MALD Capstone

Reaching for the Techno-Nationalist Toolbox:
What are the breeding grounds for state-directed internet shutdowns?

Submitted to Professor Bhaskar Chakravorti
Spring 2019
Conor L. Sanchez
In full fulfillment of the MALD Capstone requirement
April 23, 2019

THE FLETCHER SCHOOL
OF LAW AND DIPLOMACY
TUFTS UNIVERSITY

Conor L. Sanchez
Master of Law and Diplomacy
The Fletcher School of Law and Diplomacy
April 2019

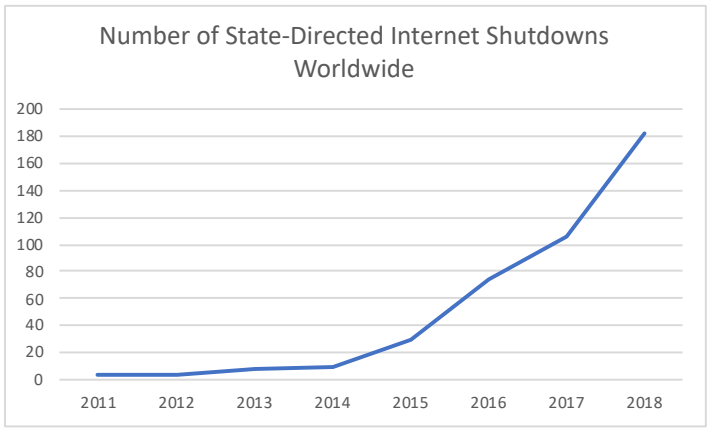
EXECUTIVE SUMMARY

In its 36 years of existence, the internet has served as a powerful information-sharing tool, transforming nearly every aspect of our lives from how we communicate to how we stay informed and transact business. By drastically reducing the cost of sending and receiving data, the technology has delivered tremendous economic, social, and political benefits to societies around the world. Owing to its decentralized nature, it is also thought to be revolutionary in its inherent resilience to political interference, leading President Bill Clinton to once joke that China's attempt to crack down on the internet was "sorta of like trying to nail Jell-O to the wall."[1]

In the 21st century these idealistic impressions have been tempered by examples of the internet's ability to serve as a conduit for more harmful human behavior, including hate speech, misinformation, and increased surveillance. Its resilience to political control has also been challenged. Whereas President Ronald Reagan once predicted that "the Goliath of totalitarianism will be brought down by the David of the microchip,"[2] several authoritarian regimes have demonstrated they can exploit the economic benefits while retaining power. In the last five years, another worrying trend has begun to stand out; governments around the world, but particularly in developing countries, are exhibiting an increased willingness to hijack the internet's control valves during bouts of social unrest. Since 2011, the number of instances and the frequency with which nation-states have disconnected internet or mobile networks has increased multifold. In fact, of the nearly 3.7 billion people that have access to the internet today, 42 percent of them lived under governments that disconnected the internet or mobile networks in 2018.[3] The cost of these so-called internet shutdowns is potentially massive and will only continue to grow as the

[1] Cunningham, "'The Great Firewall of China' Review."
[2] "Caught in the Net."
[3] Shahbaz, "Freedom on the Net 2018: The Rise of Digital Authoritarianism."

digital economy merges with the traditional. One report from the Brookings Institution found that shutdowns in nineteen countries from July 2015 through June 2016 cost $2.4 billion.[4] The reason behind them are myriad, however, many governments cite national security concerns, claiming the internet is fueling unrest and leading to violence, and the only way to control such situations is to immediately curb online information flows. Over the last few years, shutdowns sometimes coincided with elections, but a great deal of them occurred in the midst of some controversial news development, such as a high-profile trial or the rapid spread of misleading and incendiary information via social media platforms. A few countries offer more innocent but equally curious assertions, such as it prevents cheating during national exams.[5]



Internet shutdowns directed by governments have been on the rise since 2011, but they spiked significantly between 2015 and 2018 (Source: Access Now and Oracle).

Regardless of the cogency of the justification, it is important that this growing trend in online censorship be examined more closely to better understand the circumstances under which they occur and hopefully determine what steps might be taken to reverse their upward trajectory. Whereas previous work on this subject has focused on how physical vulnerabilities, such as a dearth of international internet connections, make countries more at risk of experiencing shutdowns, this paper seeks to show how political, sociological, and institutional vulnerabilities are just as significant. It also goes beyond evaluating the potential economic costs of disruption, by identifying causal pathways that make countries more susceptible to shutdowns and thus, providing clearer visibility into what specific changes might deter

[4] West, "Internet Shutdowns Cost Countries $2.4 Billion Last Year."
[5] Madory, "Iraq Downs Internet To Combat Cheating...Again! | Dyn Blog."

governments from severing internet access. Using India as a case study, I try to identify a generally applicable set of ground conditions that lead to shutdowns.

Why it matters

The growing trend in internet shutdowns should be a concern for a variety of stakeholders in the public and private sectors as well as civil society. For governments hoping to advance their digital potential and launch themselves into a more advanced category of digital development, an institutional environment that allows officials to justifiably switch off the internet from time to time is ultimately incompatible with those goals. Though relegating the disruption to a specific region might enable governments to absorb the costs at the moment, the decision will ultimately become costlier, forcing more individuals to rely on the internet for their livelihoods and financial transactions. For technology companies seeking to grow their businesses globally, especially in emerging markets where the reliability of Information Communication Technology (ICT) is already a barrier, the idea that the government might disconnect users and clients has profound economic implications that should make them reconsider how they plan to operate in such environments. For civil society members concerned with digital rights, grassroots empowerment, or poverty alleviation, the ease with which these drastic measures are taken by governments should be of grave concern as such abuses of power can further marginalize vulnerable populations. And finally, for development initiatives that bring these three sectors together in an effort to close the digital divide by bringing reliable, affordable internet to the masses, shutdowns act in the complete opposite direction. This should remind all stakeholders that such initiatives need more than just infrastructure enhancements; they require reforms that put into place laws and regulations that help foster mature digital ecosystems.

Case Study: India

Complicating this trend is the fact that disruptions are occurring in a variety of regime types. The country with the highest number of shutdowns over the last eight years has not been an autocracy; it is the world's biggest democracy – India. Other democracies that have experienced shutdowns include Brazil, the Philippines, South Korea, Indonesia, and, on at least one occasion and in a highly localized situation, the United States. India serves as a prime case study in understanding the broader trend of shutdowns globally because of its quantity and frequency of occurrences, the wide-variety of justifications used by authorities, and the fact that many of the underlying characteristics that describe India's institutional and sociological environments closely resemble that of other developing countries. It is perhaps a bellwether for the types of dilemmas many may end up facing in the 21st century as technology, especially in its mobile forms, connects us in unprecedented ways, often leapfrogging other forms of media. This development can be a force for good, giving communities access to information that strengthens their skillsets, increases their access to financial resources such as bank accounts and credit, and – at least in democracies – better informs their votes. But it can also be a force for harm, allowing for the spread of false or misleading information intended to distort the truth, influence votes, or otherwise manipulate human behavior for nefarious reasons. As many examples demonstrate, the spread of this type of low-quality information can be deadly. At the same time, the internet is said to be growing less free around the world; existing ethnic and sectarian rifts are amplified by the internet's tendency to fragment information and further polarize social groups, giving antidemocratic forces an advantage over free societies as authoritarian figures exploit such divides. Finally, India's geopolitical position also makes it a valuable case study. Caught between powers that view the internet as a force for individual empowerment and those who view it as a force for state control, it sits among a group of nations that have yet to decide which

vision it will end up pursuing; given the influence it has globally, regionally, and within global cyber policy circles, which direction India moves towards will inevitably impact how other countries deal with the technology's challenges in the years ahead. With 4 billion people still waiting to come online, most of whom live in developing countries, the lessons gleaned from India can be applicable to helping ensure their arrival to cyberspace is marked more by the internet's positive forces, both in terms of economic progress and individual rights, than its more harmful ones.

Methodology

My research was conducted through secondary sources such as books, research papers, news articles, and data collected by a digital rights advocacy group as well as the global technology company Oracle. Some empirical studies of researchers were also approached to decipher the relation between technology, social movements, and state repression. To better understand where shutdowns were occurring and under what regime types, I added up occurrences between the years 2011 and 2018. Zooming in on India, I isolated the occurrences from a global dataset during the period 2016-2018 and disaggregated this further to identify the number of occurrences and their duration at the state- and district-levels. This allowed me to develop a risk map that more accurately displays which regions have been more prone to experiencing internet shutdowns and compare that data with other trends occurring over the last three-year period in the same areas. I then evaluated how trends in the country's telecommunications market, state and national politics, institutions, and civil strife might be both pressuring and incentivizing local authorities to opt for internet shutdowns.

Key Insights

In the end, I identify a set of criteria along with potential proxies that cultivated breeding grounds for internet shutdowns across various states in India. These include:

- A rapid rise in new internet users
    - Proxy: International Telecommunication Union, World Telecommunication/ICT Development Report and database
- A history of media censorship
    - Proxy: Freedom House rankings on Freedom of the Press or Freedom of the Net
- Low levels of digital literacy
    - Proxy: Traditional literacy rates
- A rise in communal incidents and protests
    - Proxy: Armed Conflict Location & Event Data Project (ACLED) data on protests and riots
- Ethno-nationalist leadership
    - Proxy: Seats held by political parties that embrace ethno-nationalism
- A lack of public trust in criminal justice systems and a perceived lack of law enforcement
    - Proxy: Global survey by Gallup News on public's confidence in judicial systems and courts
- A weak law enforcement regime
    - Proxy: Rule of law score according to the World Justice Project (WJP)
- Sympathetic to the idea of greater sovereign control of the internet

- Proxy: New America's rankings on a country's likelihood to favor a sovereign and controlled internet

On their own, these trends do not explain the use of internet shutdowns, but taken collectively and concurrently, they describe an environment ripe for shutdowns, where forces of restraint during periods of unrest were weak. At a broader level, my conclusion states that a similar set of vulnerabilities in another country would raise the likelihood of governments acting on their more flawed inclinations when it comes to internet policy. This could come in the form of internet shutdowns but could also manifest in a number of different actions that fit within what I call the "techno-nationalist toolbox." In this toolbox are such interventions as data localization laws, strict content moderation policies, individual platform blocking, throttling, and other measures that impose strong sovereignty claims over the internet within a nation's boundaries. My conclusion urges all stakeholders, including the public and private sector as well as civil society, to push for institutional reforms to reduce the risk of such tools being used. The temptations for impeding data flows may never go away and, in fact, may only grow stronger as technology continues to challenge the state's control. The factors that decide whether shutdowns transform into habits, however, rely on the institutional environments that either restrain such temptations or enable them. Not only do strong institutions restrain governments from abusing their power, but they also alleviate situations that inspire unrest in the first place, especially vigilante justice and the impact of misinformation.

Who Will Find This Useful

This research will be useful to researchers interested in the intersection of the internet, policy, and development. By outlining the various country-level factors that lead to shutdowns, this paper lays the groundwork for future empirical research that could examine the causal links between some of these issues and the use of shutdowns. These insights can also help in the development of a global scorecard that would

hold governments accountable for their actions and hopefully encourage them to invest in strengthening their institutions and dissuade them from giving in to the temptations of using the techno-nationalist toolbox. The systematic use of ratings and rankings in making countries think twice about how their actions might impact their global reputation has become a powerful tool in bringing about change.[6] Finally, for technology industry actors who could build predictive models on shutdowns that would be valuable to various industries including investors, this paper will also prove instructive.

[6] Kelley, *Scorecard Diplomacy: Grading States to Influence Their Reputation and Behavior*.

Conor L. Sanchez
Master of Law and Diplomacy
The Fletcher School of Law and Diplomacy
April 2019

INTRODUCTION

As more people connect to an open and transnational internet, applying national policy within a specific jurisdiction has proven difficult for governments worldwide. While allowing individuals to connect and share abundant amounts of data undoubtedly grants nations significant economic benefits, the impact of the technology does not come without its fair share of difficulties. Rapid social mobilization fueled by the proliferation of mobile technology devices and their associated content-sharing platforms can produce powerful and potentially disruptive collective action, which places unprecedented pressures on government institutions. Adding to the complexity, however, is the fact that most of the platforms enabling these networks are operated by corporations headquartered outside a nation's territory. The pressure to respond is compounded when situations devolve into disorder and violence – handing leaders what they perceive as license to restore order by any means necessary. This is especially difficult in young democracies where institutions are weak and unprepared to deal with underlying issues that lead to social unrest; whereas autocratic governments face fewer constraints that would otherwise check their ability to constrain communication flows, developing democracies grapple with the need to balance notions of freedom of expression as well as economic development with the desire to maintain order. In the face of this complexity, some nations are resorting to blunt instruments that temporarily block platforms or, in the most aggressive cases, disconnect the internet completely – a practice known as state-directed internet shutdowns.

Confounding previous notions that only autocrats engage in aggressive forms of censorship, India has emerged as the biggest offender of so-called internet shutdowns. Some of the reasons behind the shutdowns are just as surprising; stopping misinformation campaigns on WhatsApp that

incite violent mobs, mitigating the potential for turmoil ahead of an election, and preventing cheating on exams are just a few examples of how governments have justified the curtailment of freedom of expression and the loss of potentially billions of dollars in revenue for companies reliant on the internet for business. With just over 4 billion people still offline, these issues may not be going away any time soon. Using data provided by Access Now, a non-profit organization that helps monitor censorship, as well as the technology company Oracle, this analysis sets out to investigate the circumstances surrounding internet shutdowns. To do this, I use India as case study in understanding the broader trend due to its large number of occurrences, the wide-variety of justifications used by authorities, and the fact that many of the underlying characteristics that describe India's sociological and institutional environment closely resemble that of other developing countries. By examining the institutional dynamics under which these drastic measures have been taken, I build off of previous research in this area and identify causal pathways that help explain why governments are treating the internet as a spigot that can be turned off during bouts of social unrest. Whereas previous work on this subject has focused on how physical vulnerabilities, such as a dearth of international internet connections, make countries more at risk of experiencing shutdowns, this paper seeks to show how political, sociological, and institutional vulnerabilities are just as significant. It also goes beyond evaluating the potential economic costs of disruption, by identifying a set of criteria that make countries more susceptible to shutdowns and thus, providing clearer visibility into what specific changes might curb their usage. The lessons derived from India's experience may be applicable to other contexts where absolute levels of digital advancement are low, but the pace of growth is high. These countries, while performing well in their overall digital

progress, are typically held back by poor institutional quality and have been encouraged to invest more in improving their institutions to make the next big leap forward.[7]

THE INTERNET AND THE STATE

The internet has served to both challenge and strengthen the state throughout its history. In its early years, many so-called "techno-optimists" preferred to think of it as a neutral space that transcended government jurisdiction. At the 1996 World Economic Forum, John Perry Barlow – co-founder of the Electronic Frontier Foundation (EFF) - went so far as to declare the independence of cyberspace from the "tyrannies" of government, admonishing them for thinking they could intervene to solve problems that needed fixing. "Where there are real conflicts...we will identify them and address them by our means...This governance will arise according to the conditions of our world, not yours. Our world is different." Likewise, in 2000, former U.S. President Bill Clinton delivered a speech at Johns Hopkins University, joking that China's attempt to crack down on the internet was "sorta of like trying to nail Jell-O to the wall."[8] While Barlow and Clinton correctly recognized the sovereign power of the internet, they may have underestimated the formidable pushback from nation-states.

The idea that a powerful information-sharing tool such as the internet would put an end to the Westphalian Treaty has its roots in the early the twentieth century, when some projected that telecommunications and jet travel would lead to the dissolvement of the territorial state; in its place nonterritorial actors such as multinational corporations, transnational social movements, and

[7] Chakravorti and Chaturvedi, "Digital Planet 2017: How Competitiveness and Trust in Digital Economies Vary Across the World."
[8] Cunningham, "'The Great Firewall of China' Review."

international organizations would come to dominate world politics.[9] The explosion in the quantity of free information that resulted from the internet would only serve to strengthen these globalizing forces. However, two years after Barlow's pronouncement, Joseph Nye, Jr. and Robert Keohane pushed back against these assumptions, writing that certain rules of the road would always be necessary to govern the internet, which would "require authority, whether in the form of public government or private or community governance."[10] Furthermore, projections of the nation-state's demise "failed to analyze how holders of power could wield that power to shape or distort patterns of interdependence that cut across national boundaries."[11] As we entered the new millennium, these debates continued, though with a growing recognition that states would come to play a significant role in internet governance.

The Conservative's Dilemma

The truth is, government policy has always been inseparable from the internet – it just wasn't big enough to notice yet. Until recently, three-quarters of the world lacked access to the internet and most of its functions operated under the guise of one nation (the U.S.), whereas today a much more heterogenous community exists online than ever before, including societies that harbor differing norms and values as they relate to information access. These populations also have varying levels of literacy and civil society strength. As Nye has asserted in recent years, "jurisdictions where [internet] technology was housed imposed their own laws and values"[12] and over the past two decades, other parts of the world have played catch up, trying to accommodate the internet's transnational

[9] Robert Keohane and Josphe Nye, "Power and Interdependence in the Information Age."
[10] Robert Keohane and Josphe Nye.
[11] Robert Keohane and Josphe Nye.
[12] "A Fragmented Internet? Proceedings of The 2017 Global Digital Futures Forum."

connectivity without compromising their own unique laws and cultural norms. The primary challenge for the state in pursuing such an objective is balancing the needs to ensure national security and retain control with the desire to leverage the internet's potential to encourage economic growth. This complex undertaking has come to be known as the "dictator's dilemma."

The concept of the dictator's dilemma refers to the balance that authoritarian governments must pursue when leveraging ICT for economic development and controlling for the democratizing influences that come from enhanced connectivity.[13] A substantial amount of research shows why such fears could be valid. So-called "liberation technologies" – which Hoover Institution senior fellow Larry Diamond defined as "any form of [ICT] that can expand political, social, and economic freedom", especially digital ICT such as the computer, the Internet, the mobile phone, and their associated social media platforms – have long been said to change the balance of power between state and society in favor of the latter. The potential for ICT to undermine repressive regimes was recognized as far back as 1989, when Ronald Reagan famously quipped that "the Goliath of totalitarianism will be brought down by the David of the microchip."[14] A number of subsequent global events appeared to affirm this prediction, from activists using mobile phones to organize against Suharto in 1998 in Indonesia and activists in Kyrgyzstan's Tulip Revolution in 2005 to Kuwait's women's suffrage movement in 2005.[15] In perhaps the millennium's first liberation technology victim, Howard Rheingold showed how Philippine President Joseph Estrada was driven from power by a "Coup de Text" in which tens of thousands of text messages were used against him by "smart mobs."[16] Clay Shirky

[13] Boas, "The Dictator's Dilemma?"
[14] "Caught in the Net."
[15] Meier, "Do 'Liberation Technologies' Change the Balance of Power Between Repressive States and Civil Society?"
[16] Howard Rheingold, *Smart Mobs: The Next Social Revolution; Transforming Cultures and Communities in the Age of Instant Access*.

elucidated how protests coordinated in part by text message, Facebook, and Twitter served to affect change in Moldova, Spain, India, South Korea, and Chile.[17] The potential of technology to help people organize and successfully challenge authoritarian leaders culminated in the Arab Spring (more accurately known as the Arab Awakening[18]), which demonstrably affected change on a regional scale.[19] As one activist in Egypt once put it, "We use Facebook to schedule our protests, Twitter to coordinate and YouTube to tell the world."[20] Since then, few doubted the role digital technology, especially social media, can play in challenging the state after seeing several leaders toppled in a matter of months.

Overtime, however, we have also learned how society's relationship with technology works both ways. After all, "citizens are not the only ones active in cyberspace. The state is online, too, promoting its own ideas and limiting what the average user can see and do."[21] Diamond as well as Patrick Meier have pointed out that equal consideration must be paid to "technologies of repression" and the power this bestows upon governments who view liberation technologies as a threat to the status quo. Here, too, the Arab Awakening illustrates the ability of states to pushback against the popular uprisings fueled by social media, most sharply evidenced by Egyptian president Muhammad Hosni El Sayed Mubarak's order that internet access and cell phone network be shut off.[22] As much as the successful uprisings are cited, it is often forgotten that the use of ICTs did not result in a successful Arab Awakening for most countries in North Africa and the Middle East. In countries like Sudan, Bahrain, Syria, and Libya, protests were brutally repressed, and thousands of protestors were killed. Meier's research, which tested whether ICTs empower repressive regimes at the expense of civil society, or vice versa, found mixed results. Using a mix of

[17] Shirky, "The Political Power of Social Media."
[18] Siobhan Macdermott, *The Folded Paper: Inventing Cyberdiplomacy,* p. 28.
[19] Siobhan Macdermott, p. 29.
[20] Meier, "Do 'Liberation Technologies' Change the Balance of Power Between Repressive States and Civil Society?"
[21] Bremmer, "Democracy in Cyberspace."
[22] Cohen, "Egyptian Internet Blackout Pushed Protests to Streets."

qualitative and quantitative methods, his conclusions suggested that increased internet access tipped the balance of power marginally in favor of civil society in Egypt, but not in Sudan.[23]

Given these two experiences, it has become widely acknowledged that while technology can be certainly be leveraged to mobilize individuals, strengthen civil society, and lead to more open and democratic societies,[24] it can also be commandeered by regimes to suppress dissent or quell grassroots social organization. In other words, governments are increasingly capable of weeding out information flows that challenge its authority from those that are conducive to growth, leading several scholars to posit that governments have actually gained the upper hand.[25] Some make more qualified arguments, that at least in the short to medium term, increased internet access around the world will benefit authoritarian regimes at the expense of dissidents and pro-democracy activists.[26] The country that has been most successful in demonstrating to the world how the internet can be brought to heel is China, which developed a firewall to monitor and censor all internet communication inside the country. James Griffith's book *The Great Firewall of China* warns how China's method of monitoring and censoring sends a message to other autocratic governments that it is possible to control the internet without compromising its ability to enhance value-added productivity.[27]

The idea that enhanced ICT development and state control over information flows are not necessarily diametrically opposed to one another defies previous understandings of how governments approach increased connectivity. Over three decades after the concept of the dictator's dilemma was expounded by former U.S. Secretary of State George Schultz's seminal piece in *Foreign Affairs*[28] (the idea

[23] Meier, "Do 'Liberation Technologies' Change the Balance of Power Between Repressive States and Civil Society?"
[24] Shapiro, *The Control Revolution: How the Internet Is Putting Individuals in Charge and Changing the World*.
[25] Morozov, *The Net Delusion: The Dark Side of Internet Freedom*.
[26] Chase and Michael Mulvenon, *You've Got Dissent! Chinese Dissident Use of the Internet and Beijing's Counter Strategies*.
[27] Cunningham, "'The Great Firewall of China' Review."
[28] Schultz, "Shaping American Foreign Policy."

was subsequently re-popularized by Christopher Kedzie in 1997[29]), growing evidence shows the complete opposite may be true. Perhaps having withstood an initial growth stage that required cautious adoption and having gained a certain level of savviness as to how to pull the communication flow levers, governments around the world appear to have leapt head-first into a global technology race that aims to both reap the economic benefits as well as to acquire a sophisticated toolbox for surveillance and dissemination within its jurisdictional borders. Whereas autocrats were once assumed to weigh the risks inherent in either too much connectivity or too little, governments seeking to gain control over a growing online public sphere may in fact be even more compelled to pursue ICT expansion. This shift has led some to argue that a better way of understanding present conditions is through the so-called "conservative dilemma," a term used by Asa Briggs and Peter Burke to describe the problem facing the Catholic Church during the age of Luther.[30] This dilemma focuses on whether or not the church should have addressed the public criticism put forward by the radicals or to fight them with their own weapons. This may be more useful in present day scenarios since it not only applies to autocrats but also to democratic governments and to religious and business leaders.[31]

Thus, the conservative's dilemma is a more apt framework for understanding state behavior when it comes to the internet not only because it acknowledges the challenges confronting a state experiencing a rapid increase in public access to information, speech, or assembly, but it also recognizes the options states possess in addressing those challenges. Shawn Powers and Michael Jabloonski argue that when a conservative government, be it in non-democratic or quasi-democratic systems, is confronted with widespread social unrest, it essentially has four options for restoring control: propaganda, censorship, total

[29] Kedzie, "Communication and Democracy: Coincident Revolutions and the Emergent Dictators."
[30] Briggs and Peter Burke, *A Social History of the Media: From Gutenberg to the Internet.* p. 76.
[31] Shirky, "The Political Power of Social Media."

information control, and violent repression. Each choice comes with certain risks and can therefore be flawed. For a growing number of states, this is the real dilemma facing leaders around the world.[32]

INTERNET SHUTDOWNS ON THE RISE

With this understanding of the broader developments in how governments confront ICT and the options they possess to control it, I now turn to situations when the state decides to deal with unrest somewhere between censorship and total information control. Network disruptions represent a unique subset of the various policy options governments can pursue in an effort to control the flow of information within its borders and its associated influences. They can be defined as the "intentional, significant disruption of electronic communication within a given area and/or affecting a predetermined group of citizens."[33] The most extreme of these cases are called internet shutdowns (also referred to as network shutdowns or blackouts), whereby electronic communications are rendered inaccessible or effectively unusable for a given population.[34] Shutdowns can entail a complete blocking of access in a country or region or it can be partial, where certain websites or applications are blocked, usually to prevent people from communicating or sharing information with each other on platforms that facilitate rapid communication, such as WhatsApp, Facebook, or other Voice over Internet Protocol (VoIP) services. A lighter version of network disruptions can also entail the slowing down of network traffic, a practice known as bandwidth throttling.

[32] Powers and Michael Jablonski, *The Real Cyber War: The Political Economy of Internet Freedom*, p. 164.
[33] Rydzack, "A Human Rights-Based Approach to Network Disruptions."
[34] "Policy Brief."

Conor L. Sanchez
Master of Law and Diplomacy
The Fletcher School of Law and Diplomacy
April 2019

Internet shutdowns imposed by governments on their own people are on the rise. According to data from Access Now and Oracle, the number of state-directed internet shutdowns jumped from just four in 2011 to 183 in 2018 (see Figures 1 and 2).[35] Though shutdowns may have occurred as far back as 2005,[36] the first well-known occurrence of a government effectively disappearing itself from the internet was in early 2011 in Egypt, with numbers starkly rising in 2016. In response, internet activists have been trying to collect and disseminate data to draw attention to the implications for both human rights and the economy.[37] In 2016, the United Nations Human Rights Council passed a resolution condemning "measures to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law."[38] In 2017, a controversial proposal was submitted to the African Network Information Center (AFRINIC), the agency that allocates the registration of internet IP addresses, that would sanction governments engaging in shutdowns by withholding IP addresses from them for one year.[39] The proposal was soundly rejected in light of concerns that doing so would merely politicize the internet address space.

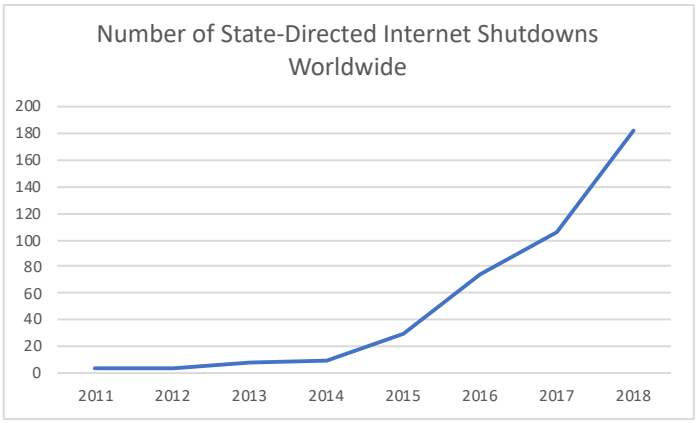


Figure 1: Internet shutdown directed by governments have been on the rise since 2011, but they spiked significantly between 2016 and 2018 (Source: Access Now and Oracle).

[35] "#KeepItOn."
[36] Vargas-Leon, *Tracking Internet Shutdown Practices: Democracies and Hybrid Regimes In: Musiani F., Cogburn D.L., DeNardis L., Levinson N.S. (Eds) The Turn to Infrastructure in Internet Governance. Information Technology and Global Governance.*
[37] Rydzack, "A Human Rights-Based Approach to Network Disruptions."
[38] "OHCHR | The Special Rapporteur's 2017 Report to the United Nations Human Rights Council."
[39] "Anti-Shutdown Proposal."

Citing national security concerns, governments claim the internet is fueling unrest. Despite that there is little evidence suggesting this,[40] authorities argue it is encouraging the spread of false information and leading to violence, especially during elections but also other politically charged events such as a high-profile case or an incendiary rumor. At most, studies have shown that social media serves as a useful but not sufficient tool for protest.[41] A few countries offer more innocent but equally curious assertions, such as it prevents cheating during national exams.[42] Regardless of the cogency of the defense, they all have the same basic objective; that is, to control the exchange of information online inside their borders. Such attempts at asserting control and the implications they have for global businesses, start-ups, or anyone that relies on internet connectivity for their livelihood make this issue deserving of further attention.

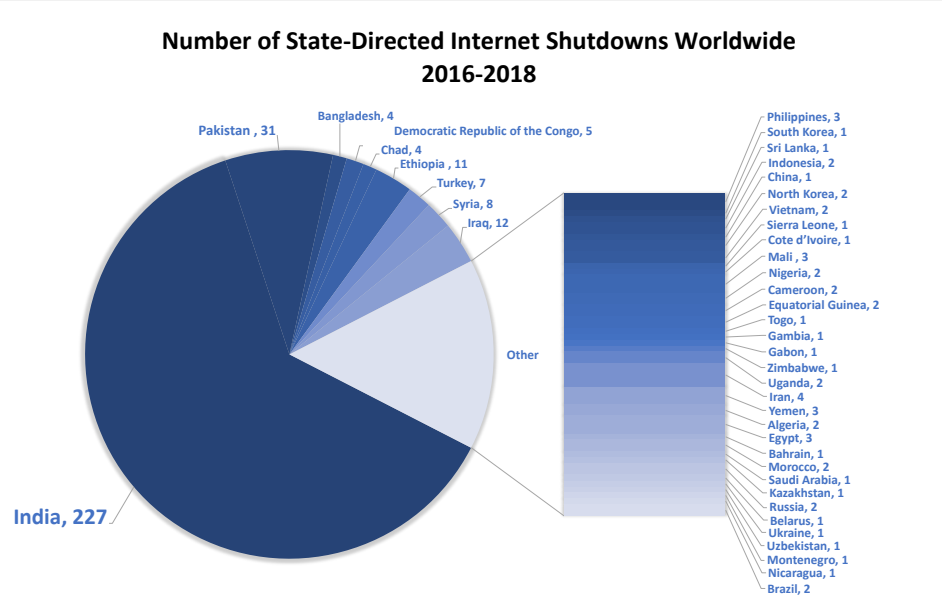


Figure 2: The vast majority of internet shutdowns have occurred in India in the years 2016-2018 (Source: Access Now and Oracle).

[40] Madrigal, "India's Lynching Epidemic and the Problem With Blaming Tech."
[41] Dewey et al., "The Impact of Social Media on Social Unrest in the Arab Spring."
[42] Madory, "Iraq Downs Internet To Combat Cheating...Again! | Dyn Blog."

Complicating this trend even further is the fact that shutdowns are occurring most often in places you might least expect (see Figure 3). In fact, the country with the highest number of shutdowns over the last three years has not been an autocracy; it's been the world's biggest democracy – India. Other democracies that have experienced shutdowns include Brazil, the Philippines, South Korea, Indonesia, and, on at least one occasion and in a highly localized situation, the United States (for a full list of countries that have experience shutdowns, see Appendix A). Despite being ranked lowest in the world for freedom on the internet, China does not rank very high in terms of shutdowns perhaps because their form of censorship is based more on a sophisticated system of monitoring and information filtering (a very strong form of total information control). In an environment where communication is constantly being censored, governments may not face the same temptation to completely disconnect. And yet, much of the research on network disruptions has focused almost exclusively on authoritarian regimes. Less attention has been paid to hybrid regimes and flawed democracies, where the vast majority of internet disruptions have occurred. While it is true that centralized state structures make life much easier by restricting the number of access points available to political leaders,[43] democratic governments are clearly finding ways to restrict information flows with relative ease.

[43] Giacomello, *National Governments and the Control of the Internet : A Digital Challenge*.

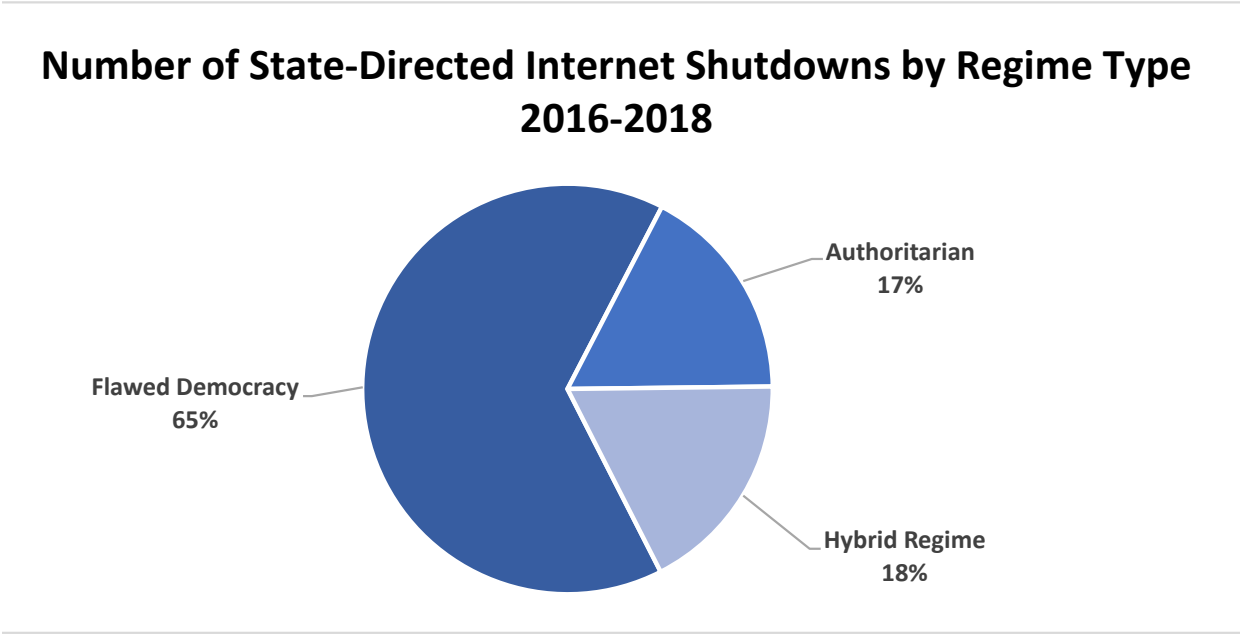


Figure 3: Most internet shutdowns are occurring in hybrid regimes and flawed democracies (Source: Access Now, Oracle, and the EIU Democracy Index).

Exploiting the Internet's Weaknesses

The assumptions held by Diamond and other techno-optimists relied heavily on the idea of the internet as a decentralized structure, giving it a high degree of resiliency. "The Net interprets censorship as damage and routes around it," John Gillmore famously told Time Magazine in 1993.[44] However, this failed to consider the various chokepoints where governments could effectively exert control. One of the big reasons why enhanced ICT can no longer be assumed to hinder or put at risk the state's control of information flows is the way in which governments have learned to manipulate those chokepoints.

When most people first learn about state-directed internet shutdowns, they immediately imagine a single point of control that would give a leader the ability to turn off internet access at the

[44] "The Internet Perceives Censorship as Damage and Routes Around It."

flip of a switch (hence, why it's often called a kill-switch option). Indeed, even the United States has considered legislation that would give the President such powers.[45] Some assume that shutdowns occur by damaging the physical cables that connect a country to the web, and while there are a few examples of this happening over the last few years,[46] it is rarely successful since countries often have multiple access points for cables. In reality, most internet shutdowns are orchestrated by targeting critical points in the internet infrastructure, namely Internet Service Providers (ISPs).

Targeting ISPs has been popular for two reasons, the first of which has been widely-acknowledged and researched – the second, less so; first, from a technical perspective, it is very effective in quickly blocking access for large groups of people. Governments simply identify which of the ISPs in their country have direct connections to foreign providers. Then, they make phone calls (sometimes followed by issuing a legal writ) ordering them to shut off power to a few of their facilities. What ISPs typically do in response is withdraw routes from the Border Gateway Protocol (BGP) – the internet's road map to autonomous systems (AS) and their respective identifying numbers (ASNs) – which essentially eviscerates a crucial mapping system that directs local traffic trying to leave a country's borders. This is exactly what happened in Egypt in 2011 during the Arab Awakening. A few minutes after midnight on January 27, the BGP route monitoring system operated by Dyn (which has since been acquired by Oracle) was able to observe the event in real-time (see Figure 4). "Every Egyptian provider, every business, bank, Internet cafe, website, school, embassy, and government office that relied on the big four Egyptian ISPs for their Internet connectivity is now cut off from the rest of the world," their blog reported the day of the event. This led analysts to make the logical conclusion that the fewer local ISPs that have international connections within a country,

[45] Lieberman, "S.3480 - 111th Congress (2009-2010)."
[46] "Something Is Happening in Congo-Brazzaville."

the easier it is to decouple the domestic internet from the global internet. Dyn actually developed an Internet Disconnection Risk index that was based on how many domestic network providers (AS) have direct connections, visible in routing, to foreign providers.[47]

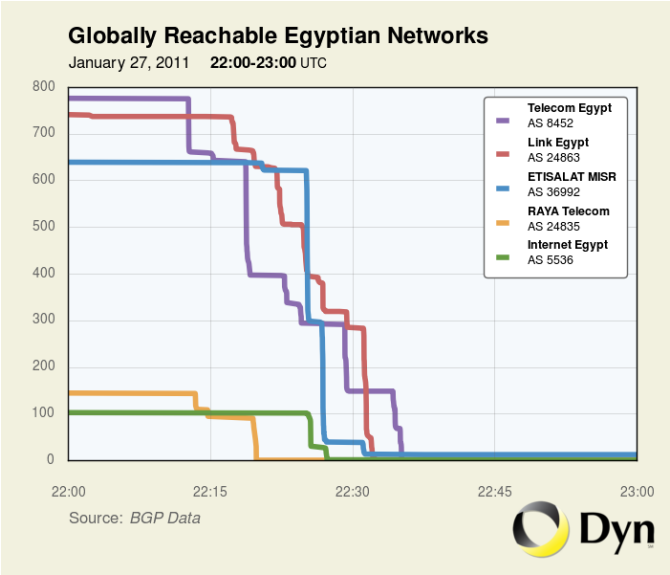


Figure 4: Dyn observed the internet shutdown in Egypt in 2011 during the Arab Awakening using their BGP route monitoring system. In the graphic above, the country's five biggest ISPs drop nearly simultaneously (Source: Oracle).

The second reason targeting ISPs is popular is because of the institutional dynamics that surround the relationships between ISPs and the state. For example, there are many contexts where telecommunication companies are state-owned, which makes compliance with government orders fairly uncontested. Even in environments where ISPs are privately held, they are typically reliant on governments for licensing contracts making them more pliant to government requests. These pressures are extremely well elucidated by Jan Rydzack in a 2018 report on how shutdowns impact human rights. Based on interviews with key stakeholders within and outside of the Global Network Initiative, a nonprofit advocating for the freedom of expression and privacy in the ICT sector, the report reveals the difficulty telecoms face in resisting orders to shut down connectivity. Telecom employees have faced threats for

[47] Cowie, "Could It Happen In Your Country?"

noncompliance, some of which have prompted them to flee the country.[48] The role of ISPs in disrupting internet services is also looked at by Tina Freyberg and Lisa Garbe, specifically in regard to ownership arrangements in sub-Saharan African countries. Their work argues that ISP ownership is a major factor in explaining internet shutdowns after finding a positive relationship between shutdowns and authoritarian states that have majority ownership in an ISP when facing election-related violence.[49]

Clearly, some combination of ICT infrastructure diversity and institutional dynamics play a role in determining a nation's risk level of experiencing an internet shutdown. However, the role of institutional dynamics has been far less examined. This research is needed since shutdowns are occurring in places that were given a low-risk designation by the Internet Disconnection Risk index developed by Dyn. India, for instance, despite holding the title for the most internet shutdowns, as well as Brazil were given a low-risk designation because they had at least 10 internationally-connected service providers. The Philippines, which has experienced the second highest number of internet disruptions over the last three years, was said to be extremely resistant. Part of the difficulty is due to the fact that shutdowns have become much more localized in recent years. It is rare for a government to shut down internet access at the country-level anymore. Instead, many countries have learned they can target shutdowns to specific regions. This makes a strong case for why institutional factors should be given closer examination, and not just generally, but specifically outside the context of an autocracy. Because India is a democracy, the ease with which an authoritarian government can shut down the internet does not help explain the set of circumstances facing young democracies or hybrid regimes. Moreover, not all deliberate network disruptions are provoked by direct threats to the state. Many are preemptive or reactive measures that seek to avoid or mitigate violence

[48] Rydzack, "A Human Rights-Based Approach to Network Disruptions."
[49] Freyburg and Garbe, "Authoritarian Practices in the Digital Age| Blocking the Bottleneck."

resulting from misinformation campaigns on social media platforms. For these reasons, my research zeroed-in on a democratic country that from a technical perspective appears fairly resilient.

CASE STUDY: INDIA

India serves as a prime case study in understanding the broader trend of shutdowns globally because of its large number of occurrences, the wide-variety of justifications used by authorities, and the fact that many of the underlying characteristics that describe India's institutional environment closely resemble that of other developing countries. It is perhaps a bellwether for the types of dilemmas many may end up facing in the 21st century as technology, especially in its mobile forms, spreads and connects us in unprecedented ways, often leapfrogging other forms of media. It also makes it another example of how governments may no longer feel torn between asserting control over online information flows and leveraging the economic benefits of ICT. In their estimation, they can do both. But before jumping into India's use of internet shutdown, I want to first provide some additional context for the country's digital development overall as well as its geopolitical positioning, both of which I believe are pertinent to the discussion.

Break Out Country

India's use of internet disruptions is all the more remarkable given its embrace of technology as a tool for development. In fact, according to the Digital Evolution Index (DEI), a research initiative by The Fletcher School in cooperation with MasterCard that ranks countries based on their progress in digital development, India falls within the Break Out quadrant of the DEI Chart (see Appendix C). These countries are said to low-scoring in their current states of digitalization but are evolving rapidly. Moreover, the digital economy in these countries has been given high priority by their policy makers.

Starting in 2012, India's national government pushed to expand internet access across the country. It recognized broadband connectivity as "a basic necessity," not unlike education or healthcare, and touted a "right to broadband." In 2015, the government under Prime Minister Narendra Modi went further by launching the Digital India initiative to transform itself into a digitally empowered society and economy.[50] The program promised to build broadband "highways," ensure universal access to mobile connectivity, and build a public internet access program. In 2018, the financial allocation for Digital India was doubled from the year prior.[51] Among other initiatives, the program proposes to use satellites, balloons, or drones to push faster digital connections to remote parts of the country.[52] A program known as *Digi Dhan Abhiyan* was designed to promote digital payments to 10 million people living in rural areas.[53] These efforts are just a few of many that have taken on urgency in the past few years as the government has pushed to digitize financial transactions.[54]

The Indian government has not been alone in its enthusiasm for increased connectivity. Global technology companies have been eager to tap into India's market by helping to connect the remaining 900 million people still offline. Google installed its own free WiFi service at over 100 railway stations across India, while Facebook swapped out its Free Basics program (which ran into problems after India passed strong net neutrality laws) for Express WiFi.[55] For Facebook's messaging app WhatsApp, India is a critical market because it has more than 200 million users here, more than any other country.[56] The rush to connect combined with consumption growth and a young population portend large growth in areas such as

[50] "Digital India Programme | Department of Electronics & Information Technology, Government of India."
[51] "Budget 2018: Booster for Digital India Plan; Govt to Install Wi-Fi Hotspots | Business Standard News."
[52] "Centre Ready to Use Satellites, Drones to Connect to Rural India: Ravi Shankar Prasad - The Economic Times."
[53] "Digi Dhan Abhiyan: Over 25 Lakh Rural Citizens Adopt Digital Payments, Claims MeitY - News18."
[54] Sorrel and Sorrel, "In India, 1,000 Villages Will Become Free Internet Hotspots."
[55] Iyengar, "India Is Planning to Give Free WiFi to More than 1,000 Villages."
[56] "Two Years Ago, India Lacked Fast, Cheap Internet -- One Billionaire Changed All That."

e-commerce, FinTech, and mHealth. In 2018, Walmart made a USD $16 billion investment into Flipkart, India's biggest online retailer with 54 million active customers, for a 77 percent share of the online retailer.[57] Other companies such as Tencent, Tiger Global, Microsoft, and Accel are also investors in the company. One report from Morgan Stanley projects that digitization efforts in India are putting the country's nominal GDP growth on track to compound annually by more than 10 percent in the next decade.[58]

Indeed, internet usage in India has climbed significantly in the last few years, attracting considerable investment from around the world. Although internet penetration remains low (43 percent as of September 2018), the composition of internet users is striking for its growth in mobile penetration (see Figure 5).[59] It is already the world's second largest smartphone market, with over 220 million users and an expected increase to 700 million in 2020.[60] As a result of these changes, it comes as little surprise that the vast majority of Indians are accessing the internet predominantly via their mobile devices, which are leaps and bounds more common than personal computers. The PC penetration rate in India is about 5 percent as compared to the 75 percent rate for

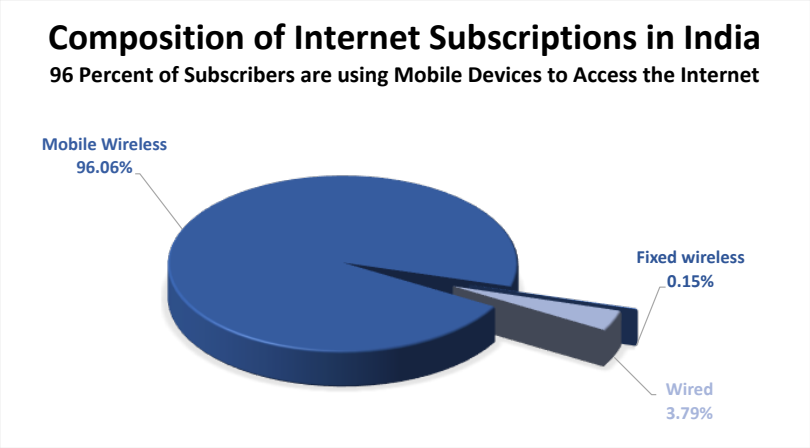


Figure 5: For most Indians, mobile is the portal to the Internet, in large part because mobile devices are now much more common than computers (Source: TRAI).

[57] "Walmart Confirms $16B Flipkart Investment, Giving It 77% in India's e-Commerce Leader."
[58] "India's Digital Future."
[59] "The Indian Telecom Services Performance Indicators July – September, 2018," p. ii.
[60] "Smartphone Market in India."

mobile devices.[61] This is further evidenced by the slow growth rate of fixed broadband internet usage rates as compared to the mobile cellular subscription rates. It is currently estimated the 34 percent of Indians access the internet exclusively via mobile devices, which is influencing how companies with online business models are approaching the Indian market. Flipkart, for example, is predicting that 75-80 percent of their traffic will come from mobile platforms.[62]

These changes have been accelerated in large part due to a major shake-up in the Indian telecommunications market. Officially, there are 156 ISPs in India, but there are 10 that control over 98 percent of the market.[63] In 2016, Reliance Jio Infocomm Ltd., a subsidiary of Reliance Industries Ltd., entered the market offering all-inclusive service plans at extremely cheap rates in an attempt to bring more people online. Within a few months, the company made massive gains, attracting over 50 million users with analysts predicting it will draw as many as 400 million users by March 2020 (see Figure 6).[64] They now have the highest ISP market share, followed by Bharti Airtel, Vodafone, Idea, and state-owned BSNL. Among the mobile operators, Bharti Airtel still controls about 24 percent of the market, followed by Vodafone, Idea, and then Reliance Jio,[65] but the impact Jio has had on the market as well as on internet usage overall throughout the country cannot be overstated; the price slashing resulted in a data binge for millions of Indians. Jio transmitted more data in its first year of operation than any carrier ever world-wide.[66] According to Morgan Stanley, monthly data traffic in India per user has jumped 570% in the two years since Jio launched.[67]

[61] West, "Jumping from Fixed Internet to Mobile."
[62] "The Mobile Revolution."
[63] "India."
[64] Bhattacharya, "Cheap Data Is Killing Broadband in India."
[65] "India."
[66] "Two Years Ago, India Lacked Fast, Cheap Internet -- One Billionaire Changed All That."
[67] "Mukesh Ambani: Why India Inc's Biggest Play next Year Will Be by Mukesh Ambani, from Connectivity, Content to Commerce."

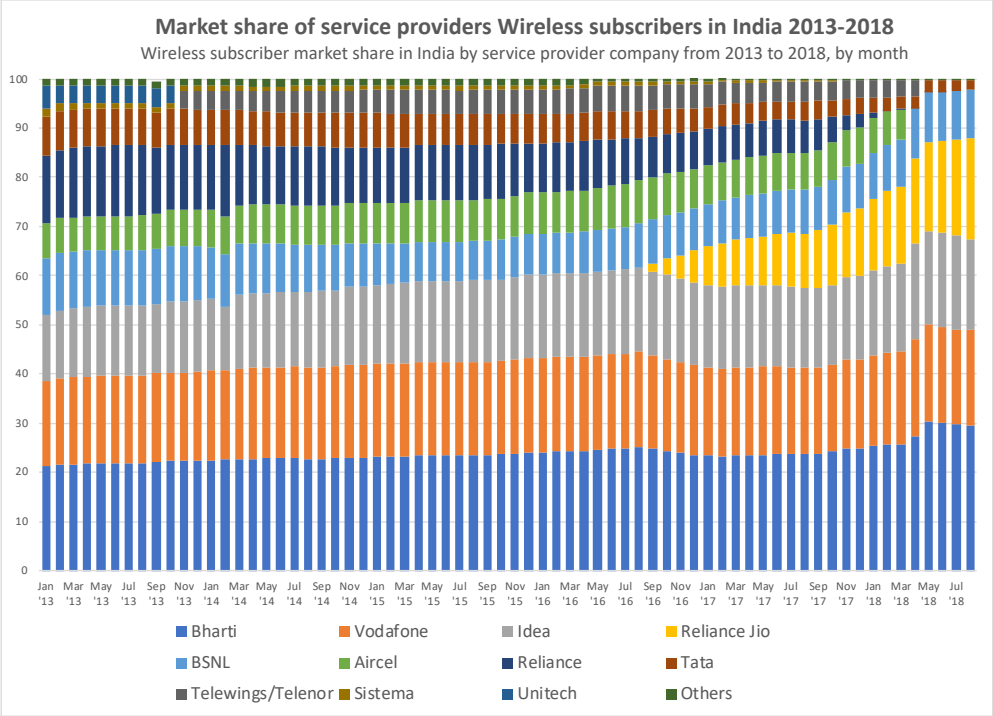


Figure 6: Since its entrance in 2016, Reliance Jio, in yellow, has captured a significant share of the telecom market by offering data at extremely cheap rates (Source: TRAI).

One of the Digital Deciders

From a more geopolitical perspective, India's digitization efforts are being courted by two sides representing opposite ends of the spectrum when it comes to internet governance. India has been listed among the world's "Digital Deciders," a group of countries that has yet to decide if it will end up adopting a global and open approach to the internet or a more sovereign and controlled one.[68] For rising powers like China, which has made its decision unequivocal, this group of nations are ripe for influence. Chinese companies investing heavily in building the technological infrastructure of the 21st century and training many of their counterparts on how to use it. Between 2017 and 2018, Freedom House published that China had installed internet and mobile networking equipment in India and also hosted local media elites

[68] "Authoritarians Are Exporting Surveillance Tech, And With It Their Vision for the Internet."

and government officials from India for weeks-long seminars on new media and information management.[69]

India has also received a big push from the West. The U.S. State Department has been vocal in encouraging India to spread its digital success story as a counter to China, which has been promoting its vision worldwide. "China is using digital systems to create an oppressive surveillance State, but India can show the world how to use digital platforms and create an 'opportunity state'," one US diplomat recently wrote in an op-ed in the *Hindustan Times*.[70] To some extent, India has shown interest in promoting itself as a model for how other countries can exploit the internet as an engine for economic growth.[71] In other areas of internet policy, India has appeared to strike a balance between the US and China, instead opting for a more European approach. For example, India has been fairly strong in areas concerning privacy and data breaches; in 2017, the Supreme Court stated that privacy is a fundamental right under the Constitution and a year later, a draft privacy bill "Personal Data Protection Bill, 2018" is up for consideration.[72]

These factors are important to keep in mind as many have argued that recent years have ushered in an era of competing ideas for how the internet should be treated at a national and even subnational level. The utilization of digital networks for geopolitical purposes is most likely just getting started, which makes countries like India important to watch. As Google's former CEO Eric Schmidt said recently, "I think the most likely scenario now is not a splintering, but rather a bifurcation into a Chinese-led internet and a non-Chinese internet led by America."[73] Given the influence it has international, regionally, and among

[69] Shahbaz, "Freedom on the Net 2018: The Rise of Digital Authoritarianism."
[70] "Spreading Its Digital Success Story Could Be India's Unique Contribution to the World."
[71] Yadunath, "Transforming India through Digital Innovation."
[72] "All You Wanted to Know about Personal Data Protection Bill 2018 - The Hindu BusinessLine."
[73] "Eric Schmidt, Ex-Google CEO, Predicts Internet Bifurcation with China."

internet governance circles, which direction India ends up moving towards will impact how other countries deal with technology's political and social challenges in the years ahead.

Internet Shutdowns in India

India now leads the world in the number of state-directed internet shutdowns. Between January 2012 and January 2019, there have been 278 Internet shutdowns, according to data provided by Access Now.[74] This number started to escalate considerably in 2016, going from 30 to 127 as of early December 2018. There is no public information made available by either the government or local ISPs that confirm these shutdowns; instead, numbers are gathered using media reports, local NGOs that monitor shutdowns, and other anecdotal data sources. As a reflection of how internet shutdowns have evolved from there early days during the Arab Awakening, when the entire nation was effectively taken offline, shutdowns in India are highly localized and conducted by the nation's state governments. These "micro-shutdowns" are almost exclusively aimed at turning off mobile networks.

Only a handful of studies have taken a subnational approach to analyzing shutdowns anywhere in the world, much less in India. Those that have been done have focused their research on the adverse economic effects. This includes a report from the Brookings Institution, which found that shutdowns in India over a year-long period cost USD $968 million.[75] Using the same methodology across a different time period, Indian think-tank ICRIER estimated that between 2012 and 2017 shutdowns in India cost as much as USD $3.04 billion.[76] A report prepared by Deloitte for Facebook calculated that

[74] "Internet Shutdowns in India."
[75] West, "Internet Shutdowns Cost Countries $2.4 Billion Last Year."
[76] Kathuria et al., "The Anatomy of an Internet Blackout."

an average low-connectivity country like India stands to lose at least 0.4% of its daily GDP for each day all internet services are shut down.[77]

So far, India appears more than willing to absorb such costs if it helps quell social unrest, but even this assumption has been challenged. In early 2019, Jan Rydzak released findings showing that in the short-term, shutdowns are ineffective in quelling unrest and in the long-term, they are too expensive to justify.[78] His report makes note of the fact that calculations on costs do not encompass less palpable economic damage and the aftermath of violent collective action incited by shutdowns. This is a high price to pay for a tactic that appears to be ineffective as a weapon against collective action. A portion of Rydzak's paper examines the role of political parties at the state level and their proclivity towards shutdowns. Recognizing that across India, BJP's rise to power coincided with increasing preference toward shutdowns as a means of quelling collective action, Jan asks whether dominance of BJP in state parliaments could help create favorable institutional environment for shutdowns. It calls for future research focusing on the institutional drivers of information control amid therefore examine political affiliations among these actors.

Legally, these orders are typically invoked under Section 144 of the Code of Criminal Procedure (CrPC), a provision from 1973 that grants Indian state governments the ability to "issue orders for immediate remedy in urgent cases of nuisance or apprehended danger," including "temporary measures to maintain public tranquility."[79] In 2017, the Indian government added a new section to The Telegraph Act of 1855 called "Temporary Suspension of Telecom Service (Public Emergency or Public Safety) Rules," authorizing national or state-level officials to issue temporary suspension orders to shut down

[77] "The Economic Impact of Disruptions to Internet Connectivity: A Report for Facebook."
[78] Rydzak, "Of Blackouts and Bandhs."
[79] Nayak, "The Anatomy of Internet Shutdowns – II (Gujarat & Constitutional Questions)."

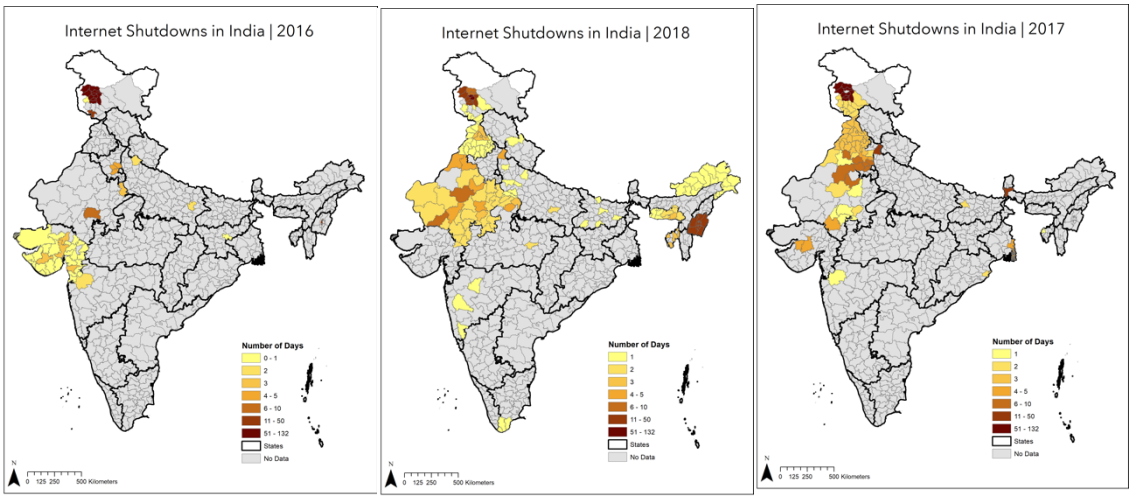
telecommunications services in times of public emergency or threats to public safety.[80] In practice, shutdowns are usually ordered by the District Magistrate (DM) or a committee chaired by the state's governor. They are usually targeted at a few districts in the state, especially ones with the most population density. If action is being taken by several districts, the decision is sometimes taken in a coordination several states under the chairmanship of one governor.[81]

Justifications for the measures are not always given, however, it is often reported that they are meant to quell riots and protests. DMs have argued that "implementing shutdowns under Section 144 is less cumbersome than other forms of addressing protest, including police engagement."[82] But a great deal of them are intended to stop the spread of misinformation on social media platforms, often blamed for inciting violence. For example, in the state of Assam, when a video showing a child being kidnapped by a masked motorcyclist went viral on WhatsApp, along with an audio message warning that 200 "Hindi-speaking" child kidnappers were entering the state, mobs killed at least two people and physically assaulted several others who were mistaken for kidnappers.[83] The video ended up being a public-service announcement against child kidnapping in Pakistan. In response, shutdowns were ordered. In July 2017, internet services were disrupted in a district in West Bengal after clashes broke out allegedly resulting from a controversial Facebook post.[84] In Tamil Nadu, the internet came down during protests against a copper smelting plant expansion.[85] There are dozens of additional examples that closely resemble these two events.

[80] "Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 | Department of Telecommunications | Ministry of Communication | Government of India."
[81] "Mobile Internet to Remain Suspended in Punjab, Haryana; Likely to Resume in Chandigarh Tonight."
[82] Rydzak, "Of Blackouts and Bandhs."
[83] Heanue, "WhatsApp Video of Fake Kidnapping Sparks Hysteria in India as Mob Beats Men to Death."
[84] "West Bengal Communal Violence."
[85] "3 Tamil Nadu Districts Shut Both Broadband and Mobile Internet Down."

Conor L. Sanchez
Master of Law and Diplomacy
The Fletcher School of Law and Diplomacy
April 2019

Duration of Internet Shutdowns by Days



Internet Shutdowns by No. of Occurrences

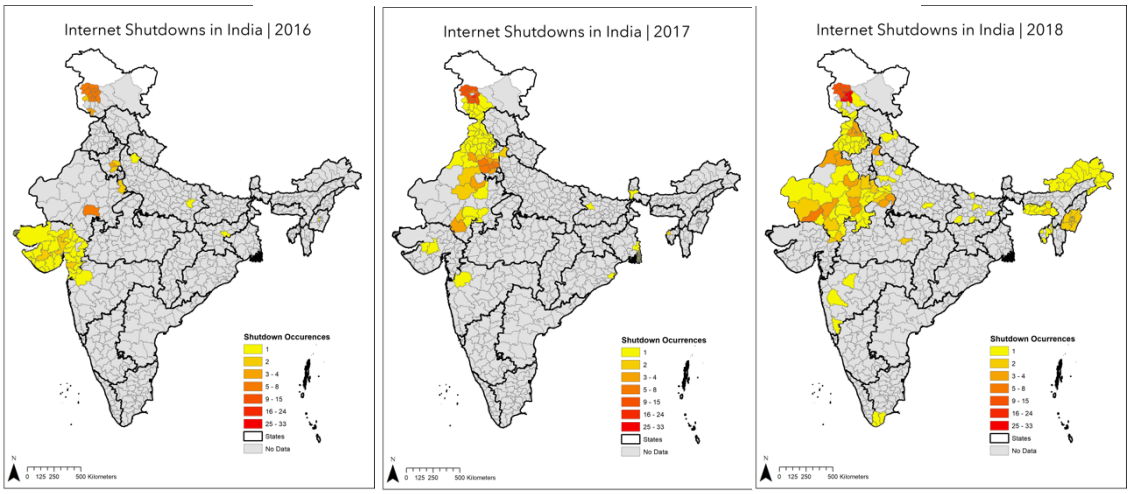


Figure 7: The above maps offer a more detailed glimpse into the growth and severity of internet shutdowns across India at the district level. The top row shows where shutdowns have been most severe in terms of duration. The bottom rows shows where they have been most severe by number of occurrences (Source: Access Now).

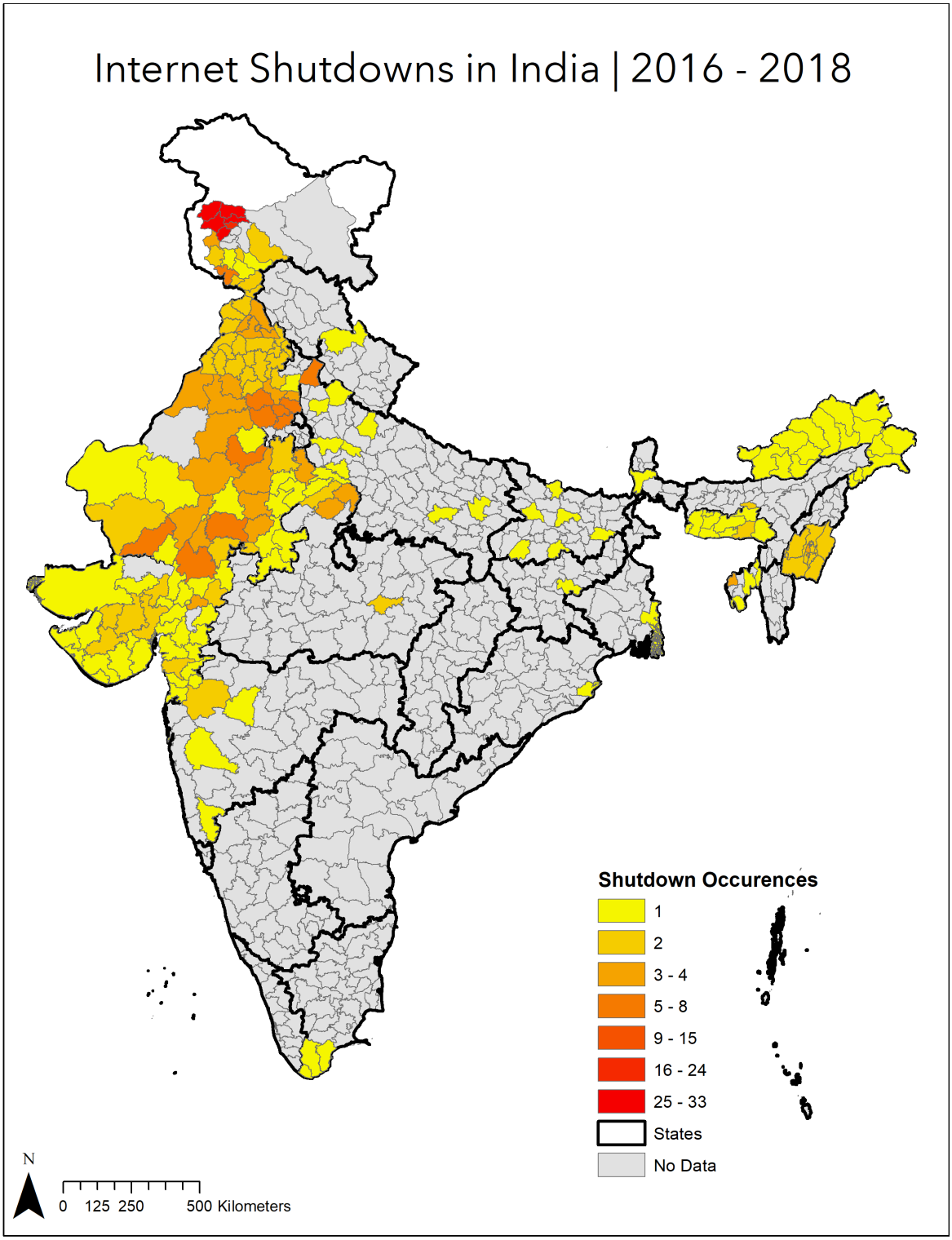


Figure 8: Internet shutdowns by number of occurrences in India at the district level during the years 2016-2018.

An interesting dynamic that is evident from numerous media reports is the apparent hierarchy that exists in the order in which ISPs suspend their services in the event of a shutdown. Unsurprisingly, the state-owned BSNL, whose clients include government officials, the police, and the army, is generally the last to go. Airtel, Aircel, Vodafone and Jio shut down their operations almost immediately.[86] It is also speculated that BSNL has some internal due diligence to complete before it disables its network.[87] Some business owners have actually tried switching to BSNL as a risk mitigation strategy. Yarikul Software Solutions, a software development company based in Srinagar, is quoted in an article saying, "In an event of an outage/ban on internet services, we are unable to work properly. In order to tackle these situations, we had to opt for more expensive alternatives like lease lines and BSNL broadband connections, which are not affected by the ban. But these connections do not allow our tiny staff to be flexible and work from home as per the need. Many a times we find it difficult to communicate with clients who are not in our time zone."[88]

It is important to note that the vast majority of Indians have not experienced an internet shutdown. Still, millions of people have been affected by its micro-shutdowns. Of the country's 36 states and union territories, 23 experienced a shutdown between 2016 and 2018. Of those, 6 have experienced more than 5 occurrences. The leader in that time period, by a considerable margin, was Jammu and Kashmir with 111 shutdowns. The duration of most shutdowns is one day, however, a few have last months at a time, including in Darjeeling in the east.[89]

To assess the institutional drivers in the rise of shutdowns in India, I broke down the number of reported shutdowns by state and also researched which political party held governorship in the state.

[86] "ISPs in Kashmir Grappling with Mounting Losses amid Recurrent Shutdowns."
[87] "#NAMAPolicy."
[88] "ISPs in Kashmir Grappling with Mounting Losses amid Recurrent Shutdowns."
[89] "Darjeeling's 100–Day Internet Shutdown: Every Town Had Its Jio Dara."

Although there is no public data on the party affiliations of DMs, these positions are appointed by State Governors whose party affiliations are publicly known. Because Jammu and Kashmir is a region known for long-term civil strife and, therefore, a frequent outlier in national datasets, I sometimes left it out to gain better visibility into the trends unfolding in other Indian states and UTs. Finally, in order to get an even more localized perspective on the shutdowns, I broke down the data I received from Access Now even further by dividing the occurrences as well as their duration in days by the districts in which they occurred. This analysis allowed me to develop a risk map that more accurately exhibits which regions have been prone to experiencing internet shutdowns over the last three-year period.

No. of Internet Shutdowns in India by State and Union Territory:

State	2016	2017	2018	TOTAL
Jammu and Kashmir	11	28	72	111
Rajasthan	5	12	14	31
Haryana	4	9	0	13
Uttar Pradesh	2	3	7	12
Maharashtra	1	1	8	10
Bihar	2	3	5	10
Gujarat	3	1	1	5
Punjab	0	1	3	4
Manipur	1	0	3	4
Meghalaya	0	0	4	4
Tripura	0	2	2	4
Odisha	0	2	1	3
West Bengal	0	2	0	2
Assam	0	0	2	2
Uttarakhand	0	0	2	2
Arunachal Pradesh	0	1	1	2
Nagaland	0	2	0	2
Tamil Nadu	0	0	1	1
Madhya Pradesh	0	0	1	1
Telangana	0	1	0	1
Jharkhand	1	0	0	1

NCT of Delhi	0	0	0	1
Chandigarh	0	1	0	1
Himachal Pradesh	0	0	0	0
Andhra Pradesh	0	0	0	0
Karnataka	0	0	0	0
Goa	0	0	0	0
Kerala	0	0	0	0
Puducherry	0	0	0	0
Mizoram	0	0	0	0
Sikkim	0	0	0	0
Chhattisgarh	0	0	0	0
Andaman and Nicobar Islands	0	0	0	0
Dadra and Nagar Haveli	0	0	0	0
Daman and Diu	0	0	0	0
Lakshadweep	0	0	0	0

KEY INSIGHTS

Based on my research, a few observations are worth mentioning. First, it is clear that exogenous political and economic factors are serving as the necessary underlying drivers of social unrest in India – not the internet. Second, many of these underlying drivers are amplified when the government decides to shut down the internet. Social unrest is the result of grievances or social discord, and if anything, these issues are exacerbated when government authorities cut off connectivity. Finally, I identify a set of criteria and potential proxies that made the regions affected by state-directed network disruptions between 2016 and 2018 within India favorable environments for such drastic measures to control information flows. These include:

- A rapid rise in new internet users
    - Proxy: International Telecommunication Union, World Telecommunication/ICT Development Report and database

- A history of media censorship
    - Proxy: Freedom House rankings on Freedom of the Press or Freedom of the Net
- Low levels of digital literacy
    - Proxy: Traditional literacy rates
- A rise in communal incidents and protests
    - Proxy: Armed Conflict Location & Event Data Project (ACLED) data on protests and riots
- Ethno-nationalist leadership
    - Proxy: Seats held by political parties that embrace ethno-nationalism
- A lack of public trust in criminal justice systems and a perceived lack of law enforcement
    - Proxy: Global survey by Gallup News on public's confidence in judicial systems and courts
- A weak law enforcement regime
    - Proxy: Rule of law score according to the World Justice Project (WJP)
- Sympathetic to the idea of greater sovereign control of the internet
    - Proxy: New America's rankings on a country's likelihood to favor a sovereign and controlled internet

In the following pages, I unpack how these country-level factors helped cultivate breeding grounds for internet shutdowns across various states in India. On their own, these trends do not explain the use of internet shutdowns, but taken collectively and concurrently, they exhibit why the environment was ripe for shutdowns and also why a similar set of vulnerabilities in any other country would raise the likelihood of their government acting on their more flawed inclinations when it comes to the internet. This could come

in the form of internet shutdowns but could also manifest in a number of different actions that all fit within the "techno-nationalist toolbox." In this toolbox are such interventions as data localization laws, strict content moderation policies, platform blocking, throttling, and other measures that impose strong sovereignty claims over the internet within a nation's boundaries.

A rapid rise in the number of internet users and low levels of digital literacy

As described earlier, India's digitalization efforts as well as Jio's entrance into the telecom market has rapidly grown the number of internet users across India, many whom have low levels of digital literacy. They also appear to be the first to be cut off. Leveraging the accessibility of mobile devices has been an effective way to bring millions online in India. However, it has also created a more segmented market that allows the state to efficiently target specific populations in circumstances that challenge their ability to maintain control. Several news sources have described how when mobile networks are shut down, especially Jammu and Kashmir, authorities often suspend pay-as-you-go mobile data plans, which disproportionally affects low-income residents who cannot afford subscriptions.[90] It appears the growth in internet usage has created a hierarchy in the application of internet disruptions, giving authorities the ability to shut down the internet without it affecting themselves, businesses, or higher-income residents who can afford subscription plans. Having mitigated with the potential economic pains of a shutdown, authorities would then consider the legal environment; and in a country where moderate censorship has existed, the use of internet shutdowns becomes far more feasible.

[90] "Freedom on the Net 2017."

A history of censorship

Although India is a democracy, there is a history of moderate censorship in its 72 years since independence. For example, in 2000, the Information Technology Act allowed authorities to search the homes of cyber café owners and internet users without warrants. It also allowed the government to block access to sites considered a danger to "public order, the integrity and security of the nation and relations with other countries."[91] Therefore, the recent enactment of the "Temporary Suspension of Telecom Service (Public Emergency or Public Safety) Rules," which authorized national or state-level officials to issue temporary suspension orders to shut down telecommunications services in times of public emergency or threats to public safety, had some precedent.

A rise in communal incidents and protests as well as ethno-nationalist leadership

India has a long history of ethnic fault lines, but recently the divides between Hindus and Muslims, and inter-caste, have worsened. The Armed Conflict Location & Event Data Project (ACLED), an organization that collects and analyses data on political violence and protest, reports there has been a spike in communal violence since 2014 (See Figure 7).[92] This corroborates with other research that ranks India as the 4th worst country for religious violence.[93] Much of this increase in violence has been attributed to the rise of Prime Minister Narendra Modi's Bharatiya Janata Party (BJP), which embraces the Hindu nationalist Hindutva ideology. This is ongoing as Modi's use of nationalism to consolidate his support ahead of the

[91] Warf, "Geographies of Global Internet Censorship."
[92] Castro, "The Complexity of Disorder in India."
[93] NW, Washington, and Inquiries, "Global Restrictions on Religion Rise Modestly in 2015, Reversing Downward Trend | Pew Research Center."

2019 election has been said to be a high risk of localized instability by encouraging the more radicalized elements of society that target minorities.[94]

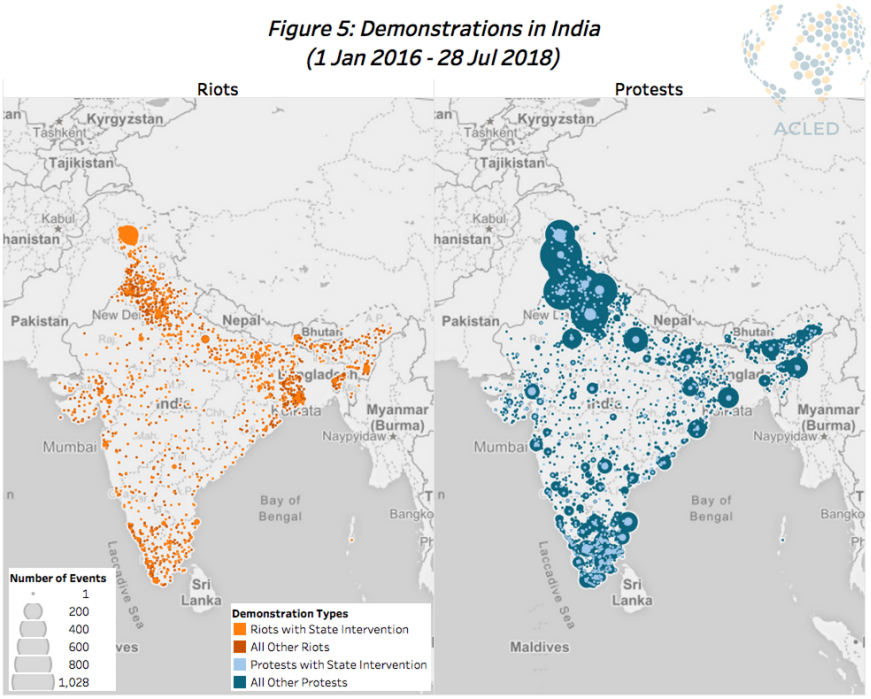


Figure 9: The most common form of political violence and protests in India come in the form of demonstrations, which make up 90 percent of all reported events in India. Since 2014, they have been on the rise (Source: ACLED).

As mentioned in prior sections, BJP's rise to power has also coincided with an increasing preference toward using internet shutdowns as a means of quelling unrest. Previous research had asked whether dominance of BJP in state parliaments helped create favorable institutional environment for shutdowns. Given that those responsible for ordering the shutdowns, DMs, are appointed by the state governor, I instead looked at the political affiliation of governors during the time of shutdowns in each state. I found that the vast majority of shutdowns in the years 2016, 2017, and 2018 have been reported in states governed by BJP, suggesting a link between the growing trend in shutdowns and BJP's rise to power.

[94] "Risk 9."

It could be, as ACLED asserts,[95] that the complexity of violence and disorder in India is making it more difficult for individual state governments to address so many interconnected and distinct issues simultaneously. The dilemma strikes at the heart of the difficult balance democratic governments have to weigh between upholding freedoms expression and ensuring safety in society. In the absence of effective institutional tools to deal with social unrest, authorities who are emboldened by a nationalist government have decided internet shutdowns are the only tool they possess to address massive collective action.

A lack of trust in the country's criminal justice systems and a perceived lack of law enforcement:

Over the last few years, India has experienced a spate in the number of public lynchings performed by locals taking law into their own hands. Especially 2018, there was a high number of lynchings due to misinformation campaigns and rumors proliferated on social media platforms regarding child. The increasing number of events involving vigilante violence against presumed criminals is indicative of the perceived lack of law enforcement and lack of trust in India's criminal justice systems. Here, again, the rise of Hindu nationalism has been said to encourage vigilantism, typically directed towards Muslims and Dalits. The majority of these have been reported post-May 2014 and in states governed by BJP.[96] If the justice system and law enforcement is not trusted, this further complicates efforts by the state to quell situations, which raises the likelihood of it opting for more drastic measures.

[95] Castro, "The Complexity of Disorder in India."
[96] Castro.

A weak law enforcement regime

Over the last few years, India has experienced a slide in the rule of law, according to the World Justice Project (WJP).[97] In 2019, it ranked 68th out of 126 countries, representing a decline in three positions for overall rule of law performance (see Figure 8). Out of the various indicators measured, its slide in check on government powers was especially concerning. A declining environment for the rule of law raises the risk of a country experiencing an internet shutdown because it means the government is more likely to engage in behavior that violates human rights, including the freedom of expression.

The factors that determine whether or not shutdowns transform into habits rely on the institutional environments that can either act to restrain such temptations or enable them. The fact that the temptation to curb information flows to quell or preempt social unrest is not relegated to developing or emerging economies may prove instructive on this point. A few months after the 2011 internet shutdown in Egypt, the United States experienced a disruption in San Francisco, when local authorities shut down cell services in anticipation of a protest in the city's subway system.[98] The response from civil society was extremely strong; two years after the shutdown, the State of California passed a law to prevent wireless communication services from being shut down,[99] while also affirming legitimate concerns for public safety by providing for the disruption of communications service without a court order if an extreme emergency exists.

This also might explain why countries that use internet shutdowns most also tend to be Break Out countries identified in Digital Planet's DEI. These countries were marked by low absolute levels of digital advancement, but high paces of growth. While performing well in their overall digital progress, they are

[97] "WJP Rule of Law Index 2019."
[98] Kravets, "San Francisco Subway Shuts Cell Service to Foil Protest; Legal Debate Ignites."
[99] "Bill in Response to BART Wireless Service Shutdown Signed into Law."

typically held back by poor institutional quality and have been encouraged to invest more in institutional improvements to sustain their progress and make the next big leap forward.[100]

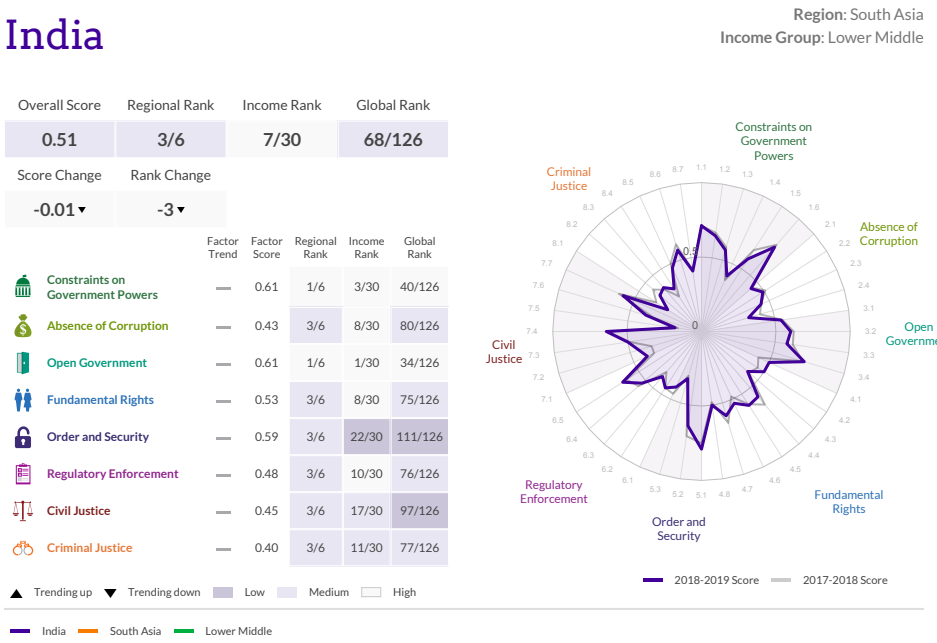


Figure 10: In 2019, it ranked 68th out of 126 countries, representing a decline in three positions for overall rule of law performance (Source: WJP).

Sympathetic to the idea of greater sovereign control of the internet

Finally, the broader geopolitical dynamics cannot be ignored. Countries that fall into the digital deciders category of not having quite settled on whether they will embrace an open internet or a more controlled internet, are at risk of internet shutdowns. Chinese companies are building the technological infrastructure of the 21st century, and Chinese officials are training many of their counterparts on how to use it. Between 2017 and 2018, Freedom House published that China had installed internet and mobile

[100] Chakravorti and Chaturvedi, "Digital Planet 2017: How Competitiveness and Trust in Digital Economies Vary Across the World."

networking equipment in India.[101] Local media elites and government officials from India have been hosted in China for weeks-long seminars on new media or information management, suggesting a closer relationship over internet governance.

NEXT STEPS

This report lays the groundwork for future empirical research that could begin to find a causal link between some of the country-level vulnerabilities I have outlined (and identified proxies for) and state-directed internet shutdowns, not just within the context of India, but other countries as well. As my research has shown, there are no shortage of cases from which to choose. These insights can also help in the development of a global scorecard that would hold governments accountable for their actions and hopefully encourage them to invest in strengthening their institutions and dissuade them from giving in to the temptations of using the techno-nationalist toolbox. The systematic use of ratings and rankings in making countries think twice about how their actions might impact their global reputation has become a powerful tool in bringing about change.[102] Finally, this insights elucidated in this paper can also be used by tech industry actors who can begin to build predictive models on shutdowns or other state interventions into the digital economy that would be extremely valuable to various industries, including investors.

CONCLUSION

Of the nearly 3.7 billion people that have access to the internet today, 42 percent of them live under governments that disconnected internet or mobile networks in 2018.[103] The reasons behind them are

[101] Shahbaz, "Freedom on the Net 2018: The Rise of Digital Authoritarianism."
[102] Kelley, *Scorecard Diplomacy: Grading States to Influence Their Reputation and Behavior*.
[103] Shahbaz, "Freedom on the Net 2018: The Rise of Digital Authoritarianism."

diverse, but most governments claim that the internet is fueling social unrest despite the fact that there is little evidence suggesting that higher levels of internet access leads to increased levels of social unrest.[104] At most, studies show that social media serves as a useful but not sufficient tool for protest. What does seem plausible, however, is that higher levels of internet access leads to increased levels of state attempts to control online information flows given a certain set of country-level factors. Contrary to the notion that the internet's decentralized nature makes it resistant to those instincts, governments around the world are showing they have learned how to hijack its control valves whenever they see fit and without completely shooting themselves in the foot. Based on data collected on shutdowns in India in the years 2016-2018, this report has identified five key political vulnerabilities that help explain the high occurrence of shutdowns in India during this time period. But at a broader level, they should also serve as a set of vulnerabilities that, without proper restraints, make governments more likely to act on their more flawed inclinations. They demonstrate why fostering better institutions and a stronger civil society can help develop a more mature digital ecosystem, one that provides assurance to all stakeholders that the internet can be trusted and relied upon, thereby sustaining the economic benefits it portends. As countries around the world are leaping ahead to exploit the rewards of bringing more people online, the politics of connectivity is becoming a major component of ensuring those benefits endure for the long-haul. Indeed, the era in which nation-states search for the appropriate scope of state authority in managing information within its sovereign borders is not going way; in many ways, it has only just begun.

[104] Madrigal, "India's Lynching Epidemic and the Problem With Blaming Tech."

Conor L. Sanchez
Master of Law and Diplomacy
The Fletcher School of Law and Diplomacy
April 2019

APPENDIX A: State-Directed Internet Shutdowns by Country and Regime Type, 2011-2018

Country	2011	2012	2013	2014	2015	2016	2017	2018	Total
India	0	3	5	7	13	30	69	128	255
Dem. Republic of Congo	0	0	0	0	1	1	2	2	6
Chad	0	0	0	0	0	1	0	3	4
Ethiopia	0	0	0	0	0	3	2	6	11
Sierra Leone	0	0	0	0	0	0	0	1	1
Cote d'Ivoire	0	0	0	0	0	0	0	1	1
Mali	0	0	0	0	0	1	0	2	3
Nigeria	0	0	0	0	0	0	0	2	2
Pakistan	0	0	0	0	0	8	11	12	31
Philippines	0	0	0	0	1	0	1	2	4
South Korea	0	0	0	0	0	0	0	1	1
Bangladesh	0	0	0	0	1	1	0	3	5
Sri Lanka	0	0	0	0	0	0	0	1	1
Indonesia	0	0	0	0	0	0	0	2	2
Iran	0	0	1	0	0	0	2	2	5
Turkey	0	0	0	0	1	5	0	2	8
Syria	0	1	0	0	0	4	3	1	9
Iraq	0	0	0	0	1	2	4	6	13
Yemen	0	0	0	0	2	0	1	2	5
Kazakhstan	0	0	0	0	0	0	0	1	1
Nicaragua	0	0	0	0	0	0	0	1	1
Russia	0	0	0	0	0	0	0	2	2
Belarus	0	0	0	0	0	0	0	0	0
Ukraine	0	0	0	0	0	0	1	0	1
Algeria	0	0	0	0	1	1	1	0	3
Egypt	1	0	0	0	0	2	1	0	4
Cameroon	0	0	0	0	0	0	2	0	2
Equatorial Guinea	0	0	0	0	0	0	2	0	2
China	0	0	0	0	0	0	1	0	1
North Korea	0	0	0	0	1	1	1	0	3
Togo	0	0	0	0	1	0	1	0	2
Morocco	0	0	0	0	0	1	1	0	2
Gambia	0	0	0	0	0	1	0	0	1

Gabon	0	0	0	0	0	1	0	0	1
Brazil	0	0	0	0	0	2	0	0	2
Bahrain	0	0	0	0	2	1	0	0	3
Montenegro	0	0	0	0	0	1	0	0	1
Saudi Arabia	0	0	0	0	0	1	0	0	1
Uganda	1	0	0	0	0	2	0	0	3
Uzbekistan	0	0	0	0	0	1	0	0	1
Vietnam	0	0	0	0	0	2	0	0	2
Zimbabwe	0	0	0	0	0	1	0	0	1
Nigeria	0	0	0	0	1	0	0	0	1
Burundi	0	0	0	0	1	0	0	0	1
Malaysia	0	0	0	0	1	0	0	0	1
Republic of Congo	0	0	0	0	1	0	0	0	1
Central Africa Republic	0	0	0	1	0	0	0	0	1
Venezuela	0	0	0	1	0	0	0	0	1
Sudan	0	0	1	0	0	0	0	0	1
Thailand	0	0	1	0	0	0	0	0	1
USA	1	0	0	0	0	0	0	0	1
Malawi	1	0	0	0	0	0	0	0	1
TOTAL	**4**	**4**	**8**	**9**	**29**	**74**	**106**	**183**	**417**

Freedom House 2018	
Regime Type	Shutdowns
Flawed Democracy	267
Authoritarian	75
Hybrid Regime	75

Conor L. Sanchez
Master of Law and Diplomacy
The Fletcher School of Law and Diplomacy
April 2019

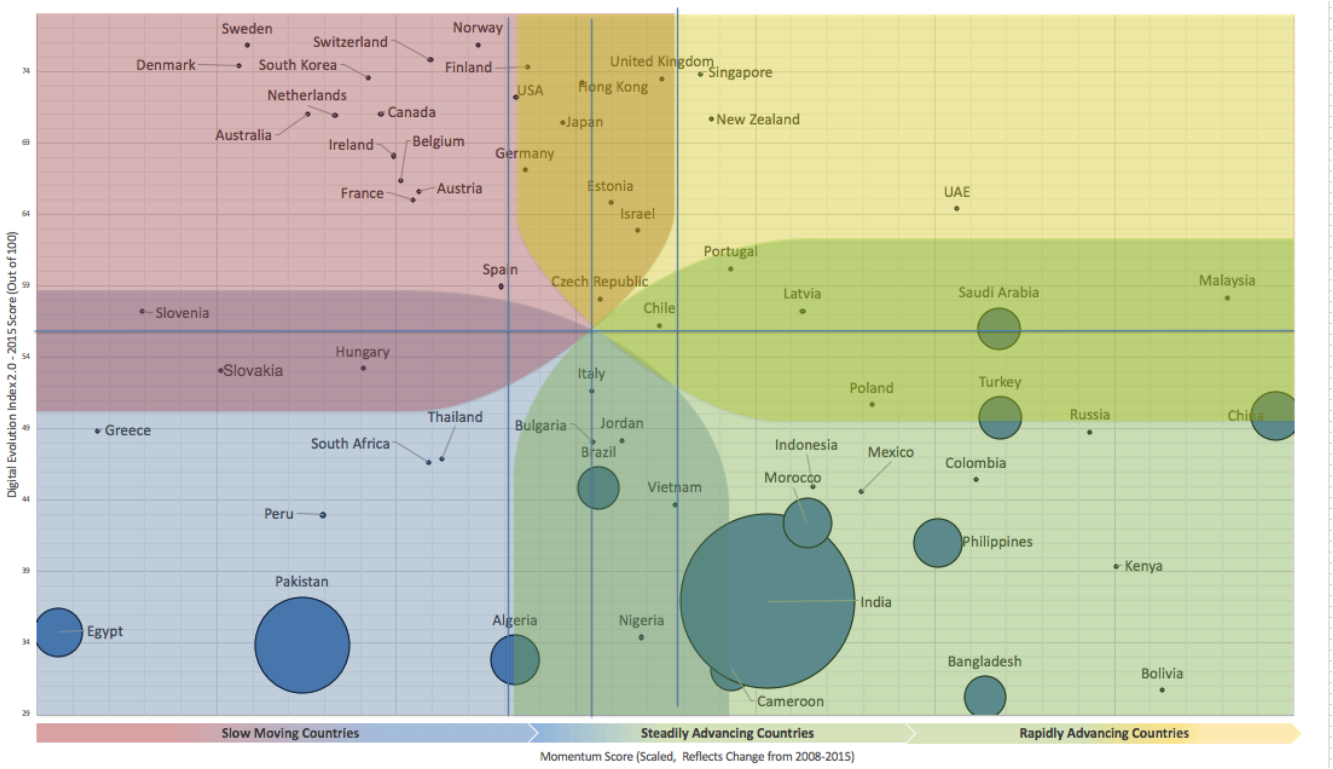
APPENDIX B: The Top 20 Digital Deciders Ranked by Influence

Country	Aggregate Influence Score
Brazil	0.91
Indonesia	0.90
Mexico	0.89
India	0.86
Singapore	0.84
Botswana	0.81
Albania	0.78
Paraguay	0.77
Serbia	0.77
Jordan	0.76
Argentina	0.75
Colombia	0.75
Armenia	0.69
Lebanon	0.69
Uruguay	0.67
South Africa	0.66
Costa Rica	0.65
Mongolia	0.63
El Salvador	0.62
Malaysia	0.62

Conor L. Sanchez
Master of Law and Diplomacy
The Fletcher School of Law and Diplomacy
April 2019

APPENDIX C: Digital Evolution Index 2017 and Internet Shutdowns 2016-2018

State-directed shutdowns between 2016 and 2018 were concentrated in the DEI's lower right quadrant, which included countries that were low-scoring in their states of digitalization but evolving rapidly.



References:

"3 Tamil Nadu Districts Shut Both Broadband and Mobile Internet Down." *MediaNama* (blog), May 25, 2018. https://www.medianama.com/2018/05/223-tamil-nadu-internet-shutdown/.

"A Fragmented Internet? Proceedings of The 2017 Global Digital Futures Forum." Columbia University School of International and Public Affairs (SIPA), 2017. https://sipa.columbia.edu/sites/default/files/embedded-media/5657_Digital%20Futures-Digital%20Final.pdf.

"All You Wanted to Know about Personal Data Protection Bill 2018 - The Hindu BusinessLine." Accessed April 1, 2019. https://www.thehindubusinessline.com/opinion/columns/slate/all-you-wanted-to-know-about/article24617362.ece.

"Anti-Shutdown Proposal." AFRINIC. Policy Archive, May 24, 2017. https://www.afrinic.net/policy/archive/anti-shutdown-02.

"Authoritarians Are Exporting Surveillance Tech, And With It Their Vision for the Internet." Council on Foreign Relations. Accessed April 1, 2019. https://www.cfr.org/blog/authoritarians-are-exporting-surveillance-tech-and-it-their-vision-internet.

Bhattacharya, Ananya. "Cheap Data Is Killing Broadband in India." Quartz India. Accessed March 31, 2019. https://qz.com/india/1512867/reliance-jios-cheap-data-is-killing-broadband-internet-in-india/.

"Bill in Response to BART Wireless Service Shutdown Signed into Law." Techwire.net, September 30, 2013. https://www.techwire.net/legislation/bill-in-response-to-bart-wireless-service-shutdown-signed-law.html.

Boas, Taylor C. "The Dictator's Dilemma? The Internet and U.S. Policy toward Cuba." *The Washington Quarterly* 23, no. 3 (September 1, 2000): 57–67. https://doi.org/10.1162/016366000561178.

Bremmer, Ian. "Democracy in Cyberspace." *Foreign Affairs*, October 21, 2010. http://www.foreignaffairs.com/articles/2010-10-21/democracy-cyberspace.

Briggs, Asa, and Peter Burke. *A Social History of the Media: From Gutenberg to the Internet*. Polity Press, 2009.

"Budget 2018: Booster for Digital India Plan; Govt to Install Wi-Fi Hotspots | Business Standard News." Accessed March 30, 2019. https://www.business-standard.com/budget/article/budget-2018-booster-for-digital-india-plan-govt-to-install-wi-fi-hotspots-118020200040_1.html.

Castro, Bhavani. "The Complexity of Disorder in India." *Acled Data* (blog), August 17, 2018. https://www.acleddata.com/2018/08/17/the-complexity-of-disorder-in-india/.

"Caught in the Net." *The Economist*, January 23, 2003. https://www.economist.com/special-report/2003/01/23/caught-in-the-net.

"Centre Ready to Use Satellites, Drones to Connect to Rural India: Ravi Shankar Prasad - The Economic Times." Accessed March 30, 2019. https://economictimes.indiatimes.com/industry/telecom/centre-ready-to-use-satellites-drones-to-connect-to-rural-india-ravi-shankar-prasad/articleshow/46115684.cms.

Chakravorti, Bhaskar, and Ravi Shankar Chaturvedi. "Digital Planet 2017: How Competitiveness and Trust in Digital Economies Vary Across the World." *The Fletcher School, Tufts University*, July 2017, 70.

Chase, James, and Michael Mulvenon. *You've Got Dissent! Chinese Dissident Use of the Internet and Beijing's Counter Strategies*. Santa Monica: Rand, 2002.

Cohen, Noham. "Egyptian Internet Blackout Pushed Protests to Streets." *The New York Times*, February 20, 2011. https://www.nytimes.com/2011/02/21/business/media/21link.html.

Cowie, Jim. "Could It Happen In Your Country?" *Dyn Blog* (blog), November 30, 2012. https://dyn.com/blog/could-it-happen-in-your-countr/.

Cunningham, Maura Elizabeth. "'The Great Firewall of China' Review: The Chinese Cyber-Padlock." *Wall Street Journal*, March 10, 2019, sec. Arts. https://www.wsj.com/articles/the-great-firewall-of-china-review-the-chinese-cyber-padlock-11552245606.

"Darjeeling's 100–Day Internet Shutdown: Every Town Had Its Jio Dara." Accessed April 14, 2019. https://www.medianama.com/2018/10/223-darjeelings-100-day-internet-shutdown-every-town-had-its-jio-dara/.

Dewey, Taylor, Juliane Kaden, Miriam Marks, Shun Matsushima, and Beijing Zhu. "The Impact of Social Media on Social Unrest in the Arab Spring." Stanford University, March 20, 2012. https://publicpolicy.stanford.edu/publications/impact-social-media-social-unrest-arab-spring.

"Digi Dhan Abhiyan: Over 25 Lakh Rural Citizens Adopt Digital Payments, Claims MeitY - News18." Accessed March 30, 2019. https://www.news18.com/news/tech/digi-dhan-abhiyan-over-25-lakh-rural-citizens-adopt-digital-payments-claims-meity-1325527.html.

"Digital India Programme | Department of Electronics & Information Technology, Government of India." Accessed March 30, 2019. https://www.digitalindia.gov.in/.

"Eric Schmidt, Ex-Google CEO, Predicts Internet Bifurcation with China." Accessed April 1, 2019. https://www.cnbc.com/2018/09/20/eric-schmidt-ex-google-ceo-predicts-internet-split-china.html.

"Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy," October 27, 2017. https://freedomhouse.org/report/freedom-net/freedom-net-2017.

Freyburg, Tina, and Lisa Garbe. "Authoritarian Practices in the Digital Age| Blocking the Bottleneck: Internet Shutdowns and Ownership at Election Times in Sub-Saharan Africa." *International Journal of Communication* 12, no. 0 (September 18, 2018): 21.

Giacomello, Giampiero. *National Governments and the Control of the Internet : A Digital Challenge*. Routledge, 2005.

Heanue, South Asia correspondent Siobhan. "WhatsApp Video of Fake Kidnapping Sparks Hysteria in India as Mob Beats Men to Death." Text. ABC News, June 12, 2018. https://www.abc.net.au/news/2018-06-12/india-whatsapp-killings-as-fake-child-kidnap-video-spreads/9861788.

Howard Rheingold. *Smart Mobs: The Next Social Revolution; Transforming Cultures and Communities in the Age of Instant Access*. Perseus, 2002.

"India." Freedom on the Net 2018, 2018. https://freedomhouse.org/report/freedom-net/2018/india.

"India's Digital Future." Morgan Stanley. Accessed March 31, 2019. https://www.morganstanley.com/ideas/digital-india.

"Internet Shutdowns in India." Accessed April 1, 2019. https://internetshutdowns.in.

"ISPs in Kashmir Grappling with Mounting Losses amid Recurrent Shutdowns." *MediaNama* (blog), September 13, 2018. https://www.medianama.com/2018/09/223-isps-in-kashmir-grappling-with-mounting-losses-amid-recurrent-shutdowns/.

Iyengar, Rishi. "India Is Planning to Give Free WiFi to More than 1,000 Villages." CNNMoney, January 30, 2017. https://money.cnn.com/2017/01/30/technology/india-free-wifi-villages/index.html.

Kathuria, Rajat, Mansi Kedia, Gangesh Varma, Kaushambi Bagchi, and Richa Sekhani. "The Anatomy of an Internet Blackout: Measuring the Economic Impact of Internet Shutdowns in India," 2018.

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

"#KeepItOn." *Access Now* (blog). Accessed September 21, 2018. https://www.accessnow.org/keepiton/.

Kelley, Judith. *Scorecard Diplomacy: Grading States to Influence Their Reputation and Behavior*. Cambridge University Press, 2017.

Kravets, David. "San Francisco Subway Shuts Cell Service to Foil Protest; Legal Debate Ignites." *Wired*, August 15, 2011. https://www.wired.com/2011/08/subway-internet-shuttering/.

Lieberman, Joseph I. "S.3480 - 111th Congress (2009-2010): Protecting Cyberspace as a National Asset Act of 2010." Webpage, December 15, 2010. https://www.congress.gov/bill/111th-congress/senate-bill/3480.

Madory, Doug. "Iraq Downs Internet To Combat Cheating...Again! | Dyn Blog." *Oracle-Dyn Research* (blog), February 26, 2017. https://dyn.com/blog/iraq-downs-internet-to-combat-cheating-again/.

Madrigal, Alexis C. "India's Lynching Epidemic and the Problem With Blaming Tech." The Atlantic, September 25, 2018. https://www.theatlantic.com/technology/archive/2018/09/whatsapp/571276/.

Meier, Patrick. "Do 'Liberation Technologies' Change the Balance of Power Between Repressive States and Civil Society?" PhD Diss, Tufts University, 2011. https://irevolution.files.wordpress.com/2011/11/meier-dissertation-final.pdf.

"Mobile Internet to Remain Suspended in Punjab, Haryana; Likely to Resume in Chandigarh Tonight." https://www.hindustantimes.com/, August 27, 2017. https://www.hindustantimes.com/punjab/mobile-internet-services-likely-to-resume-in-chandigarh-tonight/story-UGXVgdWetlRjEde4jBJQAN.html.

Morozov, Evgeny. *The Net Delusion: The Dark Side of Internet Freedom*. New York: Public Affairs, 2011.

"Mukesh Ambani: Why India Inc's Biggest Play next Year Will Be by Mukesh Ambani, from Connectivity, Content to Commerce." Accessed April 4, 2019. https://economictimes.indiatimes.com/news/company/corporate-trends/why-india-incs-biggest-play-next-year-will-be-by-mukesh-ambani-from-connectivity-content-to-commerce/articleshow/67315348.cms.

"#NAMAPolicy: How Do Internet Shutdowns Happen, and Do They Work?" *MediaNama* (blog), December 21, 2017. https://www.medianama.com/2017/12/223-namapolicy-internet-shutdowns-happen-work/.

Nayak, Nakul. "The Anatomy of Internet Shutdowns – II (Gujarat & Constitutional Questions)." *The CCG Blog* (blog), September 1, 2015. https://ccgnludelhi.wordpress.com/2015/09/01/the-anatomy-of-internet-shutdowns-ii-gujarat-constitutional-questions/.

NW, 1615 L. St, Suite 800 Washington, and DC 20036 USA202-419-4300 | Main202-419-4349 | Fax202-419-4372 | Media Inquiries. "Global Restrictions on Religion Rise Modestly in 2015, Reversing Downward Trend | Pew Research Center," April 11, 2017. https://www.pewforum.org/2017/04/11/global-restrictions-on-religion-rise-modestly-in-2015-reversing-downward-trend/.

"OHCHR | The Special Rapporteur's 2017 Report to the United Nations Human Rights Council." Accessed March 31, 2019. https://www.ohchr.org/en/issues/freedomopinion/pages/sr2017reporttohrc.aspx.

"Policy Brief: Internet Shutdowns." *Internet Society* (blog). Accessed March 28, 2019. https://www.internetsociety.org/policybriefs/internet-shutdowns.

Powers, Shawn, and Michael Jablonski. *The Real Cyber War: The Political Economy of Internet Freedom*. University of Illinois Press, 2015.

"Risk 9: Identity Politics in Southern Asia." Accessed March 31, 2019. https://www.eurasiagroup.net/live-post/risk-9-identity-politics-in-southern-asia.

Robert Keohane, and Josphe Nye. "Power and Interdependence in the Information Age." *Foreign Affairs* 77, no. 5 (October 1998): 81–94.

Rydzack, Jan. "A Human Rights-Based Approach to Network Disruptions." The Global Network Initiative (GNI), May 30, 2018. https://globalnetworkinitiative.org/gin_tnetnoc/uploads/2018/06/Disconnected-Report-Network-Disruptions.pdf.

Rydzak, Jan. "Of Blackouts and Bandhs: The Strategy and Structure of Disconnected Protest in India." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, February 7, 2019. https://papers.ssrn.com/abstract=3330413.

Schultz, George P. "Shaping American Foreign Policy: New Realities and New Ways of Thinking." *Foreign Affairs*, March 1, 1985. http://www.foreignaffairs.com/articles/1985-03-01/shaping-american-foreign-policy-new-realities-and-new-ways-thinking.

Shahbaz, Adrian. "Freedom on the Net 2018: The Rise of Digital Authoritarianism." Freedom House, 2018. https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf.

Shapiro, Andrew. *The Control Revolution: How the Internet Is Putting Individuals in Charge and Changing the World*. New York City, NY: The Century Foundation, 2000.

Shirky, Clay. "The Political Power of Social Media." *Foreign Affairs*, December 20, 2010. http://www.foreignaffairs.com/articles/2010-12-20/political-power-social-media.

Siobhan Macdermott. *The Folded Paper: Inventing Cyberdiplomacy*, 2018.

"Smartphone Market in India." Statista, 2018. http://www.statista.com/topics/4600/smartphone-market-in-india/.

"Something Is Happening in Congo-Brazzaville." *African Arguments* (blog), June 20, 2017. https://africanarguments.org/2017/06/20/something-is-happening-in-congo-brazzaville/.

Sorrel, Charlie, and Charlie Sorrel. "In India, 1,000 Villages Will Become Free Internet Hotspots." Fast Company, March 22, 2017. https://www.fastcompany.com/3067731/in-india-1000-villages-will-become-free-internet-hotspots.

"Spreading Its Digital Success Story Could Be India's Unique Contribution to the World | Opinion | Top | Hindustan Times." Accessed March 30, 2019. https://www.hindustantimes.com/opinion/spreading-its-digital-success-story-could-be-india-s-unique-contribution-to-the-world/story-eGJLLcpZF9unLrHTaLDbJK.html.

"Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 | Department of Telecommunications | Ministry of Communication | Government of India." Accessed March 31, 2019. http://dot.gov.in/circulars/temporary-suspension-telecom-services-public-emergency-or-public-safety-rules-2017.

"The Economic Impact of Disruptions to Internet Connectivity: A Report for Facebook." Deloitte, 2016. https://globalnetworkinitiative.org/wp-content/uploads/2016/10/GNI-The-Economic-Impact-of-Disruptions-to-Internet-Connectivity.pdf.

"The Indian Telecom Services Performance Indicators July – September, 2018." Telecom Regulatory Authority of India, January 8, 2019. https://main.trai.gov.in/sites/default/files/PIR08012019.pdf.

"The Internet Perceives Censorship as Damage and Routes Around It." NDItech.org, February 7, 2011. https://www.nditech.org/internet-perceives-censorship-damage-and-routes-around-it.

"The Mobile Revolution: How Mobile Technologies Drive a Trillion-Dollar Impact." https://www.bcg.com. Accessed March 31, 2019. https://www.bcg.com/publications/2015/telecommunications-technology-industries-the-mobile-revolution.aspx.

"Two Years Ago, India Lacked Fast, Cheap Internet -- One Billionaire Changed All That." *Dow Jones Institutional News; New York*. September 5, 2018. http://search.proquest.com/docview/2099772001/citation/59CCE366D7974A13PQ/1.

Vargas-Leon, P. *Tracking Internet Shutdown Practices: Democracies and Hybrid Regimes In: Musiani F., Cogburn D.L., DeNardis L., Levinson N.S. (Eds) The Turn to Infrastructure in Internet Governance. Information Technology and Global Governance.* New York: Palgrave Macmillan, 2016.

"Walmart Confirms $16B Flipkart Investment, Giving It 77% in India's e-Commerce Leader." *TechCrunch* (blog). Accessed March 31, 2019. http://social.techcrunch.com/2018/05/09/walmart-confirms-16b-flipkart-investment-giving-it-77-in-indias-e-commerce-leader/.

Warf, Barney. "Geographies of Global Internet Censorship." *GeoJournal* 76, no. 1 (February 1, 2011): 1–23. https://doi.org/10.1007/s10708-010-9393-3.

"West Bengal Communal Violence: Internet Services Disrupted in Baduria Following Clashes in North 24 Parganas." *The Financial Express* (blog), July 5, 2017. https://www.financialexpress.com/india-news/west-bengal-communal-violence-baduria-internet-services-disrupted-mamata-banerjee-facebook-post-north-24-parganas-protest/749676/.

West, Darrell M. "Internet Shutdowns Cost Countries $2.4 Billion Last Year." *Center for Technological Innovation at Brookings, Washington, DC*, 2016.

West, Joshua Bleiberg and Darrell M. "Jumping from Fixed Internet to Mobile: India Is Going Wireless." *Brookings* (blog), November 30, 2001. https://www.brookings.edu/blog/techtank/2015/03/18/jumping-from-fixed-internet-to-mobile-india-is-going-wireless/.

"WJP Rule of Law Index 2019." World Justice Project. Accessed April 5, 2019. https://worldjusticeproject.org/our-work/research-and-data/wjp-rule-law-index-2019.

Yadunath, Darshan. "Transforming India through Digital Innovation." Text. Information and Communications for Development, March 28, 2016. http://blogs.worldbank.org/ic4d/transforming-india-through-digital-innovation.