on civil unrest, including protests, riots, military operations, and digital shutdowns in India. The evidence indicates that while the goal of India's use of strategic shutdowns is to contain and reduce conflict-related violence, strategic shutdowns actually result in increased violence in the days following the shutdown event. These findings indicate that shutting off the internet and cell phone services is not an effective approach to preventing internal violence.

14. SUBJECT TERMS digital repression, violence, India, internet, cyber, social media, civil unrest, civil resistance, protests, suppression, freedom of the net, regression analysis			**15. NUMBER OF PAGES** 77
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

DIGITAL REPRESSION AND CONFLICT VIOLENCE

Colin J. Foote
Major, United States Army
BA, Norwich University, 2007

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF SCIENCE IN DEFENSE ANALYSIS
(IRREGULAR WARFARE)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2018**

Approved by: Ryan Maness
Advisor

T. Camber Warren
Co-Advisor

John J. Arquilla
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Digital repression of political speech gained prominence during the Arab Spring when governments acknowledged the power of networked collective action. The shutdown strategies that proliferated from the Arab Spring expanded around the globe. Now, almost a decade later, India leads the world in government-mandated digital repression. The rapid expansion of the internet and mobile penetration, combined with long-standing civil unrest, created a volatile issue within India. The use of strategic shutdowns by Indian authorities attempts to contain and reduce the conflict-related violence while limiting collateral economic damage. To investigate such efforts, this thesis examines patterns of civil violence across Indian states in the wake of digital repression events. This research employs both quantitative and qualitative approaches to analyze the relationship between violence and digital shutdowns using data on civil unrest, including protests, riots, military operations, and digital shutdowns in India. The evidence indicates that while the goal of India's use of strategic shutdowns is to contain and reduce conflict-related violence, strategic shutdowns actually result in increased violence in the days following the shutdown event. These findings indicate that shutting off the internet and cell phone services is not an effective approach to preventing internal violence.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACLED	Armed Conflict and Event Dataset
AIC	Akaike Information Criterion
BJP	Bharatiya Janata Party
DDoS	Distributed Denial of Service
ECD	Electronic Civil Disobedience
ICT	Information Communication Technology
IFJ	International Federation of Journalists
IIDS	Indian Institute of Dalit Studies
IRCG	Iranian Revolutionary Guard Corps
ISP	Internet Service Providers
LOIC	Low Orbit Ion Canon
SC/ST	Scheduled Castes/Scheduled Tribes
SFLC	Software Freedom Law Centre
SMS	Short Messaging Service
STEM	Science, Technology, Engineering, and Mathematics
UNESCO	United Nations Educational, Scientific and Cultural Organization
VPN	Virtual Private Networks
WCIT	World Conference on International Telecommunication

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

First, I would like to take a moment to thank my wife for enduring through this thesis with me, helping me edit and proofread while always being willing to lend an ear to my endless talks on digital repression, protests, and India. I also would like to say a special thank you to my advisors, Dr. Camber Warren and Dr. Ryan Maness—none of this would be possible without them. Their guidance and encouragement made this process truly enjoyable (and relatively painless). Finally, I would like to thank the Defense Analysis Department—this was a great experience, thank you.

THIS PAGE INTENTIONALLY LEFT BLANK

I. THE AGE OF DIGITAL LIBERATION, DIGITAL REPRESSION AND NETWORKED COLLECTIVE ACTION

A. THE INTERSECTION OF THE INFORMATION AGE AND SOCIAL MOVEMENTS

Since the onset of the Information Age, networked collective action has been the most prominent form of uprising in modern social movements. States, especially authoritarian states, are increasingly efficient at suppressing online dissidents' ability to plan, coordinate and mobilize social movements, despite the global proliferation of information and communication technology (ICT). While the battle for digital control of information between dissidents and states swings back and forth, states appear to be gaining the upper hand.[1]

Both the 2009 Green movement in Iran, and in early 2011 the Arab Spring, demonstrated to the world the power behind online tools for collective action in recent uprisings.[2] More than seven years later the repression of online dissidents is steadily increasing as a result, primarily in authoritarian states. Less discussed is how repression is evolving in democracies as well.

B. THE RISE OF NETWORKED COLLECTIVE ACTION

The Information Age has established the cyber domain as a prominent component of statecraft. As the technology matures, there is an international race between states to acquire digital tools, as both offensive weapons and defensive barriers to maintain relevance in this new global environment. The unique aspect of this human made domain is that it has opened a space that previously did not exist, empowering networked

[1] Steven Heydemann and Reinoud Leenders, "Authoritarian Learning and Authoritarian Resilience: Regime Responses to the 'Arab Awakening,'" Globalizations 8, no. 5 (October 1, 2011): 647–53, https://doi.org/10.1080/14747731.2011.621274.

[2] Negar Mottahedeh, #iranelection: Hashtag Solidarity and the Transformation of Online Life, 1st edition (Redwood City, CA: Stanford Briefs, 2015); Zeynep Tufekci, *Twitter and Tear Gas: The Power and Fragility of Networked Protest* (New Haven ; London: Yale University Press, 2017).

individuals to challenge nation-states in the information battle. Digital tools are not only available to states but also by non-state actors.

The digital age is also ushering in a new era of collective action, marked by its ability to rapidly network collective grievances and establish new media outlets that challenge conventional state media. It is important to note that the spread of ICTs does not necessarily correlate to peace, but also increases in violence.[3] Unquestionably, the Arab spring demonstrated to the world the power of networked protests. Before the Arab Spring, internet activism was coined as "slacktivism" by both autocratic and democratic countries around the world and "authorities in many countries had derided the internet and digital technology as 'virtual' and therefore unimportant."[4] However, when network enabled protests struck the world in 2011, many regimes did not initially crack down harder on the movements before they began to mobilize and eventually gave way to revolutions.[5] The surge that was the Arab spring swept the world, and with it, a new era of repression emerged as states quickly learned to mobilize effective defenses against this subversive behavior. Now there is a simmering race between dissidents and states to dominate the digital domain, as the balance of power slides back and forth. On this new power dynamic in the cyber landscape, Larry Diamond states in his article "Liberation Technologies", "Authoritarian states could commandeer digital ICT to a similar effect. To the extent that innovative citizens can improve and better use these tools, they can bring authoritarianism down—as in several cases they have."[6]

Organized movements are not a new phenomenon, "Collective actions, social movements, and revolutions are woven into the fabric of human history. They are studied at great length and for a good reason: they change history."[7] Cyber tools and platforms

---

[3] T. Camber Warren, "Explosive Connections? Mass Media, Social Media, and the Geography of Collective Violence in African States," *Journal of Peace Research* 52, no. 3 (May 2015): 297–311, https://doi.org/10.1177/0022343314558102.

[4] Tufekci, *Twitter and Tear Gas,* 16.

[5] Tufekci, *Twitter and Tear Gas,* 16.

[6] Larry Diamond, "Liberation Technology," *Journal of Democracy* 21, no. 3 (July 14, 2010): 69–83, https://doi.org/10.1353/jod.0.0190.

[7] Tufekci, *Twitter and Tear Gas, xix.*

have adjusted the landscape and lowered the threshold of participation so that anyone with connectivity can take part in the movement. It is also critical to understand that social movements are not only harnessed by revolutionaries seeking social change and states seeking control, but also by "terrorist groups such as ISIS and white-supremacist's groups in North America and Europe … to gather, organize, and amplify their narrative."[8] The convoluted, yet organized chaos which is the cyber domain continues to evolve, but one thing remains true throughout the literature: there is power in the rapid diffusion of information, and the next global struggles around the world will have to consider the liberation or repression aspects of the cyber domain.

C. DIGITAL LIBERATION

Despite the recent attention stemming from the Arab Spring on networked collective action, the concept of using computers for activism existed both in theory and practice well before the first tweet in the Twitter revolutions. In 1994, the Critical Arts Ensemble (CAE) published an essay about the use of cyberspace and technology for direct activism, by replicating traditional civil disobedience techniques such as blocking streets and transferring it into the cyberspace by blocking the digital streets (or digital access). The essay, titled "Electronic Civil Disobedience" or (ECD) would become a center post for future networked collective actions to use.[9] Groups, such as the *electrohippies* in the late 1990s would use Distributed Denial of Service or ("DDoS") techniques to conduct "virtual sit-ins."[10] Molly Sauter writes that "Hacktivists considered the primary goal of hacktivism or technology-based activism to be defeating state censorship and the disruption of online communications via the creation and distribution of tools to evade censorious regimes."[11]

---

[8] Tufekci, *Twitter and Tear Gas, xix.*

[9] Molly Sauter and Ethan Zuckerman, *The Coming Swarm: DDOS Actions, Hacktivism, and Civil Disobedience on the Internet* (New York; London: Bloomsbury Academic, 2014), 41.

[10] Sauter and Zuckerman, 39-40.

[11] Sauter and Zuckerman, 46-47.

In 1998, John Perry Barlow in his statement, "Cyberspace Independence Declaration" summarized sentiments that would sweep the world during the social media enhanced revolutions in the Arab Spring,

> Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature, and it grows itself through our collective actions.[12]

The statement is idealistic, and not entirely accurate as we have seen states slowly establish borders around their networked cyberspace, but it still encapsulates the battle of liberation and repression that is currently sweeping the technological world. Unquestionably there is a draw the pulls a global response to isolated repression events.

Digital liberation has given way to new media, which has allowed people to report on news independently, expose corruption, express opinions and mobilize protests transnationally and at a faster speed of information diffusion than has ever been possible.[13] Liberation technology is defined as physical ICT's and digital ICTs: The physical ICTs encompass computers, internet, cell phones to the more modern advances such as smartwatches. On the digital side, ICTs consist of Facebook, Twitter, Snapchat, Reddit and the ever-evolving ecosystem of "new social media."[14] Employing ICTs to promote change is not a new concept, as the telegraph and printing press also had revolutionary effects on how social movements organized and structured while demonstrating how interconnected the world is.[15]

---

[12] John Perry Barlow, "A Declaration of the Independence of Cyberspace," Electronic Frontier Foundation, January 20, 2016, https://www.eff.org/cyberspace-independence.

[13] Diamond, "Liberation Technology."

[14] Diamond, "Liberation Technology."

[15] Clay Shirky, "The Political Power of Social Media: Technology, the Public Sphere, and Political Change," *Foreign Affairs* 90, no. 1 (2011): 28–41.

Literature continually reinforces that ICTs alone are not enough to create revolutionary change, but they have altered the revolutionary process.[16] Zeynep Tufecki states in her book, *Twitter and Tear gas—the Power and Fragility of Networked Protests*, that, "Technology rarely generates novel human behavior; rather, it changes the terrain on which such behavior takes place. Think of it as the same players, but on a new board game."[17] Zeynep Tufecki's profound statement on the duality of how the digital domain is both fundamentally different and similar at the same time for modern revolutions. In the same tone, it is important to not fall into the reductive notion of "technodeterminiation" or that by existing, ICTs cause revolutions, but rather acknowledge that technology can influence the structures that make revolutions possible.[18]

The primary role that ICTs play in both democratic and autocratic societies alike is filling the void that journalists typically fill and acting as a counter voice to the state.[19] While freedom of the press enables democratic countries to hold governments accountable, ICTs are bridging the gap and providing this transparency in autocratic governments and raising the standard of information in democratic societies simultaneously. Every protester with a cell phone or internet access can document and record events in real-time, allowing for global consumption of the information. However, Brian J. Bowe notes in his article, "Cosmopolitanism, and Repression of Cyber-Dissent in the Caucasus" that "activists do not have complete control of the situation and often must rely on Western information and social network corporations to provide the tools that facilitate dissent."[20] The reliance on western technology is highlighted by the recent international call on the U.S. to ease its policy surrounding ICTs and sanctions, specifically with Iran, to enable networked

---

[16] Daniel P. Ritter and Alexander H. Trechsel, "Revolutionary Cells: On the Role of Texts, Tweets, and Status Updates in Nonviolent Revolutions," in *Conference on "Internet, Voting and Democracy," Laguna Beach, CA*, vol. 3 (Citeseer, 2011).

[17] Tufekci, *Twitter and Tear Gas*, 131.

[18] Tufekci, *Twitter and Tear Gas*, 119.

[19] Brian J. Bowe and Robin Blom, "Cosmopolitanism and Repression of Cyber-Dissent in the Caucasus: Obstacles and Opportunities for Social Media and the Web," *Journal of Media Sociology*, 2011, 5.

[20] Bowe and Blom, "Cosmopolitanism and Repression."

collective action.[21] Technology companies concerned with the penalties associated with allowing their products to be used in Iran typically resort to blocking out Iran entirely.[22]

Existing literature has also explored the area of hacker's targets and motivations, often aligned with the behavior being deviant and rebellious, primarily focusing on boosting self-esteam, online credibility.[23] However, there is an area of hacking used to further revolutionary agendas that are less studied, but still impactful: this form of hacking is called hacktivism.[24] DDoS is the primary tool used by hacktivists due to its relatively low technical skill required for entry. Hacktivist collectives publicly distribute two DDoS toolkits available for hackers to participate in the global collective action. The first one is Electronic Disturbance Theater's (EDT) FloodNet tool and the second one is Anonymous's Low Orbit Ion Cannon (LOIC).[25] These tools allow activists to leverage technology against states to create effects that will enable for collective action to coalesce. The damage caused by DDoS is temporary, usually consisting of bumping a government site offline, but the result typically draws global attention through media responses and transnational participation through botnets (allowing a computer's use for DDoS actions).

DDoS techniques are not the only tool available for networked collective action. Virtual Private Networks (VPN) also have a significant contribution to enabling the mobilizing structure of online social movements. VPN's allow people to bypass government blocks and surveillance by obscuring the transfer of information over the internet. VPNs are typically easy to install, again allowing for minimal technology understanding to employ and disguise a user's "IP address" and allows access to the

---

[21] Peter Harrell and Collin Anderson, "U.S. Sanctions Abet Iranian Internet Censorship," *Foreign Policy* (blog), accessed February 3, 2018, https://foreignpolicy.com/2018/01/22/u-s-sanction-abet-iranian-internet-censorship/.

[22] Firuzeh Mahmoudi and Fereidoon Bashar, "Tech Companies Are Complicit in Censoring Iran Protests | WIRED," accessed February 6, 2018, https://www.wired.com/story/tech-companies-are-complicit-in-censoring-iran-protests/.

[23] Victor Asal et al., "Repression, Education, and Politically Motivated Cyberattacks," *Journal of Global Security Studies* 1, no. 3 (August 1, 2016): 235–47, https://doi.org/10.1093/jogss/ogw006.

[24] Victor Asal et al., "Repression, Education, and Politically Motivated Cyberattacks," 235–47.

[25] Sauter and Zuckerman, *The Coming Swarm*, 109-110.

internet through an encrypted channel, which in turns opens sites that are usually blocked out by autocratic governments such as Twitter and Facebook.[26]

Along with DDoS and VPN's, Tor is another popular tool in a dissident's collection. Tor is a highly encrypted browser that creates both anonymity and circumvention of state censorship.[27] The complexity of Tor makes it a challenge for states to block out completely is the process slowly evolves into a "whack-a-mole" scenario, as one gets shut down another one springs up.

D. DIGITAL REPRESSION

Even with all the easily accessible tools for modern uprisings, states can respond with more resources and resiliency. The digital repression tools states have at their disposal fall into two categories: active and passive measures to counter networked collective action.

Active measures consist of physical limitations, ranging from turning off the internet within the country, blocking sites or programs used by dissidents and using ICTs to target and remove dissidents entirely physically. Passive measures are often subtle in nature and consist of adjusting the narrative of a social movement, overwhelming the movement with misinformation or completely blacking out information from having a global reach.

Anita R. Gohdes, in her article "*Pulling the plug: Network disruptions and violence in civil conflict,"* argues that governments fighting to hold political control have significant incentive to turn off the internet. Additionally, the cost of killing the internet is less than if the international community responds to atrocities discovered through ICT means.[28] Literature indicates that short-term internet shutdowns are often employed to impede movements in their ability to mobilize and coordinate. Large-scale movements often use

[26] Tufekci, *Twitter and Tear Gas*, 221-229.

[27] Tufekci, *Twitter and Tear Gas*, 230.

[28] Anita R. Gohdes, "Pulling the Plug: Network Disruptions and Violence in Civil Conflict," *Journal of Peace Research* 52, no. 3 (May 1, 2015): 352–67, https://doi.org/10.1177/0022343314551398.

Twitter or texting services to coordinate mass demonstrations or marches, as the Internet Service Providers (ISP) and cell providers usually fall under the purview of the state, they are relatively easy to turn off, but it often comes with a financial cost. When Egypt shut off the internet during the Arab Spring in 2011, the estimated cost to the government was $90 million.[29] Studies show that if states use this extreme technique multiple times, social movements begin to anticipate the military action that traditionally follows an internet crackdown and use it as an "early warning" indicator.[30] Furthermore, in the case of Egypt cutting off the internet entirely resulted in two additional outcomes. The first outcome was people already mobilized in Tahrir Square no longer needed the platforms to organize, and second, people who were unaware of the severity of the situation were plunged into the middle of it the moment the lights went out, forcing people out of their homes and into the streets.[31]

On the less severe side of physical digital repression is content filtering and blocking, which is employed through firewalls and national Internet Service Providers (ISP).[32] These techniques can be heightened and lowered with minimal notice from the global perspective, but on the other hand, these techniques are relatively easy for dissidents to combat. Traditional VPNs or encrypted web browsers such as Tor can quickly defeat these methods of repression, although states are responding with increased effectiveness as seen with the "Great Firewall of China,"[33] or the Red Web in Russia, which involves pulling all websites under the .ru domain and creating digital country boundaries.[34] Furthermore, states can increase or decrease the internet traffic speed within their countries, which is even harder for protesters to deter, such as in Iran when the Ministry of

[29] Gohdes, "Pulling the Plug: Network Disruptions and Violence in Civil Conflict."

[30] Gohdes, "Pulling the Plug: Network Disruptions and Violence in Civil Conflict."

[31] Tufekci, *Twitter and Tear Gas*. 226

[32] Leonie Maria Tanczer, Ryan McConville, and Peter Maynard, "Censorship and Surveillance in the Digital Age: The Technological Challenges for Academics," *Journal of Global Security Studies* 1, no. 4 (November 1, 2016): 346–55, https://doi.org/10.1093/jogss/ogw016.

[33] Tanczer, McConville, and Maynard, "Censorship and Surveillance in the Digital Age: The Technological Challenges for Academics."

[34] Andrei Soldatov and Irina Borogan, *The Red Web: The Kremlin's Wars on the Internet*, Reprint edition (PublicAffairs, 2017).

Information ordered all ISPs to limit the private use and internet café use to 128Kbps and commercial use to 512 Kbps.[35] Regulating bandwidth hindered gathering protests while the business sector and to a greater extent, the economy, was not damaged.

On the active side of repression, regimes can use ICT's to trace locations of weblog writers or activists and conduct arrests. The Iranian Revolutionary Guard Corps (IRCG) Cyber Force is mainly known for employing this tactic. Additionally, research shows that regimes can counter activists by sending messages infected with viruses, trojans, and keyloggers.[36]

On the passive measure aspect of digital repression, states can employ techniques such as how IRCG "Basijis" encourage the development of weblogs "to confront cultural invasion and promote Islamic and government-favored content on the Internet."[37] Narrative control can have both a positive effect on the state employing the technique and a demoralizing impact on the political activists attempting to counter this method.

Ultimately the battle between states and dissent is continuously evolving, and academic research has focused primarily on autocracies. In contrast, how democracies are employing repression tools, and how effective they are, has been far less studied.

[35] Saeid Golkar, "Liberation or Repression Technologies? The Internet, the Green Movement and the Regime in Iran," *International Journal of Emerging Technologies and Society; Hawthorn* 9, no. 1 (2011): 50–70.

[36] Golkar, "Liberation or Repression Technologies? The Internet, the Green Movement and the Regime in Iran."

[37] Golkar, "Liberation or Repression Technologies? The Internet, the Green Movement and the Regime in Iran."

THIS PAGE INTENTIONALLY LEFT BLANK

II. THE RISING TIDE OF INTERNET REPRESSION IN INDIA

> The rules India makes for its online users are highly significant – for not only will they apply to 1 in 6 people on earth in the near future as more Indians go online, but as a global power they will shape future debates over freedom of expression online.[38]

A. INDIA: AUTOCRATIC STRATEGIES OF REPRESSION USED IN A DEMOCRACY?

Academic literature focuses almost exclusively on autocracies' use of repression against internet freedom in the modern age of networked collective action.[39] The growing reality is that the steady decline of internet freedom is not only occurring in autocracies, but democracies as well are feeling the pressure of closing up the internet to ensure public safety.[40] The golden age of seeing a globally interconnected exchange of ideas ushering in a new era of peace seems to have altered course, as technology has had marginal impacts on both shifting nation-states toward democracies, and cultures toward peace.[41] This rising trend is especially evident in India, where one of the largest populations of the world is quickly coming online as internet penetration continues to increase in rural areas.[42] Additionally, India is also rapidly becoming a significant player in the Science, Technology, Engineering, and Mathematics (STEM) community, placing second in the

---

[38] Index on Censorship, "India: Digital Freedom under threat?" Index on Censorship (blog), November 21, 2013, https://www.indexoncensorship.org/2013/11/india-online-report-freedom-expression-digital-freedom/.

[39] Anita R. Gohdes, "Studying the Internet and Violent Conflict," Conflict Management and Peace Science 35, no. 1 (January 2018): 89–106, https://doi.org/10.1177/0738894217733878.

[40] *Managing Democracy in the Digital Age: Internet Regulation, Social Media Use, and Online Civic Engagement*, edited by Julia Schwanholz, Todd S. Graham, and Peter-Tobias Stoll; Brandon Valeriano, "'Closing That Internet Up': The Rise of Cyber Repression," Council on Foreign Relations, accessed May 4, 2018, https://www.cfr.org/blog/closing-internet-rise-cyber-repression; "India Country Report | Freedom on the Net 2017," November 14, 2017, https://freedomhouse.org/report/freedom-net/2017/india; Warren, "Explosive Connections?"

[41] Warren, "Explosive Connections?"; Michael L. Best and Keegan W. Wade, "The Internet and Democracy: Global Catalyst or Democratic Dud?," *Bulletin of Science, Technology & Society* 29, no. 4 (August 2009): 255–71, https://doi.org/10.1177/0270467609336304; "PolityProject," accessed May 6, 2018, http://www.systemicpeace.org/polityproject.html.

[42] "India Country Report | Freedom on the Net 2017."

number of STEM graduates in 2016, behind China and far ahead of the United States per capita.[43] India's quick rise, combined with long-standing civil unrest within the state, has created a boiling point in which authorities in India have imported tactics learned from autocracies during the Arab spring and transposed them into laws to be employed nationwide.[44] India now dominates the world in internet shutdowns, and according to *AccessNow*'s research, India consisted of 47% of the total global internet shutdowns from 2016 to 2017.[45] This chapter will explore how India has institutionalized internet shutdowns as a strategy to combat issues of collective action, rumor control, contain violence and attempt to protect counter-terrorism activities by employing existing Indian law to operationalize this capability at the state level.

B. DIGITALIZING INDIA

India is the second most populated country in the world, just behind China, and consists of 17% of the world's total population.[46] Population growth projections have India overtaking China by 2025.[47] While internet penetration in India only includes 33% of the country's population in 2017, mobile penetration has dramatically spread across the country, reaching 92% in 2017.[48] Even with only 33% of the population having an internet connection, India still ranks second in the number of internet subscribers, following closely behind China and having surpassed the United States in 2017.[49] The rapid growth of the technology sector and the advancement of internet infrastructure within the country has reached a fever pitch; the evolution of the networked progress is likely caused by the global

[43] Niall McCarthy, "The Countries with The Most STEM Graduates [Infographic]," Forbes, accessed May 4, 2018, https://www.forbes.com/sites/niallmccarthy/2017/02/02/the-countries-with-the-most-stem-graduates-infographic/.

[44] Henrik Urdal, "Population, Resources, and Political Violence: A Subnational Study of India, 1956–2002," Journal of Conflict Resolution 52, no. 4 (August 2008): 590–617, https://doi.org/10.1177/0022002708316741.

[45] "#KeepItOn," *Access Now* (blog), accessed May 4, 2018, https://www.accessnow.org/keepiton/.

[46] "United Nations Population Division | Department of Economic and Social Affairs," accessed May 6, 2018, http://www.un.org/en/development/desa/population/.

[47] "United Nations Population Division | Department of Economic and Social Affairs."

[48] "India Country Report | Freedom on the Net 2017."

[49] "India Country Report | Freedom on the Net 2017."

understanding that ICTs have positive effects on economic growth, with the most substantial increase resulting from the high-speed internet.[50] In a recent academic study *Quantifying the Value of an Open Internet for India* by Rajat Kathuria, Mansi Kedia, Vatsala Shreeti and Parnil Urdhwarshe concluded that "according to a new estimate a 10% increase in internet subscribers results in an increase of 2.4% in growth of state per capita GDP."[51] While on the other side of ICTs, research has determined that internet shutdowns have caused an economic loss of $968 million in India.[52] The question remains, how effective are internet shutdowns if knowing the financial loss associated with them, they are still a common tactic in India to contain civil unrest?

C. INDIA'S LEGAL JUSTIFICATION FOR INTERNET REPRESSION

During the World Conference on International Telecommunication (WCIT) in 2012, India stood starkly against a global internet model which allocates more control to national governments, more commonly understood as internet sovereignty, which was proposed by China, Iran, and Russia. Internet sovereignty contrasts with the European and Western countries approach, which is known as a multi-stakeholder model.[53] While internally India was steadily shifting toward methods more often used by those countries it opposed in the 2012 WCIT. The rise of strategic shutdowns is commonly observed in political protests in full autocracies such as Syria, Iran, Russia, and China, setting this aside, India has joined the international circle of internet shutdown countries and has quickly overtaken them in quantity and duration by 2017.[54]

Analyzing the heart of the legal justification for the use of strategic internet shutdowns within India, it is first essential to know where India sits globally regarding polity, freedom of the Net and state fragility. In 2016 the Polity IV project scored India as

---

[50] Rajat Kathuria et al., "Quantifying the Value of an Open Internet for India," *ICRIER*, accessed May 4, 2018, http://icrier.org/pdf/open_Internet.pdf.

[51] Rajat Kathuria et al, "Quantifying the Value of an Open Internet for India."

[52] West, Darrell M. *Internet Shutdowns Cost Countries $2.4 Billion Last Year.*

[53] Agur, Colin and Subramanian, Ramesh and Belair-Gagnon, Valerie, "Interactions and Policy-Making: Civil Society Perspectives on the Multistakeholder Internet Governance Process in India."

[54] "#KeepItOn."

a full democracy on the Polity scale.[55] The 2016 fragility index score places India in the top 30% of fragile states, likely resulting from the high level of civil unrest located in the Kashmir region combined with the longstanding confrontational posture against Pakistan.[56] The non-profit organization Freedom House's considers India's internet "partly free" citing some concerns with obstacles to access, and violation of users rights but overall not overly limited on content blocking.[57] While the scores have stabilized since 2014, the use of strategic shutdowns is on an exponential rise, depicted in Figure 1, with data collected by the Software Freedom Law Centre, India.[58] The number of shutdowns and growth rate is significantly more than any other country in the world.[59]

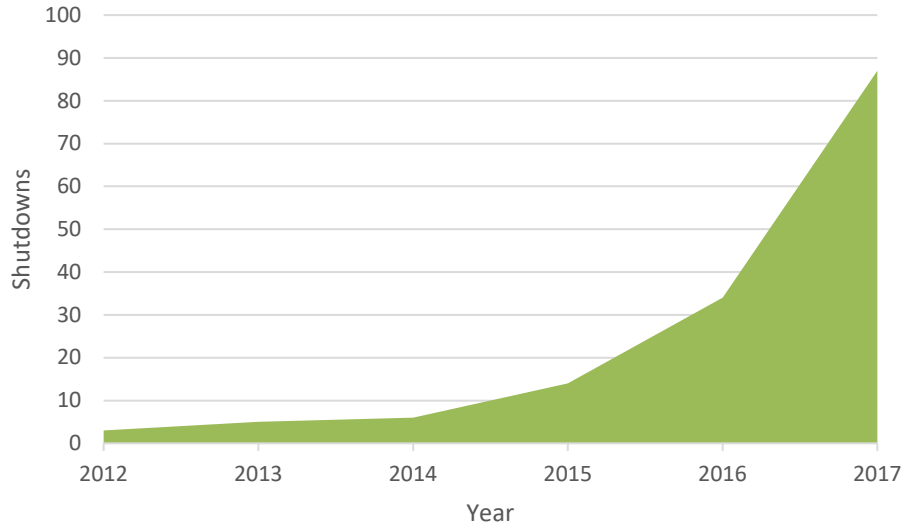

Figure 1. India Internet Shutdowns[60]

[55] "Center for Systemic Peace," accessed February 7, 2018, http://www.systemicpeace.org/index.html.

[56] Monty G. Marshall and Gabrielle Elzinga-Marshall, "TABLE 1: STATE FRAGILITY INDEX AND MATRIX 2016," 2016, 10.

[57] "India Country Report | Freedom on the Net 2017."

[58] "Internet Shutdowns in India," accessed May 6, 2018, https://internetshutdowns.in.

[59] "#KeepItOn."

[60] Adapted from "Internet Shutdowns in India," accessed May 6, 2018, https://internetshutdowns.in.

The rise of internet shutdowns correlated with higher penetration of mobile and internet coverage across the country, combined with the learning processes of implementing new and old laws to fit the modern environment. There are two primary laws Indian authorities use to shut down the internet. The first is known as Section 69A of the IT Act (established in 2008) which states.

> 69A Power to issue directions for blocking for public access of any information through any computer resource. -
>
> (1) Where the Central Government or any of its officer specially authorized by it in this behalf is satisfied that it is necessary or expedient so to do, in the interest of sovereignty and integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-section (2) for reasons to be recorded in writing, by order, direct any agency of the Government or intermediary to block for access by the public or cause to be blocked for access by the public any information generated, transmitted, received, stored or hosted in any computer resource.[61]

While Section 69A authorizes the Secretary of the Department of Information Technology to block internet access without delay in an emergency, the order must be reviewed and approved by a more extensive committee within 48 hours.[62] With this said, according to a study on laws criminalizing expression online in Asia, even with the ease of using 69A authorities are turning to an older law to order internet shutdowns across the country, known as Section 144 of the Criminal Code of Procedure.[63] Section 144 of The Code of Criminal Procedure, 1973 states:

---

[61] "Section 69A in The Information Technology Act, 2000," accessed May 6, 2018, https://indiankanoon.org/doc/10190353/.

[62] "Unshackling Expression: A Study on Laws Criminalizing Expression Online in Asia – The Internet Democracy Project," accessed May 4, 2018, https://internetdemocracy.in/reports/unshackling-expression-a-study-on-laws-criminalising-expression-online-in-asia/.

[63] "Unshackling Expression: A Study on Laws Criminalizing Expression Online in Asia – The Internet Democracy Project."

> 144. Power to issue order in urgent cases of nuisance of apprehended danger.
>
> (1) In cases where, in the opinion of a District Magistrate, a Sub- divisional Magistrate or any other Executive Magistrate specially empowered by the State Government in this behalf, there is sufficient ground for proceeding under this section and immediate prevention or speedy remedy is desirable, such Magistrate may, by a written order stating the material facts of the case and served in the manner provided by section 134, direct any person to abstain from a certain act or to take certain order with respect to certain property in his possession or under his management, if such Magistrate considers that such direction is likely to prevent, or tends to prevent, obstruction, annoyance or injury to any person lawfully employed, or danger to human life, health or safety, or a disturbance of the public tranquility, or a riot, of an affray.
>
> (2) An order under this section may, in cases of emergency or in cases where the circumstances do not admit of the serving in due time of a notice upon the person against whom the order is directed, be passed ex parte.
>
> (3) An order under this section may be directed to a particular individual, or to persons residing in a particular place or area, or to the public generally when frequenting or visiting a particular place or area.[64]

Despite Section 144 being an older law, it is still useful for authorities, as it only requires the order of a police commissioner, and can be enforced for up to two months, with state government being able to extend the order to six months.[65] Furthermore, the same study on censorship laws in Asia found that section 144 is primarily used during social or political unrest to shut down the internet.[66] Some concern arose out of the extensive use of section 144, as some saw it as an opportunity for political misuse. In February 2016, a law student in India, Gaurav Sureshbhai Vyas, challenged the states' broad power to shutdown the internet and mobile services, but the Indian Supreme Court

[64] "Section 144 in The Code of Criminal Procedure, 1973," accessed May 6, 2018, https://indiankanoon.org/doc/930621/.

[65] "Unshackling Expression: A Study on Laws Criminalizing Expression Online in Asia – The Internet Democracy Project."

[66] "Unshackling Expression: A Study on Laws Criminalizing Expression Online in Asia – The Internet Democracy Project."

sided with the states, stating that shutdown's under 144 was legal.[67] The precedent set by the court's findings is evident in the dramatic rise in internet shutdowns from 2016 to 2017. Eventually, the shutdown increase drew the attention of human rights defenders in 2017. In a statement from the UN Special Rapporteurs Michel Forst and David Kaye, "India must immediately end its ban on social media networks and mobile Internet services in the State of Jammu and Kashmir and guarantee freedom of expression for citizens."[68]

The critical takeaway gleaned from these two laws is that new laws are often set aside for old laws that fit the context of the environment and grant a more wide-ranging power to authorities. While initially developed in 1973, Section 144 did not take into account the rise of the internet. Section 69A was purposefully designed for with the internet in mind as can be depicted from the phrasing. All this said, the vagueness of Section 144 implicitly applies to the internet, as the Indian courts have demonstrated.

D. COMPARING SHUTDOWN STRATEGIES

The Arab Spring sparked substantial research on role technology played both in regimes use of repression on dissent and how protesters used networks for communication and control. Significant attention was drawn to Egypt when on January 27, 2011, the government of Egypt employed a strategy that involved a mass network blackout shutting down everything but state-run radio and television across the country.[69] While academic research seems to indicate the shutdown did inhibit communication of the protest, it did not ultimately stop the demonstrations, and further drew apolitical people into the streets.[70]

---

[67] www.ETtech.com, "Supreme Court Upholds Internet Ban by States—ETtech," ETtech.com, accessed May 25, 2018, http://tech.economictimes.indiatimes.com/news/internet/supreme-court-upholds-internet-ban-by-states/50955292.

[68] David Kaye and Michel Forst, "OHCHR | India Must Restore Internet and Social Media Networks in Jammu and Kashmir, Say UN Rights Experts" (United Nations Human Rights Office of the High Commissioner, May 2017), http://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=21604&LangID=E.

[69] Alexandra Dunn, "Unplugging a Nation: State Media Strategy During Egypt's January 25 Uprising," *The Fletcher Forum of World Affairs*, 2011, 10.

[70] Dunn, "Unplugging a Nation: State Media Strategy During Egypt's January 25 Uprising," 10.

Anita Gohdes provided an analysis of how the Syrian government employed network shutdowns during a time of war to enable tactical successes on the battlefield. Her findings suggested that battles that follow internet shutdowns were often found to have an increase in violence related fatalities.[71] Gohdes makes the argument that these large-scale outages are often employed to specifically target the communication nodes of rebels, to weaken them before a conventional military assault. Furthermore, Gohdes makes the critical distinction that internet shutdowns in Syria are used to obscure atrocities caused by the regime.

Research seems to indicate that shutdowns are mainly used to target communication and coordination nodes, but what role do ICTs play with regard to an increase or decrease in violence?[72] Camber Warren explains that vertical ICTs (such as radio and television) have a pacifying effect on populations, while horizontal ICTS (cell phones and social media networks) seems to produce an increase in violence.[73] While Warren's analysis focuses primarily on rural African countries, the premise is valid. The question remains, does the same hold true when horizontal ICTs are shut down by the state, leaving only vertical structures in place? Initial research seems to indicate that shutdowns have a strong relationship with increased levels of violence in civil unrest, despite horizontal ICTs remaining intact, these results are amplified by quantitative research in Chapter III.[74]

Setting aside the relationship between violence and technology, India's use of digital repression seems to be centered around a tactic of *strategic shutdowns* as a means to contain violence during civil unrest. In the context of this paper, a strategic shutdown event is defined as targeted regional service(s) disruption, for example, shutting down WhatsApp and Instagram in the Kashmir Valley following the killing of a militant by government forces. While shutdowns can consist of multiple service disruptions, data collected indicates they are often confined to a specific state within India and rarely cross

[71] Gohdes, "Pulling the Plug."

[72] Tufekci, *Twitter and Tear Gas*, 227.

[73] Warren, "Explosive Connections?"

[74] Raleigh Clionadh et al., "Introducing ACLED—Armed Conflict Location and Event Data," *Journal of Peace Research* 46, no. 5 (2010): 1–10; "Internet Shutdowns in India."

state boundaries, unless the incident of civil unrest crosses state boundaries as well.[75] The rarity of shutdowns crossing state boundaries is likely a result of legal restrictions discussed in Section 144 requiring a police commissioner within a state to authorize a two-month shutdown, coordination across states would require two approvals, according to the law.[76]

A further breakdown and analysis of strategic shutdowns show that mobile networks are the primary target (see Table 1). This is likely a result of the high mobile penetration, and the ease of use cell phones provide protesters.[77] Furthermore, hardwired connections are more likely to impact commercial businesses, creating a more significant financial impact from the shutdown.[78] Of note, there are instances of shutdowns consisting of both internet and mobile, but it does not diminish the fact that mobile infrastructure is the primary target more often than not. Shutdown research is limited with regard to how strategic shutdowns versus network blackouts affect commercial sectors, as there is a growing trend of shutdowns explicitly targeting the primary source of communication for the civil unrest as opposed to full network blackouts.

Table 1. Shutdown Type (India)

Year	Internet	Mobile
2016	10	24
2017	36	51
2018	29	26

Why is there a growing use of strategic shutdowns versus network blackouts? While the government of India typically indicates whether the nature of the shutdown was *reactive* or *proactive* (see Table 2), a correlation could be drawn to the ill-fated effects of complete network blackouts during the Arab Spring, or the financial loss associated to complete blackouts previously discussed.[79] Again, this is likely contributed to by the

[75] "Internet Shutdowns in India."

[76] "Section 144 in The Code of Criminal Procedure, 1973."

[77] Tufekci, *Twitter and Tear Gas, 47*; "India Country Report | Freedom on the Net 2017."

[78] West, Darrell M. *Internet Shutdowns Cost Countries $2.4 Billion Last Year.*

[79] Tufekci, *Twitter and Tear Gas*, 26.

learning process of autocracies in fighting internal unrest.[80] A study released by the United Nations Educational, Scientific and Cultural Organization (UNESCO) in May 2018 listed the five most common justifications for governments in South Asia for shutting down the internet during 2017 (with India consisting of 84% of the South Asian shutdowns) as 1. Reactive, following a killing; 2. Security-related reasons; 3. Resulting from protests; 4. During violent events; and 5. Communal Clashes.[81]

Table 2. Shutdown Nature (India)

Year	Reactive	Preventive
2016	19	12
2017	17	54
2018	39	11

Analysis indicates that strategic shutdowns typically average three days in length, but in some instances, shutdown events have lasted more than 40 days.[82] The relatively short duration of shutdowns gives further credence to the concept that strategic shutdowns are intended to do minimal disruption to society while only targeting the heart of the civil unrest, emphasizing the *strategic* aspect of the shutdown.

E. UNDERLYING CIVIL UNREST

The violent civil unrest in India focuses primarily in the northern part of India. The highest level of violence is along the border with Pakistan and in the disputed territory of Kashmir (see Figure 2).[83] The map colors are indicative of a heat map, with the higher concentration of violence being shades of dark red and limited or no violence being empty cells.

[80] Heydemann and Leenders, "Authoritarian Learning and Authoritarian Resilience."

[81] Murthy, Laxmi, *Clampdowns and Courage: South Asia Press Freedom Report.*

[82] Murthy, Laxmi, *Clampdowns and Courage: South Asia Press Freedom Report*; "Internet Shutdowns in India."

[83] Clionadh et al., "Introducing ACLED—Armed Conflict Location and Event Data."

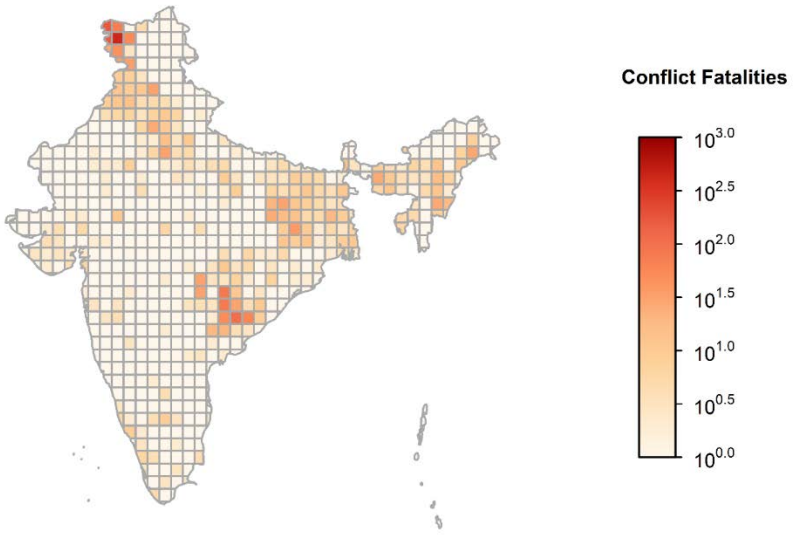

Figure 2. India's Violence, 2016–2018[84]

The origins of the conflict in Kashmir are traced back to the Pakistan and India split in 1947 and the subsequent allocation of Kashmir Valley from the British to the newly established nation-state of India.[85] In India, Kashmir is most violent region, as this is where the most riots, and protests occur and where government forces are often engaging militant organizations. Additionally, Kashmir consists of the most non-violent and violent civil unrest related events. Civil unrest events are defined as collective action ranging from student demonstrations to counterterrorism operations (see Figure 3).

[84] Data adapted from Clionadh et al.

[85] Victoria Schofield, *Kashmir in Conflict: India, Pakistan and the Unending War* (I. B.Tauris, 2000).

xi

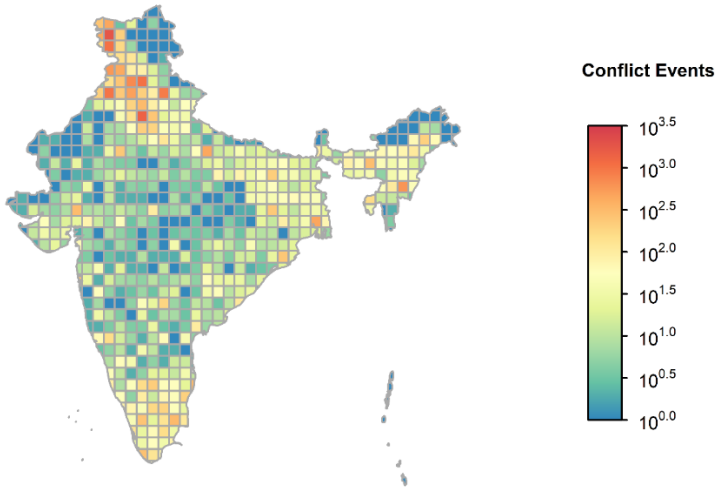

Figure 3. India's Civil Unrest Events, 2016–2018[86]

Demonstrating the concentration of violence in India is essential to understanding how strategic shutdowns are employed, as Kashmir consists of a significant number of both shutdowns and fatalities.[87] While shutdowns in India are a tactic in combating militants, research shows that typically the purpose is not weakening communication and coordination nodes of militant organizations, but rather preventing rumor control, or the further spread of violence.[88] This analysis of India's shutdowns contrasts with Gohde's conclusion as to why shutdowns occur in Syria (shutdowns used to hide atrocities and weaken communication networks).[89] While Syria is in a state of civil war, it is still essential to understand the distinction between shutdowns as means to gain a tactical advantage (Syria), as opposed to an attempt to contain violence (India).

[86] Data adapted from Clionadh et al., "Introducing ACLED—Armed Conflict Location and Event Data."

[87] Clionadh et al.; "Internet Shutdowns in India."

[88] "Internet Shutdowns in India."

[89] Gohdes, "Pulling the Plug."

F. INDIA'S ICT ENHANCED COLLECTIVE ACTION

Academic research concerning the employment of ICTs in India during networked collective action remains sparse. That said, regional news within India provides insight into some of the strategies used by protesters. A commonly employed tactic to bypass government localized strategic shutdowns is the use of encrypted routers. The use of bypass technology is evident in India, demonstrated by the number of Tor users.[90] Tor describes their service as, "free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security."[91] Tufekci in her analysis of social movements and technology indicates that Tor is a commonly used tactic to fight government censorship and strategic shutdowns, as it allows anonymity and can circumvent application shutdowns.[92] Tor users in India have been steadily increasing since 2017 (see Figure 4). The rise in Tor users indicates that the population and by extension, protesters, are attempting to fight back against strategic shutdowns by circumventing filters and blocks on popular communication applications such as Telegram, Twitter, and WhatsApp. It is important to note that total network blackouts do render Tor ineffective, as Tor still requires an initial connection to use the program.

[90] The Tor Project, "Tor Project | Privacy Online," accessed May 25, 2018, https://www.torproject.org/.

[91] The Tor Project, "Tor Project | Privacy Online."

[92] Tufekci, *Twitter and Tear Gas*, 230.

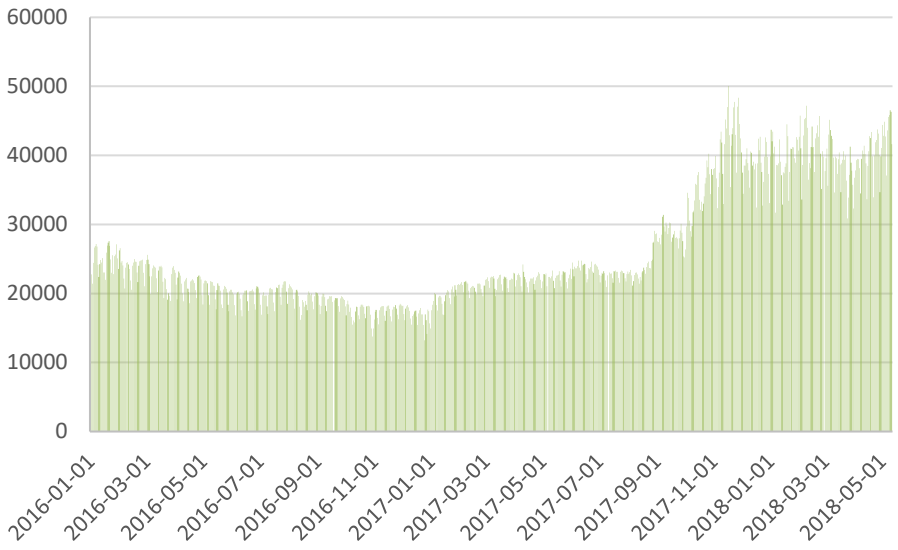

Figure 4. India's Tor Users.[93]

The limited amount of academic work concerning how protesters within India fight back against shutdowns is an indication that the balance of power with regard to the internet remains firmly in the hands of the central government, but the lingering question of how effective shutdowns are in combating violence continues to remain unanswered.

G. LOOKING AHEAD

Initial analysis indicates that India is falling into a pattern of repression used by autocracies, and while a substantial amount of research is done surrounding the financial aspects of shutdowns or the increasing number of shutdowns, very little attention is given to studying the effects they have on collective action. The remaining quantitative question is: Do strategic shutdowns reduce violence?

[93] Data adapted from The Tor Project, "Tor Project | Privacy Online."

III. QUANTIFYING DIGITAL SHUTDOWNS AND CONFLICT VIOLENCE

A. INDIA'S RISE TO REIGN IN DIGITAL SHUTDOWNS

Authoritarian regimes are globally demonstrating that they are recovering and reacting to the initial shock that social media caused during the much-publicized Arab Spring movements.[94] There is a mounting trend of social media co-option as opposed to digital repression, leveraging networks to produce increased regime resiliency instead of dissent.[95] While research continues to focus almost exclusively on the evolution of autocratic strategies to combat digital dissent, the democratic state of India rapidly emerged as the new flag bearer of digital repression, dominating over 47% of the total recorded global shutdowns from 2016 to 2017.[96] Research seems to show that India is using digital shutdowns as a strategy of stopping the onset of protest-related violence.[97] If shutdowns are intended to prevent violence, the question becomes, are the days following a shutdown event more violent than they would have been in the absence of the shutdown?

B. SHUTDOWN AND VIOLENCE DATASETS

The primary purpose of this research is to study the relationship between digital shutdowns and violence. The data to quantify *violence* in the context of all civil conflict events (both violent and non-violent), comes from the Armed Conflict and Event Dataset (ACLED).[98] While ACLED's dataset on India is relatively new, and only dates to 2016, this does not affect the results, as India only saw 14 total shutdowns from 2012 to 2014,

---

[94] Seva Gunitsky, "Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability," *Perspectives on Politics* 13, no. 1 (March 2015): 42–54, https://doi.org/10.1017/S1537592714003120; Heydemann and Leenders, "Authoritarian Learning and Authoritarian Resilience."

[95] Gunitsky, "Corrupting the Cyber-Commons."

[96] "#KeepItOn," *Access Now* (blog), accessed May 4, 2018, https://www.accessnow.org/keepiton/.

[97] "Internet Shutdowns in India," accessed May 6, 2018, https://internetshutdowns.in.

[98] Raleigh Clionadh et al., "Introducing ACLED—Armed Conflict Location and Event Data," *Journal of Peace Research* 46, no. 5 (2010): 1–10.

whereas in 2017 alone, India saw 70 shutdowns.[99] While little academic research exists explaining the reason behind India's quick rise in digital repression, the analysis indicates the swift growth of internet services and the significant expansion of social media likely made digital platforms a target during the internal civil unrest. ACLED is commonly chosen for its data precision, as it breaks down the unit of analysis to a geolocated day-event, which is critical in determining how shutdowns affect violence in the days following an event in India. Additionally, ACLED codes data based on actors and interactions allowing for detailed analysis of specific events and finally, ACLED is transparent with how it collects and authenticates data, allowing data verification for accuracy.[100]

The second source of data comes from a combined India shutdown event dataset coded specially for this research. The primary source of reporting on shutdown events comes from the Software Freedom Law Centre (SFLC), a non-profit digital rights organization that operates out of India.[101] The SFLC maintains a geolocated tracker that links to news reports of shutdowns for verification. The coded shutdown tracker also consists of scraped news stories of shutdowns not yet captured by SFLC but additionally linked to source documentation in the shutdown dataset for verification. Finally, the shutdown dataset was cross-referenced against the Accessnow's dataset and International Federation of Journalists (IFJ)'s report on South Asia internet shutdowns to ensure accuracy in the coding of the final shutdown dataset.[102] ACLED consist of approximately 30,000 events for analysis, and the internet shutdown dataset consists of 150 shutdown events, averaging three days in duration.

It is important to note that the leading research on internet shutdowns by Ghodes in *Pulling the plug: Network disruptions and violence in civil conflict* and Hassanpour in *Leading from the Periphery and Network Collective Action* primarily uses Google

[99] "#KeepItOn."

[100] Clionadh et al., "Introducing ACLED—Armed Conflict Location and Event Data."

[101] "Internet Shutdowns in India."

[102] "#KeepItOn"; Laxmi Murthy, "Clampdowns and Courage: South Asia Press Freedom Report."

transparency reports to identify network shutdowns.[103] While Google transparency reports provide an accurate representation of extensive network shutdowns by governments, it is limited in the scope of only being able to effectively monitor Google specific products, such as YouTube, Gmail or more broadly, the Google search engine itself.[104] For identifying *strategic shutdowns,* the focus of this research, that target specific regional communication applications such as WhatsApp, Telegram or Facebook, a focused temporal and geospatial dataset is required, which led to the coding of the Indian shutdown event dataset.

C. DEPENDENT VARIABLE—VIOLENCE

The dependent variable of violence is derived from ACLED. When an event results in fatalities of one or greater (and the fatalities are violent in nature, caused by protesters, security forces, or others individuals involved in the collective action) that event is considered a violent event for this research. The fatality and event are both geolocated with descriptive details of actors and interaction to ensure proper attribution. Since the dependent variable consists of a count of fatalities across Indian states, this indicates that *Poisson regression* is necessary to determine the relationship between the dependent and independent variable. Poisson regression is typically used when the dependent variable consiststs of positive integers, for example, a numerical count of rare events, occurrences or incidents over time. In the 30,000 coded events analyzed for this research, there are 2,763 fatalities from 2016 to 2018.[105] The primary location of violence within India is in the Kashmir region (see Figure 5) but India still experiences considerable violence throughout the rest of the country, this is critical to understand when analyzing violence across India with relationship to the independent variables.[106]

---

[103] Gohdes, "Pulling the Plug"; Navid Hassanpour, *Leading from the Periphery and Network Collective Action* (Cambridge, United Kingdom ; New York, NY: Cambridge University Press, 2017); "Google Transparency Report," accessed June 7, 2018, https://transparencyreport.google.com/.

[104] "Google Transparency Report."

[105] Clionadh et al., "Introducing ACLED—Armed Conflict Location and Event Data."

[106] Clionadh et al., "Introducing ACLED—Armed Conflict Location and Event Data."

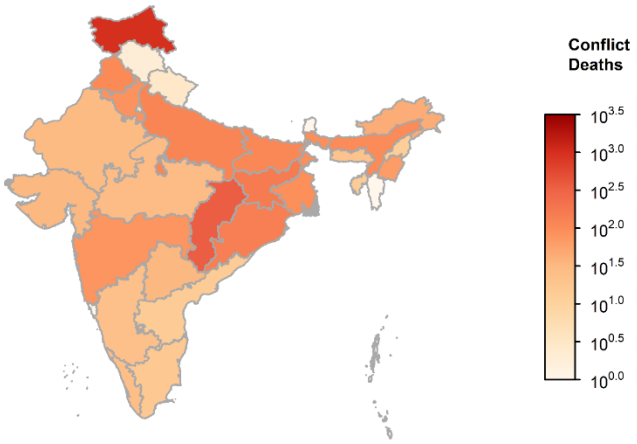

Figure 5. India, Conflict Deaths at the State Level[107]

D. PRIMARY INDEPENDENT VARIABLE—DIGITAL SHUTDOWN EVENTS

Shutdown events consist of mobile and (or) internet shutdowns. Shutdown events are either preventative or reactive, depending on whether they are used in anticipation of civil unrest or as a result of civil unrest. A *strategic shutdown* is defined in this thesis as a targeted regional disruption with the intent of limiting rumor control, containing protests and subsequent violence or in military operations as a form of operational security.

Mobile shutdowns are defined as events in which mobile services or programs are limited, such as mobile-specific Short Messaging Service (SMS) or WhatsApp. Internet shutdowns are defined as hardwired connections being limited, with traditional targets being websites, blogs, network slowdowns (bandwidth limitations) or complete network blackouts. It is important to note that the delineation between mobile and internet shutdowns can overlap, but traditionally the specific service (internet service providers and mobile service providers) disrupted determines the shutdown type. Finally, it is important to note that research is limited in the scope of the regional and national news reporting of what services are disrupted. News articles will often state *internet disruption*, *SMS disruption*, *mobile disruptions*, or discuss what specific applications were blocked. These

[107] Data adapted from Clionadh et al., "Introducing ACLED—Armed Conflict Location and Event Data."

terms are taken at face value from the news story as the targeted service that was disrupted, while often cross-referenced with other news sources to ensure accuracy, this is not always possible, falling back on the initial source alone. The shutdown variables are numerically annotated in individual columns as dichotomous 1 or 0 in the shutdown dataset to record if the occurrence of the shutdown was mobile services, internet services or a combination of services. The Indian shutdown event dataset consists of 152 geolocated coded events, and when expanded to include days in duration becomes 491 geolocated shutdown-days to model against geolocated violence. When analyzing shutdown events in context with state violence, it is essential to understand the location of shutdown events. As identified for violent events, shutdown events are typically concentrated in the Kashmir region (see Figure 6). Figure 6 was developed using data from the Indian shutdown event dataset.

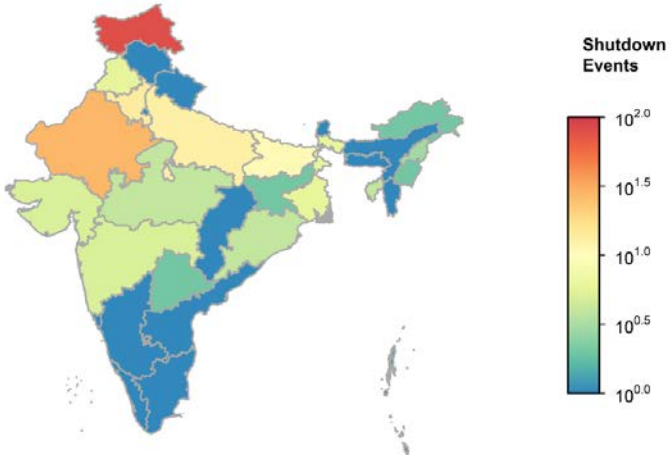

Figure 6. India, Shutdown Events at the State Level

E. CONTROL VARIABLES—MILITARY OPERATIONS, PROTESTS AND RIOTS

When controlling for events that cause violence on any given day in India, it is important to take into consideration, military operations, protests, and riots. ACLED provides a detailed account of these variables. Military operations are defined as any event with ACLED interaction codes 10 through 18.[108] Military operations range from sole

[108] Clionadh et al., "Introducing ACLED—Armed Conflict Location and Event Data."

military operations, military versus militants to military versus protesters.[109] Controlling for military violence is essential as research indicates that military action typically results in violence, especially in the contested region of Kashmir. Protests and riots are defined as events that range from demonstrations to organized movements against government institutions.

Furthermore, riots and protests can be one-sided or aimed at a specific actor.[110] It is important to note that these variables are coded as either 1 or 0, meaning that they occurred or did not occur. Additionally, days of consecutive peace are also essential to analysis with regard to violence, as this will demonstrate if peaceful days remain peaceful following a shutdown or turn violent, this variable provides a continuous count of geolocated peaceful days that resets the counter once a violent event occurs.

F. LAGGED VARIABLES

A critical component in understanding the relationship between violence and digital repression is understanding what happens the day after the digital shutdown event. To properly analyze this component, *lagged independent variables* are developed and used. For this research, lag is broken down into three categories, *lag1, lag2, and lag7,* with the number corresponding to the number of days that have passed since the event (one, two- or seven-days post incident). Research demonstrates that digital shutdowns in India on average last three days, which is why lag1 and lag2 are necessary. While looking seven days after a shutdown event provides minimal insight since both protests and shutdowns on average do not last that long, some information can still be gleaned about where conditions are at one week after the initial event. Ultimately lagged variables allow the models to capture the relationship between violence and digital repression over time.

[109] Clionadh et al., "Introducing ACLED—Armed Conflict Location and Event Data."

[110] Clionadh et al., "Introducing ACLED—Armed Conflict Location and Event Data."

G. HYPOTHESES

Since research indicates that Indian authorities are using shutdowns to contain or prevent violence, this leads to the first question, how useful is this strategy? Should ICTs be blocked to prevent or stop the spread of violence occurring within a state?

Null Hypothesis: When all else is held constant, the days following strategic shutdowns will see unchanged levels of violence.

If the null hypothesis is supported, this could indicate that the use of strategic shutdowns is not a valid tactic to be used against violence during civil unrest in India, as they have no impact on the overall violence levels. On the other hand, while existing research has demonstrated that digital shutdowns have a minimal impact on mobilization, less is known about how shutdowns affect the collective narrative during civil unrest, and it could be that the state can regain or control the narrative through digital repression. This may imply that as long as there is not an increase in violence that digital shutdowns still offer an incentive in the form of narrative suppression and control. However, this argument will not hold if shutdowns produce increased violence, especially if the ultimate goal is to reduce or stop the violence.

Alternative Hypothesis: When all else is held constant, the days following strategic shutdowns will see an increase in violence.

If the alternative hypothesis is supported with a positive relationship, this would indicate that the use of strategic shutdowns is not an effective tool to combat civil unrest related violence, as the violence following a shutdown tends to be increasing. While on the other hand, if we instead find evidence of a negative relationship this would indicate that the use of strategic shutdowns is a valid tactic to be used against violence under the civil rest context in India, as this would indicate that shutdowns generally decrease violence in the affected areas.

H. MAIN RESULTS

Empirical evidence derived from the shutdown dataset demonstrates a significant relationship between digital repression and violence. Table 3 shows the results from the

main models. Model 1 is the baseline model, with only shutdowns and lagged shutdowns included as independent variables, not taking into account any control variables. Model 2 adds three controls, days in duration (annotated as *days*), days of consecutive peace (annotated as *peace_days*), and military violence (annotated as *military_violence*), as these are essential factors to consider when analyzing violence. The final model, Model 3 adds in the last control variable, *protest*, and holistically looks at the relationship between shutdowns and violence. Adding protest into the model last is critical, as this is often the context in which shutdowns occur, controlling for this is the final step in ensuring that there truly is a significant relationship between digital shutdowns and violence.

Furthermore, Model 3 holds the lowest Akaike Information Criterion (AIC). AIC is a statistical indicator that demonstrates the relative quality of regression models, with the lowest score indicating the highest quality model. Each model in Table 1 subsequently improves the AIC demonstrating that the controls are accounted for and improve the overall quality of the model when analyzing shutdowns and violence.

The control variables of military violence, protest and days of consecutive peace produce results that are expected. Military violence has a clear relationship with the overall level of violence demonstrated by the statistically significant positive coefficient. The results of military violence demonstrate the importance of controlling for this variable when considering violence on a given day. While on the flip side, days of consecutive peace have a negative coefficient (as expected), indicating that days of consecutive peace are likely to remain peaceful when all else is held constant. Additionally, days with protests demonstrate a statistically significant positive relationship with violence, reinforcing the necessity of controlling for this variable in the final model.

When focusing on the core of the question, the relationship between digital repression and violence, the coefficient (specifically shutdown_lag1) is statistically significant ($p<0.01$) and positive, as seen in all three models. Since the coefficient is statistically significant, the null hypothesis is rejected, and the conclusion is that there is enough evidence to support the alternative hypothesis that there is a positive relationship producing an increase in violence the day after a shutdown event when all other variables are held constant. On average, one day following an internet shutdown will see an increase

in violence (demonstrated in Figure 7 as two-fold the level of the previous day) when all else is held constant, as opposed to a day without a shutdown event. It is also interesting to note that the positive coefficients on the levels of violence after two days (*lag2)* and one week (*lag7)* following the shutdown still show as statistically significant, indicating that violence remains high after a shutdown for up to a week. Since the lagged analysis still shows increased violance, it further reinforces the negative consequences of using digital repression to contain violence, if the effects of increased violence resulting from the digital repression linger for a week after the initial event. While on the micro level it is challenging to see the impact digital repression has on violence when analyzed at the macro level the results are clear—that indeed, digital repression increases violence.

Table 3. Poisson Regression—Shutdowns and Violence.[111]

	Dependent variable:		
	deaths		
	(1)	(2)	(3)
shutdown	2.233***	1.718***	1.301***
	(0.083)	(0.088)	(0.087)
shutdown_lag1	1.634***	1.176***	0.912***
	(0.099)	(0.097)	(0.096)
shutdown_lag2	1.079***	0.557***	0.503***
	(0.118)	(0.118)	(0.117)
shutdown_lag7	1.096***	0.718***	0.857***
	(0.116)	(0.112)	(0.110)
days		0.011	0.025**
		(0.010)	(0.010)
peace_days		-0.029***	-0.025***
		(0.001)	(0.001)
military_violence			2.057***
			(0.043)
protest			0.076***
			(0.003)
Constant	-2.497***	-1.508***	-1.997***
	(0.020)	(0.026)	(0.030)
Observations	29,750	29,750	29,750
Log Likelihood	-11,146.810	-9,789.663	-8,811.309
Akaike Inf. Crit.	22,303.630	19,593.330	17,640.620
Note:			*p<0.1; **p<0.05; ***p<0.01

Figure 7 visually depicts the substantive significance between digital shutdowns and violence. The positive coefficient indicates an increase in violence one day following the digital shutdown. The 95% confidence bands demonstrate that the level of violence one day after a shutdown usually ranges from doubled to tripled what the level of violence would be without a digital shutdown. This would mean that a protest in India with a digital shutdown would be expected to see two times as much violence as a protest without a digital shutdown.

[111] Clionadh et al.; Marek Hlavac, *Stargazer: Well-Formatted Regression and Summary Statistics Tables*, version 5.2.1, 2018, https://CRAN.R-project.org/package=stargazer.

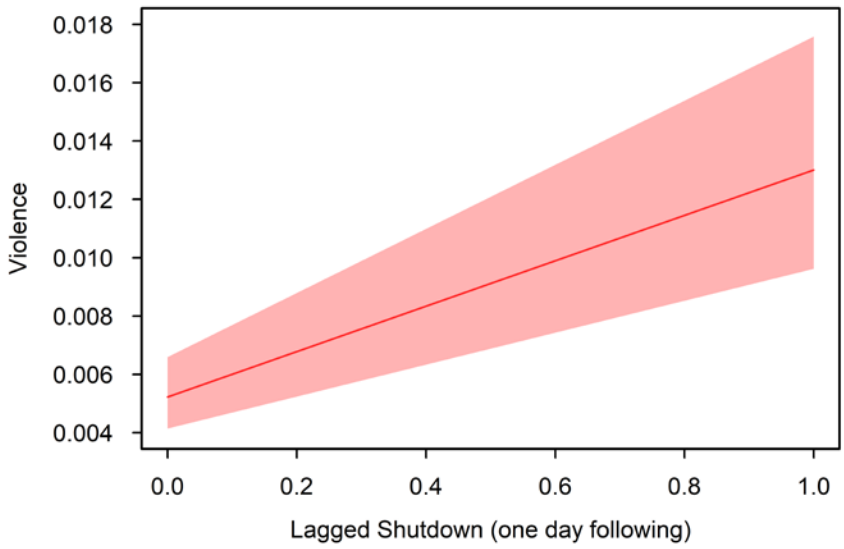

Figure 7. Poisson Regression—Shutdowns and Violence.[112]

To test the robustness of the results from the original model, *Table 4* includes longer lags of the control variables, while leaving the dependent variable of violence constant. Lags of shutdowns *model (1),* protests *model (2*) and military violence *model (3*), are individually regressed against violence before finally being combined into one model, *model (4),* that employs a Poisson regression of the fourteen variables against violence, and still produces significant results with relation to shutdowns and violence, further reinforcing the original findings. Again, *lag1* indicates one day following, *lag2* indicates two days and *lag7* indicates seven days after the initial event. Furthermore, Table 2 looks at the lagged relationship between violence, military violence, and protests, with the results producing expected outcomes; an increase in the overall level of violence for up to a week following protests and military violence compared to those days without protests or military violence. While these results are expected, they continue to reinforce the need to control for them in Model 3, which ultimately has the lowest AIC score and still produces significant results.

[112] Adapted from Clionadh et al., "Introducing ACLED—Armed Conflict Location and Event Data."

Table 4. Shutdowns, Protests and Military Violence. [113]

	Dependent variable:			
	deaths			
	(1)	(2)	(3)	(4)
shutdown	1.718***			1.179***
	(0.088)			(0.088)
shutdown_lag1	1.176***			0.839***
	(0.097)			(0.096)
shutdown_lag2	0.557***			0.349***
	(0.118)			(0.117)
shutdown_lag7	0.718***			0.573***
	(0.112)			(0.113)
days	0.011			0.026**
	(0.010)			(0.010)
peace_days	-0.029***			-0.023***
	(0.001)			(0.001)
protest		0.061***		0.062***
		(0.003)		(0.003)
protest_lag		0.045***		0.027***
		(0.004)		(0.004)
protest_lag2		0.026***		0.023***
		(0.003)		(0.004)
protest_lag7		0.063***		0.047***
		(0.003)		(0.004)
military_violence			2.272***	2.077***
			(0.043)	(0.044)
military_violence_lag			0.301***	0.056
			(0.075)	(0.075)
military_violence_lag2			0.687***	0.461***
			(0.066)	(0.066)
military_violence_lag7			0.636***	0.376***
			(0.068)	(0.069)
Constant	-1.508***	-2.680***	-2.774***	-2.252***
	(0.026)	(0.022)	(0.024)	(0.034)
Observations	29,750	29,750	29,750	29,750
Log Likelihood	-9,789.663	-10,990.510	-10,519.300	-8,660.329
Akaike Inf. Crit.	19,593.330	21,991.030	21,048.600	17,350.660
Note:				*p<0.1; **p<0.05; ***p<0.01

[113] Adapted from Clionadh et al.; Hlavac, *Stargazer*.

Also interesting is the interaction between days of consecutive peace and digital shutdown. Analysis of the results indicates that shutdowns turn peaceful days into violent days one day after a shutdown event (lagged results). First, looking at Table 3 and analyzing the interaction between *pcdays:shutdown*, the results indicate as expected, that when a shutdown occurs followng a long period of peace, it is more likely to be peaceful than when it occurs in a context of recent violence. When *pcdays:shutdown_lag1* is analyzed, meaning one day following a shutdown on a peaceful day, we see a positive relationship with the coefficient. The lagged analysis indicates that when shutdowns are used on peaceful protests that the day following will have a higher level of violence as seen in Table 5.

Figure 8 visually reinforces the concept that the interaction between lagged shutdowns (one day after) and days of consecutive peace (*peace_days*) produce a substantial increase in violence. The 95% confidence bands demonstrate that on the low end of the spectrum the level of violence is still significantly higher than those days without shutdowns, while the darker shades indicate how long the days of consecutive peace was when the shutdown occurred. These results indicate that using shutdowns on peaceful protest produce increased violence on the following day, further emphasizing the inability of digital repression to prevent violence.

Table 5. Peaceful days, Shutdowns and Violence.[114]

	Dependent variable:
	deaths
protest	0.069***
	(0.003)
protest_lag	0.042***
	(0.004)
peace_days	-0.025***
	(0.001)
shutdown	1.416***
	(0.087)
shutdown_lag1	0.554***
	(0.112)
shutdown_lag2	0.526***
	(0.123)
shutdown_lag7	0.827***
	(0.122)
military_violence	2.063***
	(0.043)
peace_days:shutdown	-0.034***
	(0.007)
peace_days:shutdown_lag1	0.038***
	(0.003)
peace_days:shutdown_lag2	-0.048***
	(0.017)
peace_days:shutdown_lag7	-0.025*
	(0.015)
Constant	-2.056***
	(0.031)
Observations	29,750
Log Likelihood	-8,715.271
Akaike Inf. Crit.	17,456.540
Note:	*p<0.1; **p<0.05; ***p<0.01

[114] Adapted from Clionadh et al., "Introducing ACLED—Armed Conflict Location and Event Data"; Hlavac, *Stargazer*.

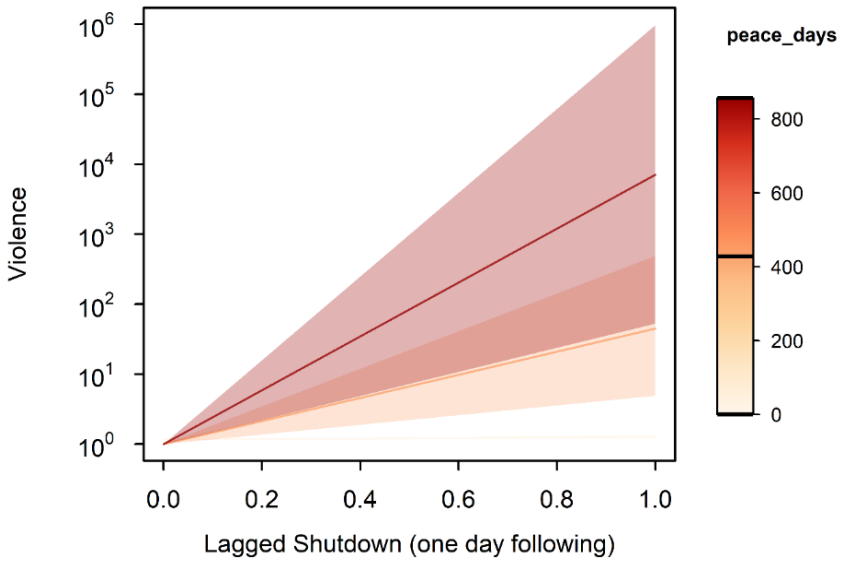

Figure 8. Interaction of Peaceful Days and Shutdowns with Violence.[115]

I. CONCLUSION AND ASSESSMENT

As the global internet model continues to shift toward a concept of internet sovereignty, the reality is that strategic shutdowns will continue to be a tactic to fight civil unrest in both democracies and autocracies around the world.[116] Furthermore, shutdowns will continue to be used to hide atrocities committed by authoritarian regimes, as Ghodes demonstrated in Syria.[117] With this said, large-scale digital disruptions to fight civil unrest are globally becoming less frequent, and likely only a last resort due to the financial aspect, and we should expect that the increasing trend of social media co-option will continue as will the strategic shutdowns examined in this research.[118] Despite these trends, India still employs digital shutdowns to fight violence. Research demonstrates this tool to fight violence is fruitless, and in actuality, creates the opposite effect. While digital shutdowns

[115] Adapted from Clionadh et al., "Introducing ACLED—Armed Conflict Location and Event Data."

[116] "#KeepItOn"; "Freedom House," accessed February 7, 2018, https://freedomhouse.org/.

[117] Gohdes, "Pulling the Plug."

[118] West, Darrell M. *Internet Shutdowns Cost Countries $2.4 Billion Last Year*; Gunitsky, "Corrupting the Cyber-Commons."

are likely viewed as an easy and non-violent approach by the state to combat violence stemming from civil unrest, in reality, the inverse is true, and there is a quantitative increase in violence associated with shutdowns.

Ultimately, this research will beg the question as to why violence occurs during digital shutdowns. Possible answers include but are not limited to, the fragmentation of a semi-organized protest, frustration over the inability to express public opinions, and the loss of an outlet to deal with anger, or that the state feels empowered to extract harsher measures when the ability to digitally document the crackdown is limited. An in-depth look into a protest involving digital repression and violence is necessary to better understand both why violence occurs during digital repression and the granularity of how digital repression manifests on the micro level.

IV. CIVIL UNREST AND DIGITAL REPRESSION: AN INTIMATE LOOK

A. CASE STUDY SELECTION CRITERIA

India has a long history of civil unrest that predates the partition of India and Pakistan and the establishment of the state. Furthermore, India is a country where a wide variety of cultures, religions, and castes merge, ultimately leading to division. Selecting a case to analyze digital repression at the ground level is essential to providing a clear picture of how internet shutdowns and violence intersect.

Given that internet shutdowns did not reach prominence until 2016, the case study window included all documented civil unrest events from 2016 to 2018. Within this temporal window, potential cases must have documented violence and use of digital repression. The final requirement is that the case needs multiple reporting sources, as it is important to note that there is little academic research on individual protests within India and that sources primarily include local, regional and national news outlets. The April 2018 Bharat Band protests met the criteria. Furthermore, the size of the protest drew international media attention, allowing for multiple sources to ensure documentation accuracy.

B. APRIL 2018, #BHARATBANDH PROTESTS

On the morning of April 2, 2018, social media in India started to circulate #BharatBandh along with pictures of protesters in India stopping trains in Punjab, rallying against the weakening of the Scheduled Castes/Scheduled Tribes Prevention of Atrocities Act (SC/ST) protection act.[119] Throughout three days, India would see digital shutdowns, massive protests and violence culminating with ten dead and hundreds arrested.[120] While

[119] "Bharat Bandh: Protests by Dalit Groups over SC/ST Act on April 2, 2018—As It Happened," Zee News, April 2, 2018, http://zeenews.india.com/india/live-updates/bharat-bandh-live-news-updates-strike-across-india-2095564; Sandya Fuchs, "Indian Supreme Court Curbs One of the World's Most Powerful Anti-Discrimination Laws," *Opendemocracy.Net*, May 26, 2018, https://www.printfriendly.com/p/g/7Kxgrw.

[120] Fuchs, "Indian Supreme Court Curbs One of the World's Most Powerful Anti-Discrimination Laws."

this sounds dramatic, protests are commonplace in India, a country where divides between social castes, religions and cultures clash in a nation that is quickly closing the gap with China to have the world's largest population by 2025.[121] The collision of digital repression, digital liberation, and violence during civil unrest in India will be analyzed using the social movement theory of McAdam et al. for the contextual framework.[122] Social movement theory provides the essential understanding for what contributed to the establishment of the 2018 Bharat Bandh protests and to better understand the subsequent repression employed during the movement. The foundation of social movement theory is collective grievances, political opportunities, mobilizing structures and finally how the movement framed the narrative which provides insight into why the social movement arose and thrived.[123] Of note, the conclusion will analyze how digital shutdowns and levels of violence impacted the social movement.

C. GRIEVANCES

At the core of the Bharat Bandh protests of 2018 lies the SC/ST act.[124] The SC/ST act was established in 1989 and protects India's formerly untouchable (Dalit) communities.[125] Sandhya Fuchs, a scholar specializing the interaction between state law and local forms of law and order, who spent time studying at the Indian Institute of Dalit Studies (IIDS) in India, explains that the controversy surrounding SC/ST act lies in the severe punishments that it can impose.[126] The punishments include immediate arrest with a minimum of six months to five years of imprisonment accompanying violations of the

[121] "United Nations Population Division | Department of Economic and Social Affairs," accessed May 6, 2018, http://www.un.org/en/development/desa/population/.

[122] Doug McAdam, John D. McCarthy, and Mayer N. Zald, eds., *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Cultural Framings*, First Edition (Cambridge England ; New York: Cambridge University Press, 1996).

[123] McAdam, McCarthy, and Zald., *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Cultural Framings*.

[124] "Bharat Bandh," April 2, 2018; "Eight Dead in Massive India Caste Protests," *BBC News*, April 2, 2018, sec. India, https://www.bbc.co.uk/news/world-asia-india-43616242.

[125] Fuchs, "Indian Supreme Court Curbs One of the World's Most Powerful Anti-Discrimination Laws."

[126] Fuchs, "Indian Supreme Court Curbs One of the World's Most Powerful Anti-Discrimination Laws."

SC/ST act.[127] Fuchs continues to explain that since the origins of the law, there has always been a significant push to remove or reduce the severity of the act, and as of 20 March 2018, the act was adjusted to curb suspected misuse. Dalit groups perceived this weakening of the SC/ST as an injustice.[128] While it is important to note that Fuchs' own research in Rajasthan contradicts the widespread misuse of the act suggested by India's Supreme Court, the act remains both highly controversial and complex. Controversy aside, caste violence is still a significant issue in India. Amnesty International reports that in 2016 alone there were 40,000 crimes on lower castes.[129] Ultimately, it was the perceived injustice from the weakening of the SC/ST act that caused the mass protests of 2 April 2018.

D. POLITICAL OPPORTUNITIES

The March 20 Supreme Court ruling on the SC/ST act provided the opportunity for Dalit groups to take to the streets and protest collective anger. Specifically, the Supreme Court of India removed the mandatory arrest portion of the law along with the registration of law violators.[130] On March 21, local news stated that members of the Bharatiya Janata Party (BJP) which are traditionally known to have strong Hindu nationalist priorities, pressed the Union Law Minister to review the newly added amendment.[131] Indian national news indicated that the BJP state governments were using excessive retaliatory violence against a peaceful Dalit protest.[132] Initially, to demonstrate outrage over the SC/ST act

---

[127] Fuchs; "The Scheduled Castes and The Scheduled Tribes (Prevention of Atrocities) Act 1989," Pub. L. No. 33 of 1989, 9 (1989).

[128] Fuchs, "Indian Supreme Court Curbs One of the World's Most Powerful Anti-Discrimination Laws"; "Eight Dead in Massive India Caste Protests."

[129] "India 2017/2018," accessed September 4, 2018, https://www.amnesty.org/en/countries/asia-and-the-pacific/india/report-india/.

[130] "Bharat Bandh: Death Toll in Madhya Pradesh Hits 7, 51 FIRs Lodged—Times of India," The Times of India, accessed August 31, 2018, https://timesofindia.indiatimes.com/city/bhopal/bharat-bandh-death-toll-in-madhya-pradesh-hits-7-51-firs-lodged/articleshow/63595081.cms.

[131] Sumanta Banerjee, "Civilizing the BJP," *Economic and Political Weekly* 40, no. 29 (2005): 3116–19; The Hindu Net Desk, "The Hindu Explains: What Triggered the 'Bharat Bandh'?," *The Hindu*, April 2, 2018, sec. National, https://www.thehindu.com/news/national/the-hindu-explains-what-triggered-the-bharat-bandh/article23416602.ece.

[132] "Congress Accuses BJP Govts of Targeting Dalits after Bharat Bandh," accessed October 6, 2018, https://www.nationalheraldindia.com/india/congress-accuses-bjp-governments-of-targeting-dalits-after-bharat-bandh.

changes, small protests started to occur from March 21 to April 2. Local leaders in the town of Phagwara, Punjab who are part of the Dalit community, called for a Bandh, which would be the actual start of the massive April 2 Bhara Bandh protests.[133] Local news reported that the date of April 2 was established by a WhatsApp group operating out of western Uttar Prades. The message primarily stated that it was time to take the conversation from WhatsApp to the streets and shut down India on April 2.[134]

E. MOBILIZING STRUCTURES

Academic literature agrees that social media has adjusted the landscape of social movements, specifically in the mobilization structures, creating *horizontal movements.*[135] Horizontal (leaderless) movements drew significant attention during the Arab Spring when many of the movements were decentralized and pushed multiple agendas simultaneously.[136] While research often concludes that leaders are critical in social movements, it does not change the fact that they still occur worldwide.[137] It is essential to understand how and why horizontal movements arise, as research indicates that this is primarily what the Bharat Bandh protest embodied.

During the Bharat Bandh in 2018, the protests were reported to be primarily established through social media, with WhatsApp being the primary application used to organize marches.[138] Furthermore, the movement did not have direct leadership, but rather a horizontal movement through the use of social media, which primarily played a role in

---

[133] Shoaib Daniyal, "The WhatsApp Wires: How Dalits Organized the Bharat Bandh without a Central Leadership," Text, Scroll.in, accessed August 31, 2018, https://scroll.in/article/874714/the-whatsapp-wires-how-dalits-organised-the-bharat-bandh-without-a-central-leadership.

[134] Daniyal, "The WhatsApp Wires."

[135] Vincent Durac, "Social Movements, Protest Movements and Cross-Ideological Coalitions—The Arab Uprisings Re-Appraised," *Democratization* 22, no. 2 (February 23, 2015): 239–58, https://doi.org/10.1080/13510347.2015.1010809.

[136] Durac, "Social Movements, Protest Movements and Cross-Ideological Coalitions—The Arab Uprisings Re-Appraised."

[137] Snow, David A. Soule, Sarah A. and Hanspeter Kriesi, *The Blackwell Companion to Social Movements* (Malden, MA: John Wiley & Sons, 2008). 171—172

[138] Daniyal, "The WhatsApp Wires."

mobilizing the location of marches.[139] It is important to note that opposing groups are known to infiltrate Dalit protests and change the narrative to shout pro-Pakistan slogans, as had happened in a previous Dalit protest in February 2016.[140] Users on social media suggest that if this was seen at protests that they should, "Beat them up and shoot the whole thing on video."[141] While social media is often used to call for violence, it theoretically makes sense to shutdown the internet and effectively kill this violent rhetoric, but again, research indicates that shutting down the internet will have an opposite effect.

In answering why social media is often used, Anant Kamath, a scholar studying how Dalit communities have used ICTs to further themselves finds that ultimately that despite having access to the internet, Dalit groups remain low within the countries relative literacy rate, furthermore the technology is primarily being used as a tool for communication.[142] Anant Kamath notes that the use of technology as only a communication tool exasperates the developmental divide among castes in India, and the divide will remain strong until there is greater political participation and increased education among Dalit Groups.[143] Kamath's research indicates that shutdowns inhibit Dalit groups from political participation, only further alienating marginalized groups.

F. FRAMING

Bharat Bandh translates to "shut down India," in Hindi, Bharat meaning *India* and Bandh meaning *closed*, or *shutdown*. The April 2018 bandh is not the first Bharat Bandh in India, as bandhs are a common form of protest, while a powerful tool of civil disobedience it is also highly controversial.[144] Research seems to indicate that bandhs are

---

[139] Daniyal, "The WhatsApp Wires."

[140] Daniyal, "The WhatsApp Wires."

[141] Daniyal, "The WhatsApp Wires."

[142] Anant Kamath, "'Untouchable' Cellphones? Old Caste Exclusions and New Digital Divides in Peri-Urban Bangalore," *Critical Asian Studies* 50, no. 3 (July 3, 2018): 375–94, https://doi.org/10.1080/14672715.2018.1479192.

[143] Kamath, "'Untouchable' Cellphones? Old Caste Exclusions and New Digital Divides in Peri-Urban Bangalore."

[144] Sk Jahangir Ali and Santanu Sen, "Is 'Bandh' Constitution or Unconstitutional in India?" (Balurghat Law College, February 7, 2013).

distinguished from one another primarily by the date they occur. The April 2018 Bharat Bandh epitomizes the ideals of a bandh, by creating a space for a political conversation through civil disobedience and collective action. As for how the bandh forms a narrative, it is primarily through motivational pictures or internet memes that were circulated to embolden people to protest.[145] On the surface, the framing of the narrative is standard for modern horizontal movements and protests, without traditional leadership framing an overarching narrative, but rather individuals with collective outrage.[146]

While individuals would offer up suggestions to the protesting community at large, such as anticipating counter-protests, again, research indicates that very little was done on the surface to shape the narrative.[147] Bandhs tend to follow a similar life-cycle of outrage, anger, concession, and remission, with the narratives primarily circulating the grievances to build the common base of unrest.

G. DIGITAL LIBERATION, REPRESSION AND VIOLENCE DURING #BHARATBANDH

While it is easy to fixate on the role technology played in enabling civil unrest, it is important to remember that civil unrest is not a new phenomenon; that merely by existing, technology does not produce civil unrest but rather changes its dynamics.[148] Furthermore, the timeline of violence is important to understand how the digital shutdown occurred and what immediately followed.

Initial reports and photos from the April 2 protest indicate the collective action focused on blocking streets and rail stations. It is important to note that blocking streets is a common tactic in civil disobedience, with an aim at causing disruption to routine and

[145] Daniyal, "The WhatsApp Wires."

[146] Daniyal, "The WhatsApp Wires."

[147] Daniyal, "The WhatsApp Wires."

[148] Zeynep Tufekci, *Twitter and Tear Gas: The Power and Fragility of Networked Protest* (New Haven ; London: Yale University Press, 2017), 131.

forcing attention to the movement.[149] Protesters can be seen marching, taking photos, and placing bricks and tires in the road. While initially, the protest seemed large, a level of organization is apparent. As the protest gained momentum, protester deaths are noted in reports of violence.[150] Videos and photos of the early stages of the protest also indicate that the majority of the protest is working-age adults, but as the protest continues into the late morning and early afternoon, younger adults are seen in videos and photos, which is likely related to both the mass disruption and the closing of schools in anticipation of the protest.[151]

The protest quickly moved to social media, as a fight to control the narrative began between the BJP, protesters and the state. From approximately 10 a.m. local time to 5 p.m. local time there were a reported six deaths from protester clashes with riot control police forces.[152] While reports conflict on who the aggressors were in the violence, YouTube videos show alleged protester-on-protester violence. In one video posted on YouTube, a younger crowd can be seen beating a man on the ground as older men step in to stop the crowd. While the older men initially quell the violence, it is not until the riot control police arrive that the crowd disperses, leaving the wounded man on the ground.[153] The protest continues to remain semi-organized, as trucks lead lines of protesters down roads playing music, as the protesters chant and march behind.[154]

---

[149] "PHOTOS: Bharat Bandh Pictures: Protests against SC/ST Act Turn Violent | The Indian Express| Page 36," *The Indian Express* (blog), April 2, 2018, https://indianexpress.com/photos/india-news/bharat-bandh-dalit-protest-sc-st-atrocities-act-violent-5120337/.

[150] "PHOTOS: Bharat Bandh Pictures: Protests against SC/ST Act Turn Violent"

[151] "Elaborate on 'Conspiracy' Behind Violence in Bharat Bandh: SC Panel to States," News18, accessed October 6, 2018, https://www.news18.com/news/india/send-detailed-report-on-conspiracy-behind-violence-in-bharat-bandh-scheduled-caste-panel-to-states-1708089.html; Kamal Sappra Films, *Bharat Band | 2 April 2018 |*, accessed October 6, 2018, https://www.youtube.com/watch?v=X2ypeJk112U.

[152] "Bharat Bandh," April 2, 2018.

[153] It's Bunny Sharma, *Bharat Band 2 April Protest Latest Video Violence.*, accessed October 6, 2018, https://www.youtube.com/watch?v=ZBUp9_R6YVU&has_verified=1.

[154] It's Bunny Sharma, *Bharat Band 2 April Protest Latest Video Violence.*

At 7 p.m. local time, Section 144 was imposed, and internet services were shut down.[155] Shortly after Section 144 was imposed, the protest transitioned into amorphous riots with a heavy emphasis on looting.[156] It is possible people feel emboldened by the inability to use ICTs and transitioned to opportunistic looting, combined with feelings of helplessness and frustration from further repression on an already marginalized group. By the time the protest slowed down on April 4, another four people would die during the ensuing violence.[157] Ultimately, it is apparent that shutting off the internet did not stop, or slow the violence, but rather it forced an environmental and subsequently a human behavior change in how the collective action evolved, resulting in increased violence. Interestingly, while technology is not responsible for creating protests, it becomes an expected resource. When that resource is denied, there is a frustration associated with its loss. Additionally, the internet likely provides an outlet for expression, while also providing a degree of organization to the protests.

India does not plan to alter its tactics regarding the use of strategic shutdowns. Despite this research demonstrating that shutdowns do not stop violence and other academic research demonstrating that shutdowns do not stop mobilizations, the question remains why do we see high rates of shutdowns across the world, but specifically in India? It appears that the notoriety from the repression of networked collective action by autocracies to eliminate opposing views garnered significant attention by states globally, which could be viewed as a metric of success, even if the metric is flawed. This is likely compounded with the concept that in democracies, demonstrating action to political base is an important aspect of power. The action of strategic shutdown is likely viewed as a positive non-violent approach to a civil unrest event, while in reality, the opposite is true.

---

[155] "Bharat Bandh," April 2, 2018.

[156] It's Bunny Sharma, *Bharat Band 2 April Protest Latest Video Violence.*

[157] Sandya Fuchs, "Indian Supreme Court Curbs One of the World's Most Powerful Anti-Discrimination Laws," *Opendemocracy.Net*, May 26, 2018, https://www.printfriendly.com/p/g/7Kxgrw; Kamal Sappra Films, *Bharat Band | 2 April 2018 |*, accessed October 6, 2018, https://www.youtube.com/watch?v=X2ypeJk112U.

H. BEYOND THE #BHARATBANDH

The Bharat Bandh case study provides a glimpse into digital repression, violence, protest and civil unrest. As technology changes, collective action and states adapt at varying speeds, but technology is rapidly outpacing both research and norms. States are no longer denying the internet's consequences, but instead, acknowledge it for the dangers and opportunities that exist through it.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION AND FUTURE STUDIES

A. AREAS OF FURTHER RESEARCH

This research provides a qualitative and quantitative analysis of how digital repression impacts violence in India. Furthermore, the research demonstrated that the current tactics of utilizing internet shutdowns to combat or contain violence are ineffective at best and damaging at worst. While this research primarily focused on how digital repression affected violence, it also touched on how current digital repression appears to change the dynamics of mobilization during the collective action, but this is an area that remains open for academic research to answer fully. Additionally, a comparison of violence levels between autocracies and democracies following digital shutdowns would further provide insight. Finally, sentiment and narrative analysis of both the protesters and state before and after the shutdown would provide a deeper understanding of why the increase of violence occurs following a shutdown.

B. SUMMARY OF ANALYSIS

This thesis is a stark reminder that the internet is deeply intertwined with human behavior and that misunderstanding this implication is dangerous. It is concerning that the tactic of using digital repression as a tool to stop internal violence is increasing in India, as the data demonstrates that the opposite is true. While there are many non-governmental organizations approaching the problem of digital repression as a freedom of speech issue, the relationship of digital repression and increased violence goes unnoticed. The challenge of drawing the connection between digital repression and violence is that the effects are not immediate. The moment the internet is turned off the streets do not instantly turn violent, but rather the day following, as the protest organizational structure fails, and the internet as an outlet of expression goes away that the civil unrest events increase in violence.

The battle between digital liberation and digital repression is far from over. The scale will continue to swing back and forth from the states to individuals as the world struggles to understand the complex and evolving nature of technology. While there are

still many unknowns in how technology, collective action, and repression evolves, this research on digital repression in India clearly shows a relationship between digital repression and increased violence.

LIST OF REFERENCES

Agur, Colin, Ramesh Subramanian, and Valerie Belair-Gagnon. “Interactions and Policy-Making: Civil Society Perspectives on the Multistakeholder Internet Governance Process in India,” *Internet Policy Observatory*, 2015, 32.

Ali, Sk Jahangir, and Santanu Sen. “Is ‘Bandh’ Constitution or Unconstitutional in India?” Balurghat: Balurghat Law College, February 7, 2013.

Asal, Victor, Jacob Mauslein, Amanda Murdie, Joseph Young, Ken Cousins, and Chris Bronk. “Repression, Education, and Politically Motivated Cyberattacks.” *Journal of Global Security Studies* 1, no. 3 (August 1, 2016): 235–47. https://doi.org/10.1093/jogss/ogw006.

Banerjee, Sumanta. “Civilizing the BJP.” *Economic and Political Weekly* 40, no. 29 (2005): 3116–19.

Barlow, John. “A Declaration of the Independence of Cyberspace.” Electronic Frontier Foundation, January 20, 2016. https://www.eff.org/cyberspace-independence.

Best, Michael L., and Keegan W. Wade. “The Internet and Democracy: Global Catalyst or Democratic Dud?” *Bulletin of Science, Technology & Society* 29, no. 4 (August 2009): 255–71. https://doi.org/10.1177/0270467609336304.

“Bharat Bandh: Death Toll in Madhya Pradesh Hits 7, 51 FIRs Lodged—Times of India.” *The Times of India*. Accessed August 31, 2018. https://timesofindia.indiatimes.com/city/bhopal/bharat-bandh-death-toll-in-madhya-pradesh-hits-7-51-firs-lodged/articleshow/63595081.cms.

“Bharat Bandh: Protests by Dalit Groups over SC/ST Act on April 2, 2018—As It Happened.” Zee News, April 2, 2018. http://zeenews.india.com/india/live-updates/bharat-bandh-live-news-updates-strike-across-india-2095564.

Bowe, Brian J., and Robin Blom. “Cosmopolitanism and Suppression of Cyber-Dissent in the Caucasus: Obstacles and Opportunities for Social Media and the Web.” *Journal of Media Sociology*, 2011, 5.

Censorship, Index on. “India: Digital Freedom under Threat?” *Index on Censorship* (blog), November 21, 2013. https://www.indexoncensorship.org/2013/11/india-online-report-freedom-expression-digital-freedom/.

“Center for Systemic Peace.” Accessed February 7, 2018. http://www.systemicpeace.org/index.html.

Clionadh, Raleigh, Andrew Linke, Hegre Håvard, and Karlsen Joakim. “Introducing ACLED—Armed Conflict Location and Event Data.” *Journal of Peace Research* 46, no. 5 (2010): 1–10.

“Congress Accuses BJP Govts of Targeting Dalits after Bharat Bandh.” Accessed October 6, 2018. https://www.nationalheraldindia.com/india/congress-accuses-bjp-governments-of-targeting-dalits-after-bharat-bandh.

Daniyal, Shoaib. “The WhatsApp Wires: How Dalits Organized the Bharat Bandh without a Central Leadership.” Text. Scroll.in. Accessed August 31, 2018. https://scroll.in/article/874714/the-whatsapp-wires-how-dalits-organised-the-bharat-bandh-without-a-central-leadership.

David Kaye, and Michel Forst. “OHCHR | India Must Restore Internet and Social Media Networks in Jammu and Kashmir, Say UN Rights Experts.” United Nations Human Rights Office of the High Commissioner, May 2017. http://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=21604&LangID=E.

Desk, The Hindu Net. “The Hindu Explains: What Triggered the ‘Bharat Bandh’?” *The Hindu*, April 2, 2018, sec. National. https://www.thehindu.com/news/national/the-hindu-explains-what-triggered-the-bharat-bandh/article23416602.ece.

Diamond, Larry. “Liberation Technology.” *Journal of Democracy* 21, no. 3 (July 14, 2010): 69–83. https://doi.org/10.1353/jod.0.0190.

Dunn, Alexandra. “Unplugging a Nation: State Media Strategy During Egypt’s January 25 Uprising.” *The Fletcher Forum of World Affairs*, 2011, 10.

Durac, Vincent. “Social Movements, Protest Movements and Cross-Ideological Coalitions—The Arab Uprisings Re-Appraised.” *Democratization* 22, no. 2 (February 23, 2015): 239–58. https://doi.org/10.1080/13510347.2015.1010809.

“Eight Dead in Massive India Caste Protests.” *BBC News*, April 2, 2018, sec. India. https://www.bbc.co.uk/news/world-asia-india-43616242.

“Freedom House.” Accessed February 7, 2018. https://freedomhouse.org/.

Fuchs, Sandya. “Indian Supreme Court Curbs One of the World’s Most Powerful Anti-Discrimination Laws.” *Opendemocracy.Net*, May 26, 2018. https://www.printfriendly.com/p/g/7Kxgrw.

Gohdes, Anita R. “Pulling the Plug: Network Disruptions and Violence in Civil Conflict.” *Journal of Peace Research* 52, no. 3 (May 1, 2015): 352–67. https://doi.org/10.1177/0022343314551398.

Gohdes, Anita R. “Studying the Internet and Violent Conflict.” *Conflict Management and Peace Science* 35, no. 1 (January 2018): 89–106. https://doi.org/10.1177/0738894217733878.

Golkar, Saeid. “Liberation or Suppression Technologies? The Internet, the Green Movement and the Regime in Iran.” *International Journal of Emerging Technologies and Society; Hawthorn* 9, no. 1 (2011): 50–70.

“Google Transparency Report.” Accessed June 7, 2018. https://transparencyreport.google.com/.

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

Harrell, Peter, and Collin Anderson. “U.S. Sanctions Abet Iranian Internet Censorship.” *Foreign Policy* (blog). Accessed February 3, 2018. https://foreignpolicy.com/2018/01/22/u-s-sanction-abet-iranian-Internet-censorship/.

Hassanpour, Navid. *Leading from the Periphery and Network Collective Action*. Cambridge, United Kingdom ; New York, NY: Cambridge University Press, 2017.

Heydemann, Steven, and Reinoud Leenders. “Authoritarian Learning and Authoritarian Resilience: Regime Responses to the ‘Arab Awakening.’” *Globalizations* 8, no. 5 (October 1, 2011): 647–53. https://doi.org/10.1080/14747731.2011.621274.

Hlavac, Marek. *Stargazer: Well-Formatted Regression and Summary Statistics Tables* (version 5.2.1), 2018. https://CRAN.R-project.org/package=stargazer.

“India 2017/2018.” Accessed September 4, 2018. https://www.amnesty.org/en/countries/asia-and-the-pacific/india/report-india/.

“India Country Report | Freedom on the Net 2017,” November 14, 2017. https://freedomhouse.org/report/freedom-net/2017/india.

“Internet Shutdowns in India.” Accessed May 6, 2018. https://internetshutdowns.in.

Kamath, Anant. “‘Untouchable’ Cellphones? Old Caste Exclusions and New Digital Divides in Peri-Urban Bangalore.” *Critical Asian Studies* 50, no. 3 (July 3, 2018): 375–94. https://doi.org/10.1080/14672715.2018.1479192.

“#KeepItOn.” *Access Now* (blog). Accessed May 4, 2018. https://www.accessnow.org/keepiton/.

Murthy, Laxmi, *Clampdowns and Courage: South Asia Press Freedom Report 2018*, (Brussels, Belgium: International Federation of Journalists 2018), https://reliefweb.int/sites/reliefweb.int/files/resources/Clampdowns_and_Courage_-_LR_DP_0.pdf

Mahmoudi, Firuzeh, and Fereidoon Bashar. "Tech Companies Are Complicit in Censoring Iran Protests | WIRED." Accessed February 6, 2018. https://www.wired.com/story/tech-companies-are-complicit-in-censoring-iran-protests/.

Managing Democracy in the Digital Age: Internet Regulation, Social Media Use, and Online Civic Engagement, edited by Julia Schwanholz, Todd S. Graham, and Peter-Tobias Stoll. New York, NY: Springer Berlin Heidelberg, 2017.

Marshall, Monty G., and Gabrielle Elzinga-Marshall. "TABLE 1: STATE FRAGILITY INDEX AND MATRIX 2016," 2016, 10.

McAdam, Doug, John D. McCarthy, and Mayer N. Zald, eds. *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Cultural Framings*. First Edition. Cambridge England ; New York: Cambridge University Press, 1996.

McCarthy, Niall. "The Countries with the Most STEM Graduates [Infographic]." Forbes. Accessed May 4, 2018. https://www.forbes.com/sites/niallmccarthy/2017/02/02/the-countries-with-the-most-stem-graduates-infographic/.

Mottahedeh, Negar. *#iranelection: Hashtag Solidarity and the Transformation of Online Life*. 1st edition. Redwood City, CA: Stanford Briefs, 2015.

"PolityProject." Accessed May 6, 2018. http://www.systemicpeace.org/polityproject.html.

Rajat Kathuria, Mansi Kedia, Vatsala Shreeti, and Parnil Urdhwareshe. "Quantifying the Value of an Open Internet for India." *ICRIER*. Accessed May 4, 2018. http://icrier.org/pdf/open_Internet.pdf.

Ritter, Daniel P., and Alexander H. Trechsel. "Revolutionary Cells: On the Role of Texts, Tweets, and Status Updates in Nonviolent Revolutions." In *Conference on "Internet, Voting and Democracy," Laguna Beach, CA*, Vol. 3. Citeseer, 2011.

Sauter, Molly, and Ethan Zuckerman. *The Coming Swarm: DDOS Actions, Hacktivism, and Civil Disobedience on the Internet*. New York ; London: Bloomsbury Academic, 2014.

The Scheduled Castes and The Scheduled Tribes (Prevention of Atrocities) Act 1989, Pub. L. No. 33 of 1989, 9 (1989).

Schofield, Victoria. *Kashmir in Conflict: India, Pakistan and the Unending War*. 3rd edition. London: I.B.Tauris, 2000.

"Section 69A in The Information Technology Act, 2000." Accessed May 6, 2018. https://indiankanoon.org/doc/10190353/.

"Section 144 in The Code of Criminal Procedure, 1973." Accessed May 6, 2018. https://indiankanoon.org/doc/930621/.

Shirky, Clay. "The Political Power of Social Media: Technology, the Public Sphere, and Political Change." *Foreign Affairs* 90, no. 1 (2011): 28–41.

Snow, David A., Sarah A. Soule, and Hanspeter Kriesi. *The Blackwell Companion to Social Movements*. 1 edition. Malden, MA: Wiley-Blackwell, 2007.

Soldatov, Andrei, and Irina Borogan. *The Red Web: The Kremlin's Wars on the Internet*. Reprint edition. New York: PublicAffairs, 2017.

Tanczer, Leonie Maria, Ryan McConville, and Peter Maynard. "Censorship and Surveillance in the Digital Age: The Technological Challenges for Academics." *Journal of Global Security Studies* 1, no. 4 (November 1, 2016): 346–55. https://doi.org/10.1093/jogss/ogw016.

The Tor Project. "Tor Project | Privacy Online." Accessed May 25, 2018. https://www.torproject.org/.

Tufekci, Zeynep. *Twitter and Tear Gas: The Power and Fragility of Networked Protest*. New Haven ; London: Yale University Press, 2017.

"United Nations Population Division | Department of Economic and Social Affairs." Accessed May 6, 2018. http://www.un.org/en/development/desa/population/.

"Unshackling Expression: A Study on Laws Criminalizing Expression Online in Asia – The Internet Democracy Project." Accessed May 4, 2018. https://internetdemocracy.in/reports/unshackling-expression-a-study-on-laws-criminalising-expression-online-in-asia/.

Urdal, Henrik. "Population, Resources, and Political Violence: A Subnational Study of India, 1956–2002." *Journal of Conflict Resolution* 52, no. 4 (August 2008): 590–617. https://doi.org/10.1177/0022002708316741.

Valeriano, Brandon. "'Closing That Internet Up': The Rise of Cyber Repression." Council on Foreign Relations. Accessed May 4, 2018. https://www.cfr.org/blog/closing-Internet-rise-cyber-repression.

Warren, T Camber. “Explosive Connections? Mass Media, Social Media, and the Geography of Collective Violence in African States.” *Journal of Peace Research* 52, no. 3 (May 2015): 297–311. https://doi.org/10.1177/0022343314558102.

West, Darrell M. *Internet Shutdowns Cost Countries $2.4 Billion Last Year,* (Washington, DC: Brookings, 2016), https://www.brookings.edu/research/internet-shutdowns-cost-countries-2-4-billion-last-year/

www.ETtech.com. “Supreme Court Upholds Internet Ban by States—ETtech.” ETtech.com. Accessed May 25, 2018. http://tech.economictimes.indiatimes.com/news/Internet/supreme-court-upholds-Internet-ban-by-states/50955292.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California