

JAN RYDZAK FOR THE GLOBAL NETWORK INITIATIVE

DISCONNECTED:

**A HUMAN RIGHTS-BASED APPROACH
TO NETWORK DISRUPTIONS**



GLOBAL
NETWORK
INITIATIVE



CONTENTS

ABOUT THE AUTHOR	3
ACKNOWLEDGMENTS	
ATTRIBUTION	
EXECUTIVE SUMMARY	4
INTRODUCTION	5
THE DYNAMICS OF NETWORK DISRUPTIONS	6
What is a network disruption?	6
When do network disruptions occur?	8
How do network disruptions occur?	10
The challenges of resisting shutdown orders	10
THE IMPACTS OF NETWORK DISRUPTIONS	11
Civil and Political Rights	11
— Freedom of expression, association, and assembly	11
— Right to equality and digital discrimination	12
— Freedom of religious belief	13
— Right to life, bodily integrity, and security of persons	13
Economic, Social, and Cultural Rights	15
— Economic rights	15
— Right to mental and physical health	16
— Right to education	17
— Right to take part in cultural life and benefit from scientific progress	17
Humanitarian Impacts	18
RECOMMENDATIONS: AN INTEGRATED APPROACH	19
Broaden the scope of human rights impact assessments	19
Improve and expand data collection efforts	20
Support responsible partnerships to expand connectivity	21
Conduct case studies	22
Engage directly with government actors and support training	22
CONCLUSION	23
ANNEX: HOW ARE DISRUPTIONS TYPICALLY EXECUTED?	24
Shutdown orders	24
Technical aspects of large-scale shutdowns	25
Sabotage of infrastructure and cable cuts	26
Bandwidth throttling	26
EXTERNAL RESOURCES	27



ABOUT THE AUTHOR

Jan Rydzak is a PhD candidate in Government & Public Policy at the University of Arizona and a former Google Policy fellow for the Global Network Initiative. His research covers new, technologically enabled means of repression and protest, as well as the uses of technology and innovation in protecting human rights, promoting sustainable development, and improving humanitarian action. His dissertation revolves around the relationship between network shutdowns and mass protest. He has also worked with the European Commission and the UN Special Rapporteur for Indigenous Rights, among others. He has a background in Modern Languages and a sustained interest in exploring their frontiers.

ACKNOWLEDGMENTS

The author would like to thank Kath Cummins, Judith Lichtenberg, Jason Pielemeier, Chris Sheehy, and David Sullivan for their consistent and unflinching support throughout and after the Google Policy Fellowship. David Sullivan and Jason Pielemeier in particular improved this report greatly with invaluable contributions, volunteering their time, effort, and attention to produce a final product vastly superior to past incarnations. The participants and organizers of the 2016 Summer Doctoral Programme at the Oxford Internet Institute provided intellectual rocket fuel and inspiration. Arturo Filastò and Doug Madory kindly provided vital guidance on the technical appendix. Thank you to all who agreed to contribute to this project through interviews and stimulating discussions. Prof. Alex Braithwaite and Prof. John P. Willerton were instrumental in bringing the Fellowship to fruition, as were Angela Hackett, Ian Wilson, Kelly Huff, Christine Wong, and Michael Matthews, all Wildcats at the University of Arizona. Steven Garza from Google helped me navigate difficult waters. Finally, bottomless thanks to my family and to Hoa Nguyen for the never-ending motivation and the daily reminder that I'm "almost there."

ATTRIBUTION

This report comes out of conversations and interviews that took place with GNI staff and members, as well as members of the Telecom Industry Dialogue (which has since become part of GNI), during the author's Google Policy Fellowship. While informed by those discussions, the content, analysis, and recommendations of this report are those of the author alone.



EXECUTIVE SUMMARY

Since 2011, network disruptions and large-scale network shutdowns have become a widespread tool of information control. Governments in at least four continents (Africa, Asia, Europe, and South America) have shut down connectivity or social media in ways that vary in scope, precision, motivation, and impact. Although attention to disruptions is growing within the digital rights and technology policy community, this new form of digital repression requires far greater attention from stakeholders, including companies, policymakers, investors, human rights advocates, and researchers.

This report presents the findings of the author's research tackling the **impact of network disruptions on human rights**. This includes ongoing statistical work as well as a set of 15 interviews with stakeholders within and outside of the Global Network Initiative, conducted between July and October of 2016 as part of a Google Policy Fellowship. Insight from the interviews is presented throughout the report.

- The **statistical study** determines that **network interferences are more likely to happen at higher rates of expansion of Internet connectivity until a tipping point**, suggesting that efforts to extend Internet access in low- and middle-income countries may lead to less overt restrictions. This threshold stands at an annual rate of expansion of about 7 percent.
- The **interviews** reveal that individual actors within the digital rights community are seeking **more coordinated efforts to resist shutdowns**. The interviews are also used to support points made throughout the report.
- A calculation of the cumulative duration of network disruptions reveals **that the Internet and/or social media were disrupted around the world for about 2,500 cumulative days** in 2017 alone. Approximately **105 known shutdowns** took place that year, surpassing each previous year.
- The report outlines a broad range of **civil and political, as well as economic, cultural, and social rights** that are typically impacted by network disruptions, moving beyond the typical focus on freedom of expression, elections, and economic impacts to broaden the arguments and actors discouraging disruptions.

The report concludes with **recommendations** for civil society organizations (CSOs), activists, academics, companies, and others working to discourage governments from ordering future disruptions. These recommendations include:

- **Widening the human rights lens** through which disruptions are examined and critiqued, to include freedoms of association, assembly, and religious belief, as well as rights to health, education, and cultural participation, in order to demonstrate the full impacts of disruptions and expand engagement with actors active on those issues.
- **Enhancing efforts to document**, share information on, and raise awareness of the impacts of network disruptions, including data collection at the subnational level.
- **Underscoring and further funding efforts to expand Internet connectivity** through responsible partnerships with national and local actors as well as exclusively local initiatives.

It is tempting to look at the Internet as a standalone technology, but it is in fact a mirror of human behavior.

— INTERGOVERNMENTAL ORGANIZATION REPRESENTATIVE



INTRODUCTION

Around the globe, access to digital communication technologies is much more of a privilege than it is a right. Governments routinely shut down or disrupt access to the Internet, cell phones networks, and other forms of telecommunication. Whether executed on a national level or targeting a city, region, or specific population, blackouts and related barriers to access are inherently indiscriminate, affecting people of all professions, creeds, ethnicities, political beliefs, and genders. Nevertheless, specific disruptions often have great impact on particular groups. Large-scale disruptions constitute a radical form of **digital repression** — one that curbs multiple rights established in international treaties while undermining local, regional, and national economies.

Network disruptions and large-scale shutdowns have become increasingly common in recent years.

The aim of this report is to assess the circumstances surrounding network disruptions, present the full range of effects and risks that they generate, describe the mechanisms used to execute disruptions, outline the legal context that underpins them, and establish a number of recommendations for future action. It combines prior quantitative, statistical research on the causes and effects of interference in digital networks with a set of 15 semi-structured

interviews conducted during a Google Policy Fellowship with the Global Network Initiative (GNI), a multistakeholder initiative that works to protect and advance freedom of expression and privacy in the technology sector. The subjects of these interviews include industry associations, international organizations, mobile network operators (MNOs or telcos), non-governmental organizations (NGOs), and policy spokespersons from tech companies, as well as one academic. Interviewees were drawn from both within and outside GNI. Insight from the interviews is presented throughout the report, although interviewees' identities are protected.

Where possible, the large-scale disruptions outlined here were verified using a combination of interviews, triangulation of news sources and Google's Traffic and Disruptions tool, made available through Google's Transparency Report. This last tool, which measures the accessibility of various Google products and registers sudden disruptions to them, is arguably the most objective and comprehensive publicly available verification system for large-scale network disruptions¹. In addition, publicly available resources from digital rights organizations Access Now and the Software Freedom Law Centre (SFLC) were used to corroborate shutdown events and elaborate on selected cases.

The report also builds on GNI's efforts to document the impact of network shutdowns and service restrictions, including an overarching statement condemning network disruptions,² a report released in October 2016 highlighting the significant economic damage caused when countries deliberately shut down or otherwise disrupt connectivity,³ and a one-pager addressed to policymakers listing the consequences of such disruptions for human rights, the economy, and public safety.⁴



THE DYNAMICS OF NETWORK DISRUPTIONS

WHAT IS A NETWORK DISRUPTION?

For the purposes of this report, a **network disruption** is the intentional, significant disruption of electronic communication within a given area and/or affecting a predetermined group of citizens.⁵ Extreme manifestations of network disruptions involve the large-scale or complete disconnection of digital communication, with the impact radius covering a local area, an administrative region, several regions, or an entire country. These extreme disruptions are often called network shutdowns, Internet shutdowns, or blackouts. In this report, these terms will be used synonymously, in tandem with “network

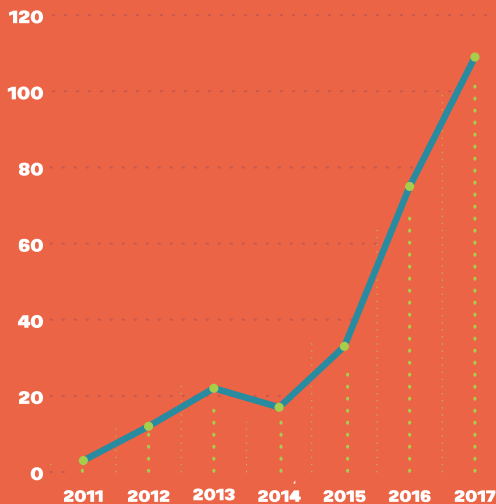
disruption.” Unlike technical failures, intentional disruptions are typically mandated by governments, which carry them out as either a reactive or, increasingly, a preventive measure against perceived real and potential threats. The most common objective of this kind of interference is to restrict the flow of information through digital channels, particularly social media, mobile communication, and dedicated digital communication tools (e.g. WhatsApp, Voice over Internet Protocol [VoIP] services). This is especially prevalent when rising public dissent and protests are deemed to be fueled by digital communication networks.

For the purposes of this report, a network disruption is the intentional, significant disruption of electronic communication within a given area and/or affecting a predetermined group of citizens. Extreme manifestations of network disruptions involve the large-scale or complete disconnection of digital communication, with the impact radius covering a local area, an administrative region, several regions, or an entire country. These extreme disruptions are often called **network shutdowns, Internet shutdowns, or blackouts**.

In this report, these terms will be used synonymously, in tandem with “network disruption.” Unlike technical failures, intentional disruptions are typically mandated by governments, which carry them out as either a reactive or, increasingly, a preventive measure against perceived real and potential threats. The most common objective of this kind of

interference is to restrict the flow of information through digital channels, particularly social media, mobile communication, and dedicated digital communication tools (e.g. WhatsApp, Voice over Internet Protocol [VoIP] services). This is especially prevalent when rising public dissent and protests are deemed to be fueled by digital communication networks.

Network disruptions and large-scale shutdowns have become increasingly common in recent years, in tandem with growing rates of connectivity and the expansion of digital communication infrastructure. This is particularly apparent in developing and non-democratic countries, where legal provisions protecting against such measures are non-existent or limited and rarely acted upon. Aggregating data from various sources, approximately **109 shutdowns or disruptions were reported in 2017**, topping the number of cases reported in 2016 (75).⁶ Both years stand in radical contrast to 2015, when between 15 and 33 major disruption episodes were registered (*figure 1*). Although degrees of confidence, volumes of evidence, and criteria of selection vary, it is possible that as many as **184 network shutdowns** or disruptions of particular platforms have taken place in 2016-17, not counting smaller-scale disruptions undetected by researchers and analysts.⁷ Disruptions have been used in response to protests, riots, ethnic tension, and mass events,



¹ Aggregating data from various sources, approximately 109 shutdowns or disruptions were reported in 2017, topping the number of cases reported in 2016 (75).^[1] Both years stand in radical contrast to 2015, when between 15 and 33 major disruption episodes were registered (*Figure 1*). Although degrees of confidence, volumes of evidence, and criteria of selection vary, it is possible that as many as 184 network shutdowns or disruptions of particular platforms took place in 2016-17, not counting smaller-scale disruptions undetected by researchers and analysts.

but also during professional and secondary-school exams in Algeria, Ethiopia, Gujarat (India), Iraq, Syria, and Uzbekistan.⁸

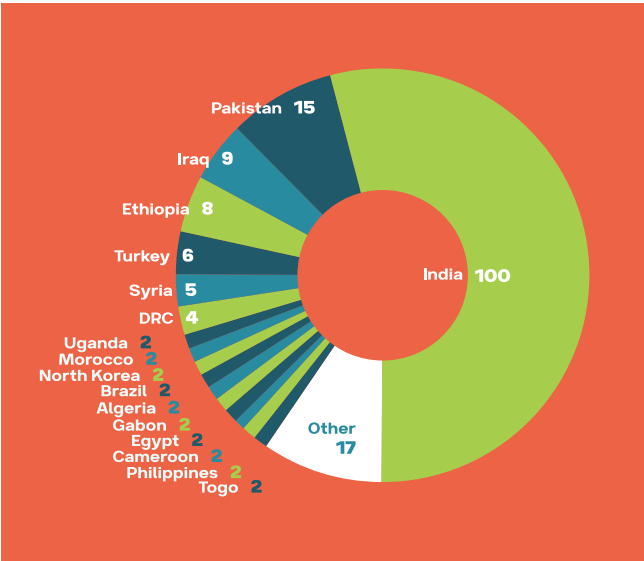
Recent shutdown events in countries like Brazil and India, multiple suspected disruptions in the October 2017 Catalan independence referendum, and the emergence of provisions for network disruption and shutdown in the laws of mature democracies (e.g., Poland⁹) all reveal that the phenomenon is **not limited to authoritarian and non-democratic regimes**. Democracies are not immune to the threat of network disruptions.¹⁰ India alone accounts for around 70 percent of all known large-scale shutdowns

in 2017. While this suggests that India is an outlier among all countries, it also sets a precedent for indiscriminate abuses in fragile or hybrid democratic systems (figure 2).

Targeted website blocking and takedowns that do not reach the threshold for network disruptions also occur frequently, typically at the Domain Name System (DNS) level.¹¹ The profiles of these websites vary considerably. Many are focused on specific activities, such as gambling, pornography, or file sharing, as opposed to serving as general communications platforms. Thus, while broader network disruptions are often intended to disrupt collective action and communication, targeted website blocking can stem from a broader set of goals, even as the blocking can end up creating broader disruptions, either intentionally or inadvertently. Hackers periodically carry out Distributed Denial of Service (DDoS) attacks and other cyberattacks, either independently or at the behest of influential clients, including governments.¹² Two prominent attacks have targeted Dyn, an Internet intelligence company whose research arm investigates politically motivated Internet disruptions (2016), and GreatFire, a repository of

tools to resist Chinese Internet censorship (2015). Notwithstanding the widespread damage that stems from these incidents, they are not discussed in this report for two reasons: 1) they focus on temporarily flooding or disrupting individual DNS providers or websites rather than impeding many-to-many communication on a macro level, and 2) it is often very difficult to assign responsibility for and understand the motivations behind them.¹³ While these tactics fall outside the scope of this report, they often form part of the same suite of offensive tools that includes large-scale disruptions.

It is also useful to distinguish between disruptions and government requests to companies to remove data. Information and communications technology (ICT) companies — like Facebook, Google, and Twitter, as well as telcos — receive an increasing number of user data requests and requests for content removal from governments every year. These companies regularly disclose information about such requests in their transparency reports. While there is an overall upward trend in the number of removal requests, their distribution is highly skewed: over 34 percent of those received by Google in the first half of 2017 originated in the United States, and both executive and judicial authorities in democratic countries are responsible for hundreds or thousands of them.¹⁴ In Africa, Orange revealed a similarly lopsided distribution of subscriber data requests, with a preponderance of cases in Cameroon, Mali, and Senegal.¹⁵ While there is a correlation between network disruptions and requests in some countries, it does not exist in many others (figure 3). User data requests and removal requests are part of the mechanics of surveillance and information control in many states, but they create less overt restrictions on access to information and communication than large-scale disruptions.



2 Number of network disruptions by country (2016-17). The "Other" category includes multiple countries that have only implemented one known shutdown during this period: Bahrain, Bangladesh, Belarus, Chad, China, Congo, Equatorial Guinea, the Gambia, Iran, Mali, Montenegro, Saudi Arabia, Somalia, Ukraine, Yemen, and Zimbabwe.

NETWORK DISRUPTIONS 2016-17		REMOVAL REQUESTS 2016		
		GOOGLE	TWITTER	FACEBOOK
INDIA	100	575	140	13,613
IRAQ	9	1	0	1
PAKISTAN	15	36	22	1,721
SYRIA	5	0	0	0
TURKEY	6	1,781	5,569	1,452

3 Top five countries executing network disruptions (2016-17) and respective figures for data or removal requests made to Google, Twitter, and Facebook (2016). Sources: Google, Twitter, and Facebook Transparency Reports.

WHEN DO NETWORK DISRUPTIONS OCCUR?

The majority of known shutdown events have revolved around issues of **national or regional security**. Governments are particularly prone to disconnecting communication networks during or in anticipation of mass protest, whether violent or non-violent. For instance, 37 of the 61 shutdowns identified by Access Now between January and September of 2017 were suspected to be caused by either protests or political instability. Shutting down communication in such circumstances disorients the protesters and disrupts coordination among the protest or movement leaders. Shutdowns can also be used as a security measure in the period of uncertainty or cooling following violent clashes or terrorist attacks.¹⁶

Contentious elections and the existing or expected unrest that accompanies them has been a routine justification in numerous African countries (see next section). Similar arguments have been made with regard to **spreading rumors** and multimedia that may lead to collective action — primarily in India and Pakistan.¹⁷ Disruptions to prevent cheating in **professional and school exams** are a new trend in several countries, most commonly taking the form of Internet curfews, i.e., full or partial blackouts at prescribed times throughout an examination period. Finally, a subset of network disruptions occurs around **mass public events** such as religious processions, which are a common target for technologically enabled terrorism (e.g., IEDs triggered by cell phones and other devices). Other recorded mass public events include wrestling matches (India), visits by public figures (India, Philippines), and beauty contests (Philippines).

Targeted shutdowns can be understood as either **preventive** or **reactive**. Although reactive shutdowns remain the norm, preventive action is becoming increasingly common, most notably in anticipation of unrest, military operations, mass events, and elections.

Democracies are not immune to the temptation of network disruption. India alone accounts for around 70 percent of all known large-scale shutdowns in 2017.

Although there are valuable contributions on individual cases, academic research has not made rigorous attempts to determine the factors that affect the likelihood of network disruption or the repercussions of these incidents. One example is the full, national-level shutdown in Egypt during the Arab Spring (January 2011) and the backfire it generated. Navid Hassanpour has documented how the Egyptian shutdown ordered by the government of embattled dictator Hosni Mubarak caused street

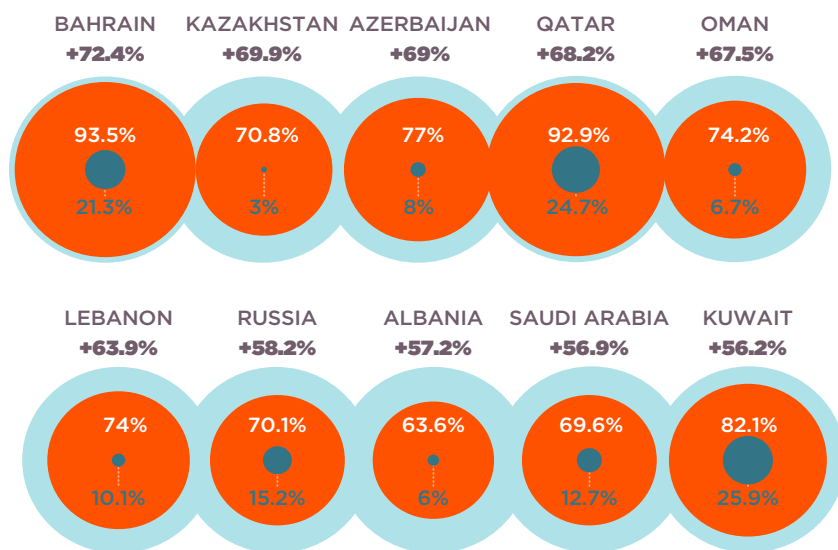
protest to spiral out beyond a central point in Cairo, expanding the protesting crowds in numbers and space to include large swathes of the general population in more urban districts.¹⁸ This work suggests that when central communication is disrupted, protest movements may find unconventional, local leaders. Despite these adverse effects, national-level disruptions continue to occur, particularly when opposition to the government is vocal and engages the entire country. Anita Gohdes has linked blackouts to increased rates of political violence in Syria, raising important questions about disruptions as a substitute for physical repression.¹⁹

Structurally, the resilience of a country's Internet as a whole depends on several factors. One notable component is the degree of decentralization and diversity of the Internet infrastructure on a national level. The more domestic providers a country has with direct connections to foreign providers at the international frontier, the greater the resilience of the network as a whole. By extension, such countries may be at a lower overall risk of large-scale disconnection.²⁰ Research connecting telco ownership with shutdowns is slowly emerging. Conversely, the **socioeconomic conditions associated with disruptions** are more difficult to gauge and must be interpreted with caution.

While the likelihood of 'traditional' repression has often been linked to underlying structural conditions and socioeconomic problems, empirical research exploring the same conditions in connection with digital forms of repression is scant. Studies that are relevant to network disruptions typically tackle larger topics within which disruptions are embedded or discuss peripheral forms of digital aggression. Not surprisingly, research has shown that authoritarian regimes place overt restrictions on access much more often than do states with democratic regimes or those in the grey area between the two. The latter, also known as hybrid regimes, often enjoy some flexibility given their selective interpretation and application of the law, accompanying components that lend them a veneer of democracy.²¹

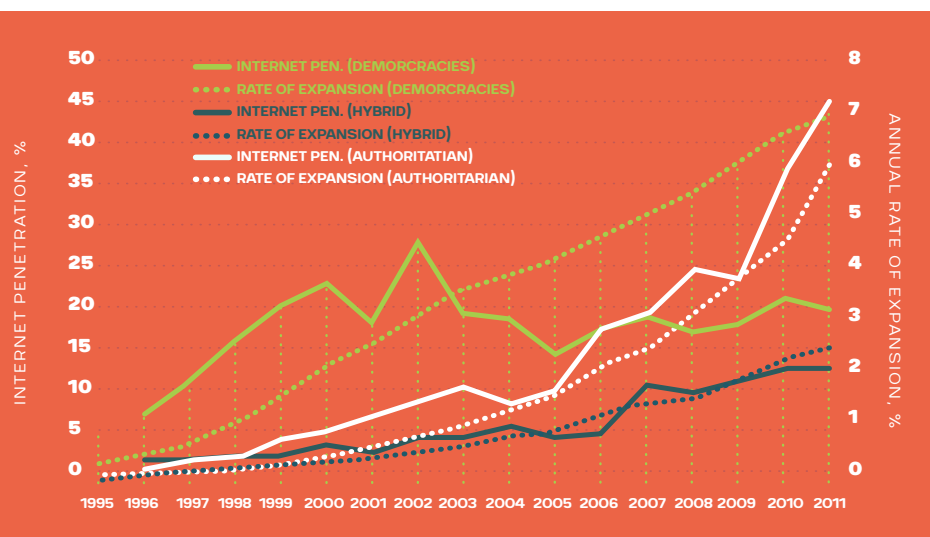
However, the expansion of connectivity has been demonstrably vigorous in non-democratic regimes and those that actively prevent the development of an independent public sphere (figure 4).²² As connectivity grows, non-democratic systems, which are less predictable than consolidated democracies, are opening a digital sphere that is increasingly vulnerable to their ambition of information control. On the other hand, rising connectivity and social media activity have been linked to greater incidence of street protest.²³ This is important because governments may perceive digital networks as a threat to their power due to their potential ability to mobilize disgruntled masses, which can lead to further crackdowns on free expression.

Uncertainty regarding the criteria for content that could trigger a disruption increases the potential for human rights impacts. In Zimbabwe, for instance, a nationwide stay-away protest in July 2016 was partially coordinated through WhatsApp, a fully encrypted instant messaging service that attracts a large subscriber base in the country.²⁴ Despite its lack of access to WhatsApp content, the government briefly suspended the app's services and issued a vaguely-worded warning to users deemed responsible for spreading malicious rumors online.²⁵ This approach, enacted without clear guidelines on what constitutes appropriate online expression, encourages users to remain silent on a broader range of issues as a precautionary measure, deepening the chilling effect on free expression.²⁶



4 Countries with fastest-growing Internet penetration, 2005-15. Source: Own work based on World Development Indicators (2017).

Regardless of whether the criteria and processes for ordering disruptions are clear, certain justifications seem to garner more attention than others. For example, when these measures specifically target alleged coordination efforts by terrorists to detonate bombs via Short Messaging Service (SMS), the interviews conducted for this report suggest that many network operators accept the justification.



5 Annual Internet connectivity (left vertical axis) and rate of expansion of Internet connectivity (right vertical axis) in democratic, hybrid, and authoritarian regimes, 1996-2011. Note pace of expansion peaks in 2001-2 in democracies and several years later in authoritarian regimes.. Democracy scores based on Polity 2 dataset. Internet penetration and rates of expansion calculated using World Development Indicators (2017)

In separate research covering the period between 1995 and 2011, this author tentatively established that network interference, defined broadly to include micro-level events,²⁷ is more likely in countries that experience a faster pace of expansion of Internet connectivity. However, there seems to be a tipping point in the speed of expansion beyond which the likelihood and frequency of network interference begin to fall. Further statistical inquiry suggests that this tipping point lies at an annual rate of expansion of approximately 7 percent. Ongoing research using detailed, daily data suggests that shutdowns trigger a surge in

protest followed by a steep decline as a shutdown extends into what can be described as an economically devastating **digital siege**.

These conclusions are tentative until verified by extensive review. The Arab Spring was an inflection point for both digitally enabled protest movements and the escalation in the use of large-scale shutdowns by governments. Given their increasing frequency, these incidents can now be isolated from the landscape of network interference and investigated separately using advanced statistical tools. Recent years have seen a vigorous expansion of communication technology in the developing world, including considerable transnational investments in terrestrial cable,²⁸ the continued growth of submarine cables,²⁹ and multiple innovations in the delivery of Internet to disconnected communities. These factors, aside from galvanizing considerable decreases in the cost of connectivity, have had two, at times conflicting, effects: introducing new costs and barriers to information control, while challenging governments to devise new ways to manage the flow of digital content.

HOW DO NETWORK DISRUPTIONS OCCUR?

On a technical level, network disruptions can be implemented in various ways, most of which are not mutually exclusive. Both the institutional dynamics of shutdown orders (weak checks and balances, enabling chains of command, state ownership of telcos) and the technical facets of blackouts may have important policy implications. Permissive legal environments also enable a variety of government-mandated restrictions. (For a more extensive discussion of these dynamics, see the annex, as well as the work of network analysis firms and organizations, including Akamai, the Center for Applied Internet Data Analysis (CAIDA), the Open Observatory of Network Interference (OONI), and Oracle.)

Freedom of expression and elections-related impacts are the most commonly highlighted and well-documented human rights impacts of network disruptions.

THE CHALLENGES OF RESISTING SHUTDOWN ORDERS

Resisting shutdown orders can be particularly hazardous for Internet Service Providers (ISPs) and mobile operators. Nearly all of the telco representatives interviewed for this report referred to direct threats made to their employees on the ground for noncompliance with a shutdown order, with several employees having to leave their operating countries to protect their families.³⁰ One spokesperson for an international organization referred to the shutdown in Ethiopia during the ethnic protests in 2016³¹ as an example of governmental use of threats and other forms of extreme pressure that prompted some employees to flee the country. Similarly, the activation of the EASSy undersea cable in Somalia — the first connection of this kind in the country — was announced discreetly amid threats by the Islamist group al-Shabaab directed at employees of telecom provider Hormuud, which banned mobile communication in early 2014. Indeed, militants soon kidnapped several Hormuud employees when the company refused to provide al-Shabaab with protection payments.³²

Telcos in particular are bound by the laws governing the countries in which they operate and are thus obligated to comply or face threats, fines, license revocations, and/or gateway shutdowns. Interviewees stated that shutdown requests often come in the form of written (or, in some cases, verbal) orders from national telecom regulatory authorities as well as interior and defense ministries. Whether or not a particular law is cited differs by country, but where it is not, companies often utilize the gap to challenge the order by requesting legal justification. According to one telco representative, “sometimes companies are put in the awkward position of having to inform the government of the content of its own laws.” However, while telcos can and, depending on the circumstances, should be expected to challenge network disruption orders, the vague wording of ICT and national security regulations, and the requirements of the company’s operating license, together with other pressures, render it virtually impossible to resist most of them.



THE IMPACTS OF NETWORK DISRUPTIONS

Freedom of expression and elections-related impacts are the most commonly highlighted and well-documented human rights impacts of network disruptions. The UN Special Rapporteur on freedom of expression has identified many of them as elements of a broader, global drive to expand control over digital communication, as have civil society organizations.³³ Without diminishing these impacts, it is also important to widen the scope of analysis and understand the broader set of human rights impacts of these events.³⁴ This section will review a non-exhaustive variety of human rights impacts caused by network disruptions, grouped into two main categories: impacts on civil and political rights, and impacts on economic, social, and cultural rights.

CIVIL AND POLITICAL RIGHTS

A.1. FREEDOM OF EXPRESSION, ASSOCIATION, AND ASSEMBLY³⁵

Disruptions undermine civil and political rights. In July 2016, the United Nations Human Rights Council adopted a resolution that, among other provisions, “condemns unequivocally measures to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law.”³⁶ The resolution also affirms that “*the same rights that people have offline must also be protected online, in particular **freedom of expression**,*” in accordance with articles 19–22 of the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR).



The impact of disruptions on expression is perhaps most acute when they **coincide with restrictions on freedom of the press**, particularly in light of the expansion of digital media and the growing online presence of traditional media outlets across the world. For instance, a 15-day shutdown in July 2016 in the Indian state of Jammu and Kashmir was implemented concurrently with the suspension of several newspapers and cable television, exacerbating the underreporting of abuse by all sides.³⁷ Syria and Nauru present similarly challenging environments for journalists, as do many countries that witness repeated communications blackouts. While some countries still score higher on Internet freedom than on freedom of the press, the digital capabilities of governments are expanding, particularly with regard to the use of disinformation and bots, leading to a continued overall decline in Internet freedom.³⁸

Bans on digital communication have also been **a mainstay of recent elections**, particularly in Africa, including Chad,³⁹ Uganda,⁴⁰ the Democratic Republic of the Congo,⁴¹ the Republic of the Congo,⁴² and Gabon.⁴³

In each case, the suspension of services reduced the visibility of opposition, either during or after the election itself. Governments typically offer one of two justifications for elections-related disruptions: national security or concern for the fairness of the electoral process. Similarly, regional governors in India have repeatedly cut access to Internet and mobile services as a preventive measure to combat the spread of rumors amid caste-based unrest across the country, including several incidents that occurred around elections.⁴⁴ Opting for such blanket bans over precision tools to weed out individual

advocates of mass violence (during an election or otherwise) jeopardizes free expression on both contentious and everyday topics.

Disruptions also frequently target and/or restrict **freedoms of association and peaceful assembly**. Disruption incidents are often justified by fear of unchecked rumors and the capacity of online debate to incite violent protest in socially and politically sensitive moments. Social media platforms in particular are perceived as a threat to regimes due to their logistical and organizational potential as well as the state's lack of direct control over content. For instance, one

study found that 49 percent of the participants in 2014's Euromaidan protests learned about exact gathering locations through Facebook.⁴⁵ In Turkey, the primary hashtag associated with the 2013 Gezi Park protests (#direngeziparki) was used more times in the first 24 hours than its counterpart from the Egyptian Revolution was used throughout the entire revolution.⁴⁶ Depending on the user base in a given country, one or both of these platforms may be used as cornerstones of protest mobilization. Similar examples elsewhere provide more than circumstantial evidence that social media are increasingly used as a tool of collective action. In cases where they do play a leading role, they are at least complementary to traditional forms of coordination and organization.

Furthermore, due to the largely unpredictable dynamics of online movements, regimes may view communication via social media as a threat, even as governments' perceptions may not match reality.⁴⁷

The decentralization of protest and social movements in the digital age has led several analysts to consider them leaderless, as many of them lack traditional hierarchical structures.⁴⁸ Not all online movements that translate to demonstrations on the street are leaderless. For instance, the #BringBackOurInternet campaign that was initiated following the extended blackout in Anglophone Cameroon has a small cluster of coordinators, that include activists based outside the country.⁴⁹ Moreover, disconnecting civilians on the ground from external backing in the form of online mobilization may skew local activists' perception of broader support for their cause. This can further hinder expression and association on a local level.⁵⁰

A.2. RIGHT TO EQUALITY AND DIGITAL DISCRIMINATION⁵¹

Large shutdowns are sometimes executed in regions where a marginalized ethnolinguistic or religious group forms a considerable part of the population. Recent research recognizes **digital discrimination** in access to communication technology as a global trend that strongly affects disenfranchised ethnic groups, and large-scale disruptions only magnify this problem.⁵² Shutdowns may constitute a targeted form of digital repression that **disproportionately affects a marginalized community and thus constitutes collective punishment**.

Vulnerable groups, including women, refugees, migrants, and internally displaced persons, experience further barriers to education, access to services, and both communication and transfer of remittances to their families.

This was the case during the protests in the region of Oromia (Ethiopia) in 2016. Large-scale unrest, motivated by the grievances of the Oromo ethnic group, prompted prolonged social media shutdowns in the Oromia region in March and August, as well as disruptions and slowdowns that appeared to be nationwide in scope between October and December.⁵³ Another wave of disruptions prompted by turbulence in Oromia was reported nationwide in mid-December 2017 and continued through the end of the year.⁵⁴

On the other side of the continent, the extended blackout in Cameroon in January 2017 specifically targeted the country's two Anglophone regions, where opposition to the Francophone regime of Paul Biya is strong and persistent. Vulnerable groups, including women, refugees, migrants, and internally displaced persons, experience further barriers to education, access to services, and both communication and transfer of remittances to their families.

A.3. FREEDOM OF RELIGIOUS BELIEF⁵⁵

The role of the Internet and mobile communications in expanding access to and delivery of information about religion and freedom of thought, as well as engagement in education and dialogue around these topics, is poorly understood. Clearly, increasing numbers of people are using the Internet and mobile platforms to share relevant information, whether through targeted evangelism or the provision of generally available religious resources. These mediums also play an increasingly important role in facilitating various forms of religious practice, including by providing reminders, guides, and access to religious authorities.

To date, much examination of the impact of the ICT sector on religion focuses on the misuse of these tools to either spread hateful ideology (i.e., religious extremist views) or to target minorities or non-believers (i.e., the persecution of atheist bloggers in Bangladesh). These scenarios are important to understand and address.⁵⁶ However, these kinds of 'negative' case studies are often

Governments face a conundrum: letting technology flourish, or restricting and controlling it. Both options may invigorate mass protest, generate social movements, and trigger other forms of collective action.

also used to justify censorship, surveillance, or restrictions that can violate human rights if not carefully tailored. Without diminishing the need for further analysis of those scenarios, it is also imperative that digital rights activists develop a deeper understanding of the positive role that the Internet plays to facilitate the freedom of thought, conscience, and religion to better understand how network disruptions impact these activities. This could lead to strategies where new and important actors fight against network disruptions.

A.4. RIGHT TO LIFE, BODILY INTEGRITY, AND SECURITY OF PERSONS⁵⁷

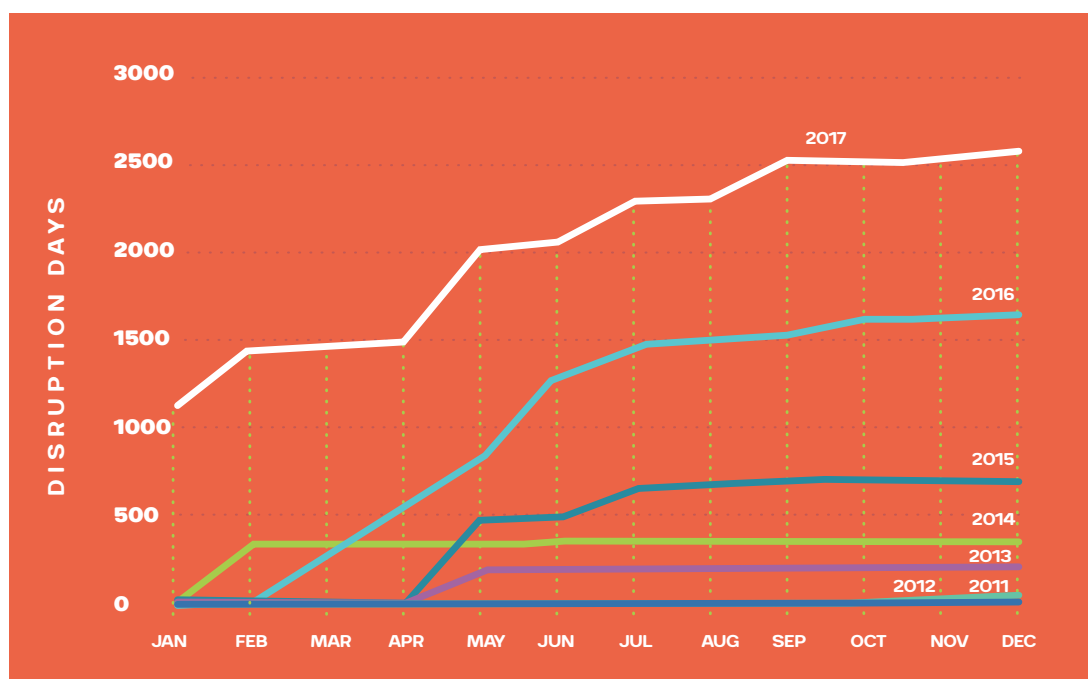
Network disruptions and shutdowns provide an invisibility cloak for violence as well as gross violations of human rights and/or the laws of war. Shutdowns enable governments and non-state actors to conceal violations of the right to bodily (or physical) integrity and security of persons behind a digital smokescreen. These rights, enshrined in the UDHR and the ICCPR, extend to internal conflicts, where they are covered by Protocol II of the Geneva Conventions. By interrupting the flow of information beyond the borders of the city, region, or country, governments severely undermine reporting on these violations. Furthermore, network disruptions interrupt communication between family members caught in the fog of war, trying to escape the violence. This is especially acute when basic telephony (e.g., SMS) is blocked, as has happened numerous times in India and Pakistan in 2017.⁵⁸ Such large shutdowns sometimes accompany aggressive military or paramilitary operations, rendering them virtually impossible to document in real time by reporters and citizen journalists.

Research has confirmed that a **concentration of Internet disruptions in the Syrian Civil War** was observed immediately prior to and during military offensives carried out by the Syrian Army between 2011 and 2013. These incidents, occasionally presented by the Syrian government as technical outages or cable cuts, coincide with an increased number of killings attributed to government forces.⁵⁹ In Nauru, another temporary ban on Facebook and other online services in 2015 raised concern among human rights advocates that the measure was used to conceal human rights abuses and deplorable living conditions in the island's detention centers for asylum-seekers attempting to reach Australia.⁶⁰ One civil society representative reported that the extent of the human rights abuses in

the Pool region of the Republic of the Congo (October 2015) and Port-Gentil, Gabon (February 2015) was unknown due to the communications blackouts that took place in both countries for ten and three days, respectively.⁶¹

The proliferation of prolonged, large-scale shutdowns in particular has given rise to previously unknown phenomena and threats to individuals' safety and physical integrity. One of these is the emergence of **Internet refugees** or **digital refugees** in affected areas. According to individual testimonies collected at the time, at least some of those killed by the Islamist militant group Boko Haram in the Benisheik massacre (Borno State, Nigeria) in September 2013 had traveled to the border town of Damaturu (Yobe State) to make phone calls after cell phone service in Borno State was blocked amid a military offensive against the insurgents.⁶² In the 2017 Cameroon shutdown, flows of Internet refugees from the disconnected Anglophone regions of the country poured into neighboring Francophone regions, Nigeria, and border areas in an effort to obtain Internet access. Residents, migrant workers (primarily from Nigeria), NGO affiliates, and individuals working in the tech sector regularly undertook perilous journeys through highly militarized areas and set up makeshift camps where at least intermittent access was possible.⁶³ These new, spontaneous population flows, whose full scale is yet to be determined, create additional risk and windows for abuse.

These effects are exacerbated by the fact that, on a cumulative level, **shutdowns and disruptions are getting longer every year** (figure 7) displays a rough estimate of the number of days during which the Internet or social media were rendered unavailable around the world between January 1, 2011 and



7 Cumulative shutdown duration for each month between 2011 and 2017. Shutdowns that began in a given month and lasted for several months are classified in the month in which they began. Thus, a shutdown that began in January and lasted throughout the year will have contributed 365 days to the total and the figure will be registered under January. A shutdown that differed from previous years in that a number of shutdowns carried over from the previous year and/or lasted for most of 2017 – hence the higher starting point. Disruptions that lasted several hours are classified as single-day shutdowns. Totals do not include cases in which certain services are permanently banned as a matter of national policy (e.g., social media in the People's Republic of China). Note: the calculation is approximate due to multiple differences between sources in both conceptualization methodology applied to network disruptions. Existing data are also highly fragmented. Source: Own calculations based on triangulated news sources, Google's Traffic Disruptions tool, Access Now's STOP, SFLC's InternetShutdowns.in, and Bytes4All's Killswitch.pk.

December 31, 2017. Across all countries, disruptions in connectivity were found on **2,576 cumulative days** in 2017. The total number of blackouts that year far exceeded the results recorded in each of the preceding years. These dynamics were fueled both by scattered, single-day shutdowns and prolonged incidents such as the ones in Anglophone Cameroon that occurred at the end of the year. Prolonged shutdowns can amount to a state of what could be called a **digital siege**, wearing down public dissent under the guise of pacifying volatile situations. In such conditions, all of the aforementioned impacts are exacerbated, as lack of accurate reporting on violence can become the new normal. The combination of frequent and prolonged shutdowns is perhaps best captured in the Indian state of Jammu and Kashmir, which experiences regular, back-to-back shutdowns that conceal the real security situation in the region.⁶⁴ The repercussions of shutdowns for local, regional, and national economies are described in the next section.

ECONOMIC, SOCIAL, AND CULTURAL RIGHTS

Disruptions undermine economic, social and cultural rights. The International Covenant on Economic, Social and Cultural Rights (ICESCR) defines a number of rights stemming from each individual's right to self-determination, most notably the free pursuit of his or her economic, social, and cultural development (Art. 1). The treaty's 164 signatories are committed to upholding and progressively ensuring the full protection of these rights. Large-scale disruptions violate many of them. While significant work has been done to document and highlight the economic impacts of network disruptions, more can and should be done to underscore the wider social and cultural impacts.⁶⁵

B.1. ECONOMIC RIGHTS⁶⁶

Disruptions significantly damage the financial ecosystem and local economy of their impact zone. The scale of the economic losses incurred by businesses and institutions as a result of deliberate network disruptions is difficult to ascertain. Revenue losses in particular are rarely reported. Organization for Economic Co-operation and Development estimates of the financial impact of Egypt's 2011 shutdown suggested a minimum figure of \$90 million.⁶⁷ A more recent blackout in Gujarat (India) froze an average of \$225 million in daily mobile transactions across the state, according to an industry spokesperson.⁶⁸ A separate incident in Gujarat coincided with the income tax filing deadline, forcing taxpayers to fill out their returns by hand at local service counters.⁶⁹ Disruptions affect e-commerce sites, taxi services, Internet and mobile banking, and the startup ecosystem,⁷⁰ in addition to creating a climate of uncertainty for international investments.⁷¹ There is evidence of governments using shutdowns as a tool to compel telecommunications companies to modify their business models, creating a significant chilling effect.⁷² In the September 2017 Togo shutdown, Access Now's Shutdown Stories Project documented delayed paychecks due to disconnected ATMs, local journalists being forced to incur prohibitive costs to find an Internet connection, and business deals that failed due to the lack of connectivity.⁷³

Prolonged disruptions perpetuate the digital divide, not only within countries, but also across borders, mostly affecting girls and women.

The World Bank has stated that the digital dividends of Internet and cell phone connectivity are more numerous and widespread than can be measured. In this same sense, the repercussions of their absence are more pervasive than can be observed.⁷⁴ On an individual level, some instances of protracted shutdowns have forced businesses to shut their doors permanently due to irreparable economic damage, especially when the next blackout is certain to arrive shortly (e.g., Kashmir). Small vendors who depend on the Internet are the first to be swept from the digital economy, as they lack necessary resources for resilience and recovery.

In many African countries, the repercussions of large blackouts are particularly acute given the popularity of mobile services. Industry intelligence reported that Sub-Saharan Africa's complex mobile ecosystem provided 3.5 million jobs, generated \$110 billion in economic value, and raised \$13 billion in taxes in 2016.⁷⁵ Mobile Internet was available to 26 percent of the region's population — a figure estimated to increase to 38 percent by 2020. ICT investment is on the rise across the continent. In fact, the Internet is expected to contribute an average of 5-6 percent of each country's GDP by 2025.⁷⁶ The mobile industry's productivity impacts in 2016 amounted to \$62 billion while total impacts (direct, indirect, and productivity) reached \$110 billion.⁷⁷ Mobile money services in particular fuel both formal and informal economies, helping individuals to exchange goods and services and cutting the costs of doing business. Across 39 countries, 140 mobile money and banking services host about 280 million registered accounts, providing safe, low-cost, and rapid financial transfers while broadening financial inclusion. Disruptions to these services (e.g., Uganda 2016) reverberate among the companies and individuals who use them, eroding the economic rights of civilians while diminishing the beneficial effects of mobile services in the digital economy.

Prolonged digital sieges wear down businesses that would otherwise have survived multiple short disconnections. For instance, businesses reliant on an Internet connection have been crippled in Jammu and Kashmir (various shutdowns with a cumulative length of several months), the Federally Administered Tribal Area in Pakistan (450+ days), and Cameroon (93 days), among others.⁷⁸ The threat

of future disconnection, as expressed by the Government of Cameroon following the 2017 shutdown, can permanently erode confidence in the market and business environment among both local entrepreneurs and international investors.

Three studies have attempted to assess the impact of large-scale network disruptions on the economies of affected countries.⁷⁹ In 2016, the Global Network Initiative released a study that estimated the impact of a full Internet shutdown by level of connectivity.⁸⁰ Under this framework, with each day of complete blackout, high-connectivity countries would lose an average of \$23.6 million per 10 million population, medium-connectivity countries would lose \$6.6 million, and countries with low penetration could expect to lose \$0.6 million. Another study by the Brookings Institution estimated that shutdowns had cost the world economy \$2.4 billion in 2015 alone, with nearly half of the damage to GDP concentrated in India.⁸¹ Finally, a report by the Collaboration on International ICT Policy in East and Southern Africa (CIPESA) employed an innovative methodology that included lost cost savings, efficiency gains, and reputational effects to determine that disruptions cost the economies of Sub-Saharan Africa more than \$218 million in 2016.⁸² All three studies acknowledge that they underestimated the economic impact of shutdowns, which resonate in supply chains, distort the stable growth of local businesses, and culminate in foregone investments, among many other negative impacts.

Finally, it is important to establish whether network disruptions have a noticeable economic effect on the flow of remittances to low and middle-income countries. Remittances, or money transfers sent by foreign workers back to their home countries, provide a vital and stable contribution to the GDP of many countries, including Kyrgyzstan (34.5 percent of GDP), Haiti (27.8), The Gambia (20.4), and Nepal (29.7).⁸³ Remittance inflows in India, which remain the largest in the world in absolute terms (\$62.7 billion in 2016), experienced a decline of 8.9 percent in 2016. While this is generally attributed to a drop in gas prices and changes in the fiscal policy of oil-producing countries, disruptions to the technology that enables the receiving of remittances are worth investigating as potential additional causal factors.

It is important to establish whether network disruptions have a noticeable economic effect on the flow of remittances to low and middle-income countries.

B.2. RIGHT TO MENTAL AND PHYSICAL HEALTH⁸⁴

Article 12 of the ICESCR establishes “the right of everyone to the enjoyment of the highest attainable standard of physical and mental health.” While the effects of disruptions on health care and emergency services are not yet widely known, at least one gynecologist in Pakistan was not able to communicate with a pregnant patient due to a cell phone shutdown in 2013, leading the patient to a miscarriage.⁸⁵ A three-week-long disruption in Somalia in June–July 2017 also reportedly hindered the delivery of crucial medical paperwork in individual cases, in addition to obstructing remittances, education, business, and humanitarian action.⁸⁶ While the incident was probably caused by accidental cable damage by a commercial ship, it dramatically reduced connectivity across most of the country and exemplified the complex impacts of disruptions, whatever the cause.

In India, journalist Safeena Wani reported that, due to an ongoing shutdown in 2016, a hospital in Srinagar (Jammu & Kashmir) was unable to contact a specialist in another part of the state to repair the facility’s CT scanner, leading to delays in life-saving procedures.⁸⁷ Digital Empowerment Foundation has highlighted the particular psycho-social impacts of disruptions that take place in the context of ongoing conflict. These effects are just as severe outside conflict zones. The Indian government’s Digital India campaign, for example, promotes the use of digital technology in health services, but intermittent or non-existent access prevents patients to reap the benefits of the program.⁸⁸ It is possible that many similar cases remain underreported, even as many of the human costs of disruptions remain. As more and more health services and related resources become available online, the impacts of disruptions on mental and physical health will no doubt become more severe.

B.3. RIGHT TO EDUCATION⁸⁹

Article 13 of the ICESCR expresses the foundational nature of education, explaining that it is necessary to “enable all persons to participate effectively in a free society, promote understanding, tolerance

and friendship among all nations and all racial, ethnic or religious groups, and further the activities of the United Nations for the maintenance of peace.”

The role of the Internet in education is increasingly important as one moves into higher levels of education. Most academic fields include components that require online resources, and their absence jeopardizes academic success for all civilians. However, its importance is particularly acute in Science, Technology, Engineering, and Mathematics (STEM) fields, which are commonly seen as the beacons of progress and development in modern societies.

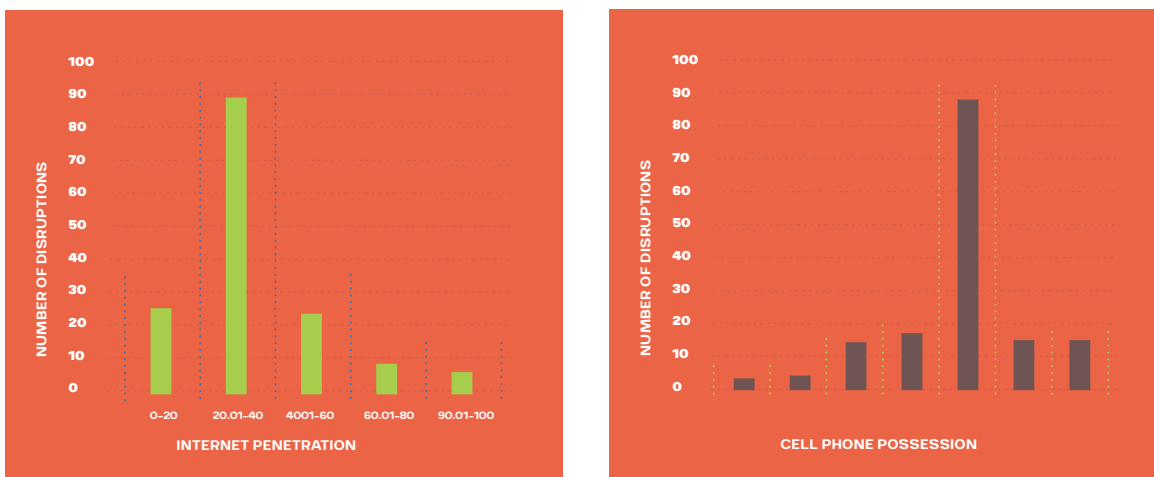
In prolonged blackouts, students at all levels fail to achieve success for this reason, as reported everywhere from Kashmir to Ethiopia.⁹⁰ Furthermore, one third of the students that are enrolled in online courses via the online learning platform Coursera live in low and middle-income countries, which are more sensitive to disruptions and outages than high-income countries and are prone to numerous other forms of network instability (Robertson 2015).⁹¹

The specter of shutdowns places a heavy burden on **vulnerable populations**, whose access to education is already a challenge relative to their peers. Girls and women in particular are underrepresented in both STEM and general education in most of the states affected by disruptions. Sophie Ngassa, a tech entrepreneur in Cameroon working with young girls to improve their digital skills and encourage them to enter the STEM fields, later described the repercussions of the blackout for this group, which was unable to compete in innovation challenges on both the national and international level.⁹² Prolonged disruptions perpetuate the digital divide, not only within countries, but also across borders, mostly affecting girls and women. The proliferation of shutdowns to stem cheating and leaks during school exams in Algeria, Ethiopia, India, Iraq, Republic of the Congo, Syria, and Tunisia not only exemplifies disproportionate repressive action, but also undercuts educational opportunities for all groups in all regions across each country.⁹³

B. 4. RIGHT TO TAKE PART IN CULTURAL LIFE AND BENEFIT FROM SCIENTIFIC PROGRESS⁹⁴

The Internet has facilitated the ability of people in otherwise remote areas to **participate in cultural life and benefit from scientific progress**. Curbing access to digital networks not only cuts entire populations off from these opportunities, but also generates impacts that bleed into employment, health, education, and free expression. Social media platforms in particular play a significant role in creating new and dynamic mediums for cultural expression.

Shutdowns take place in areas where Internet use is expanding and cell phone possession is relatively high (*figure 8*). As these industries grow, so will the reliance on digital networks in various aspects of life. The multi-layered impact of disruptions will become more acute as countries become more digitized, particularly as multinational companies partner with weakly connected states (e.g., Google’s Project Loon, Facebook’s Aquila and Free Basics, O3B’s and SpaceX’s low-orbit satellite constellation projects) to extend Internet access to billions of unconnected civilians. The more that people, institutions, and organizations rely on digital communications, the greater the negative impact of a shutdown.

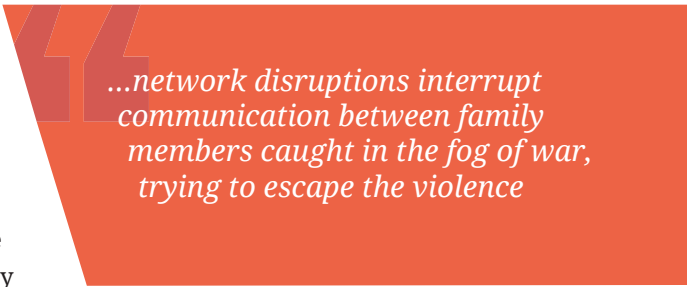


8 Number of network disruptions (January 2016 to October 2017) by internet penetration (left) and cell phone possession (right). Source: own work based on World Development Indicators (2017).

HUMANITARIAN IMPACTS

Large-scale shutdowns can undermine humanitarian efforts. These impacts fall within international humanitarian law rather than the narrow scope of international human rights law that undergirds this report. In February 2014, humanitarian groups and NGOs in Somalia reported on the impact of severed communication between field and central teams when Islamist militant group al-Shabaab forced Hormuud, the country's largest operator, to shut down mobile Internet services, accusing it of enabling espionage by Western intelligence agencies.⁹⁵

As of late 2017, 3G service continued to be unavailable in southern Somalia, impeding the everyday activities of individuals, aid agencies, and humanitarian organizations alike. According to one interviewee, emergency services may be difficult to reach during a disruption, causing delays that diminish a patient's chances of survival or recovery. Violence amid a digital information blackout is difficult to objectively measure, track, and address, as are the needs and mobility patterns of any affected populations. Timely and accurate crisis communication is key in natural disasters, which can disrupt digital information flows on a massive scale. However, as of late 2017, no known political network disruption coincided with a natural disaster.

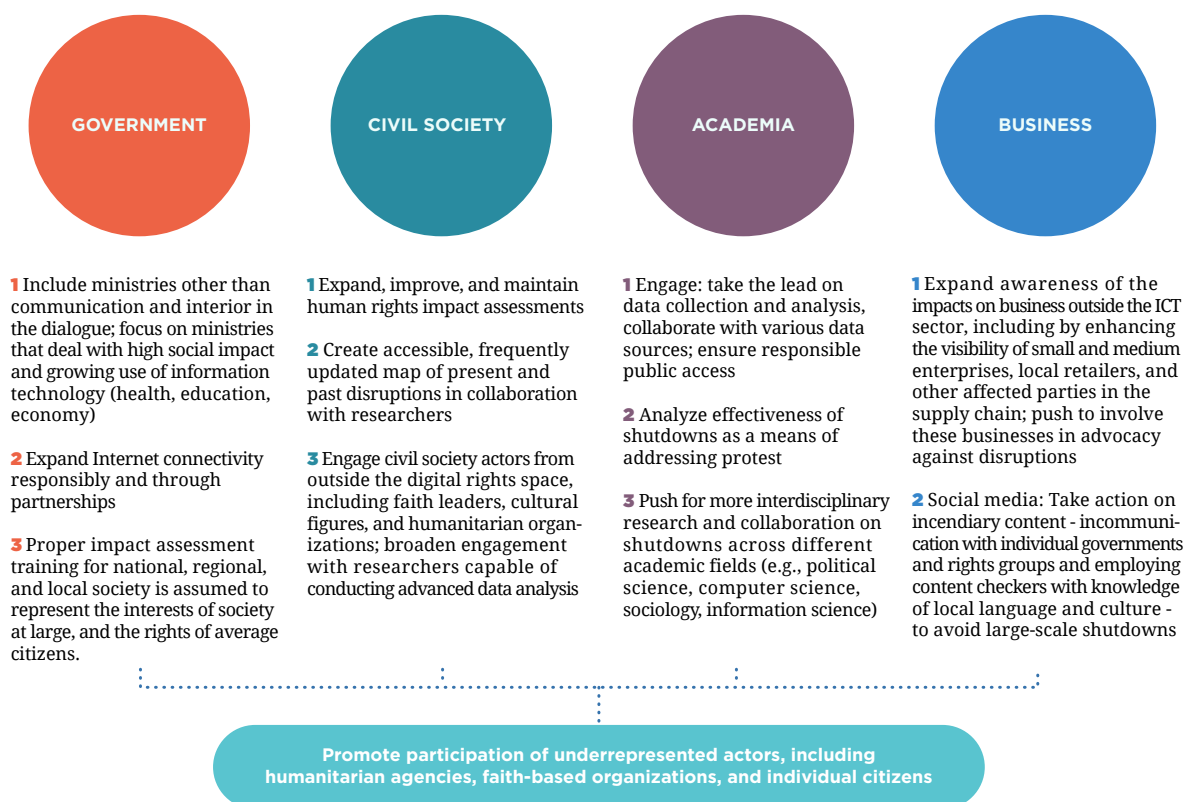


...network disruptions interrupt communication between family members caught in the fog of war, trying to escape the violence



RECOMMENDATIONS: AN INTEGRATED APPROACH

Shutdowns remain prevalent in spite of the efforts of civil society, the corporate world, and academia to highlight and counteract their impact. In India, the total number of shutdowns in April 2018 already exceeded levels for all of 2016. Despite the success of Access Now's #KeepItOn campaign, new countries continue to disconnect communication, often under the unverified assumption that such a measure is effective at ensuring public safety. This report highlights opportunities to engage new actors and angles of discussion. **For shutdowns to subside, advocates must demonstrate that these actions are both ineffective and prohibitively expensive.** Advocacy campaigns must use clear, measurable evidence to illustrate the counterproductive consequences of shutdowns for all human rights, stakeholders, and social and economic sectors (figure 9).⁹⁶



9

BROADEN THE SCOPE OF HUMAN RIGHTS IMPACTS ASSESSMENTS

As stated in section 3 of this report, the range of human rights impacts of network disruptions is quite broad. While advocacy on this issue focuses on the immediate civil and political rights impacted by disruptions, and research has allowed all actors to better understand and call attention to the economic impacts, more can be done to underline other lasting impacts on human rights. For instance, there is a dearth of both data and individual accounts regarding the repercussions of shutdowns in the area of health care. Similarly, humanitarian agencies and organizations have not taken vocal stances on the harms they experience from network shutdowns disruptions to their workflows, logistical difficulties, and risks to the well-being of vulnerable populations. On an international level, Access Now is at the forefront of the initiative to collect testimonies from individual events. These efforts must be supported

and expanded to include local NGOs, which are well positioned to gather both broad statistical evidence and individual accounts.

Despite the encouraging steps taken by the UN Human Rights Council and other institutions, many governments still do not see access to digital communication as a human right. Hence, future efforts should incorporate the language of broadly accepted human rights treaties and draw attention to the impact of network disruptions on rights such as freedom of association, assembly, and religious belief.

By making these impacts more clear, advocates can broaden the range of CSOs, companies, and investors who may advocate around network disruptions and raise awareness with decisionmakers. In particular, it is important to engage and involve businesses from outside the ICT sector, along with civic leaders whose primary focus may not be digital rights (e.g., faith leaders, cultural figures, and humanitarian organizations).

IMPROVE AND EXPAND DATA COLLECTION EFFORTS

Nearly all of the interviewees agreed that data collection on various aspects of network disruptions must be improved and expanded. Here are some examples of existing data collection efforts:

- **Access Now**'s meticulous reporting via their #KeepItOn campaign, their Shutdown Stories project (individual testimonies from shutdowns, largely submitted by local volunteers and activists on the ground), and their Shutdown Tracker Optimization Project (STOP) aggregate valuable information about disruptions in the form of a spreadsheet file.
- **SFLC**'s Internet shutdowns tracker maps past and current disruptions across India on a state-by-state level.
- **Bytes for All**'s KillSwitch.pk tracks and reports on shutdowns in Pakistan (but does not yet map them).
- Network measurements by Oracle's **Internet Intelligence** (formerly Dyn Research) and **Akamai**'s State of the Internet project.
- Explorer from the **OONI**, a division of the Tor Project, uses measurements collected since 2012 to detect various kinds of website blocking, censorship, surveillance, and traffic manipulation. Users can contribute by installing an ooniprobe.
- **Google**'s Transparency Report includes a real-time graph charting Internet traffic in each country with a high level of precision.
- The Internet Outage Detection and Analysis (IODA) project from **CAIDA** is an experimental effort to aggregate a variety of measurements to identify Internet disruptions.
- **GNI**'s Principles on Freedom of Expression and Privacy, as well as its Country Legal Frameworks on Freedom of Expression and Privacy in Telecommunications, contain critical guidelines for operators in challenging regulatory environments and compile information about relevant national laws.⁹⁷

Other sources of raw data include the Route Views Project, the RIPE network, and Measurement Lab (M-Lab). Organizations such as Internet Sans Frontières, Paradigm Initiative, and CIPESA have also conducted important work at the intersection of research and advocacy.

Many of these initiatives were developed or extended in the last two years. While they have significantly deepened our knowledge about network disruptions, the space for expansion is vast. Multiple measurement experts interviewed and/or consulted for this report agreed that traffic data at a more granular, subnational level of analysis (e.g., city or administrative region) would be beneficial. For instance, since the January 2017 Cameroon shutdown was limited to two regions, the change in the country's cumulative activity registered in Google's traffic tool was minimal. The increasing frequency and sophistication of localized shutdowns warrant a more in-depth approach to data collection. According to interviewees, the areas that require more attention include more accurate data on the scope of each shutdown, the protest activity generated (or stifled) by each incident, the large-scale human impact of disruptions beyond isolated examples, and data that distinguishes between mobile and fixed Internet traffic.⁹⁸ Furthermore, fine-grained mapping of affected areas is not currently available for any country other than India. The Center for Communication Governance at National Law University in Delhi has been tracking disruptions in India since 2013, identifying several cases from as early as 2010 and reporting

them publicly in the earliest known effort to produce precise data on the topic in India.⁹⁹ SFLC maintains a popular platform (InternetShutdowns.in) where disruptions are mapped subnationally using an interactive map that covers India's 36 states and union territories. Applying this model to other countries would allow researchers, civil society, and the public to better visualize the scope of each disruption.

Although the three existing reports on the economic impact of shutdowns are excellent contributions that fill an important gap in current knowledge, these models must be continually used and improved should countries continue to experience large-scale disruptions.

Academics and researchers should take steps to disseminate new data collection and analysis efforts through peer-reviewed academic journals. While network shutdowns justifiably prompt a scramble to report the details of each incident in the press and social media, this should be balanced by cross-disciplinary research on the topic, buttressed by rigorous review. This applies to the social sciences in particular, as very few studies in political science and sociology focus on disruptions to connectivity as a form of digital repression.¹⁰⁰ Both statistical work on the cross-national ramifications of disruptions and case studies are needed. This is a promising space for collaboration between academia, NGOs, and tech companies.

Despite the encouraging steps taken by the UN Human Rights Council and other institutions, many governments still do not see access to digital communication as a human right.

It is imperative to carry out more in-depth research on the effectiveness of network disruptions as a strategy of stifling protest and opposition. Further proof that disruptions can backfire, expanding unrest and other public expressions of outrage, would provide activists with a powerful argument against the primary justification for shutdowns. Conversely, the opposite finding could catalyze CSOs and encourage them to raise awareness on the importance of public dissent when communication is uprooted.

Overall, researchers would benefit greatly from more precise data to carry out objective, independent studies. Investors and companies would acquire valuable and accurate insight on the financial, technological, and social risks of entering a volatile market. CSOs would be better equipped to coordinate their activities on the ground and would gain from the interconnectedness of the human rights and economic impact narratives.

SUPPORT RESPONSIBLE PARTNERSHIPS TO EXPAND CONNECTIVITY

The author's statistical research tentatively suggests that certain network interferences begin to wane once Internet connectivity reaches a certain threshold. This finding must be corroborated through review and a separate study covering a narrower definition of interference (large-scale disruptions) between 2011 and 2018. The results of this research and rising Internet penetration may compel governments to reevaluate shutdowns as a valid strategy in the quest for security. Similarly, cell phones are ubiquitous in many of the countries that have experienced deliberate disruptions. The convergence of both technologies may further discourage governments from executing shutdowns as awareness of their consequences grows. Technological development brings new infrastructure, new jobs, new sources of revenue, and new opportunities for investment. Governments face a conundrum: letting technology flourish, or restricting and controlling it. Both options may invigorate mass protest, generate social movements, and trigger other forms of collective action. This is known as the "dictator's dilemma" in social science research,¹⁰¹ and it implies that governments will usually favor expanding connectivity. This is because the latter makes the country more competitive on the world stage and brings in revenue that the other option specifically denies. The risk of upheaval, meanwhile, remains comparable.¹⁰²

Thus, homegrown initiatives to ensure Internet and cell phone expansion would be welcome. Responsible partnerships to expand access to communication technology are promising, with benefits for both local and national economies. At each step, care must be taken to ensure responsible consumption and sharing of data in the interest of avoiding the escalation of pre-existing social tensions, to which the rapid spread of information in a newly connected society can ultimately contribute. Partnerships of this kind could involve international, national, and local actors focusing on: 1) negotiating and creating greater provider diversity at the international frontier (thus lowering the ease with which disruptions can be executed), and 2) ensuring sustainable expansion of access without bypassing the fundamental needs of local populations. Such ventures should be carried out with an eye to promoting the UN Sustainable Development Goals, emphasizing the role of local providers and entrepreneurs.

CONDUCT CASE STUDIES

At least one tech company representative advocated for a detailed case study that would cover the complex consequences of shutdown events in a specific country, encompassing both human and economic impact. This study could be conducted in house, outsourced to a consulting firm with deep market insight, or commissioned from academic researchers. India was identified as a promising candidate for such an analysis. India's legal system stipulates a clear separation of powers, and its status as a democracy with a strong tradition of social movements adds important dimensions to the conditions under which shutdowns can occur. It is also deeply mired in the world of technology, with relatively easy access to market data and businesses on the ground for the purpose of conducting research. A robust and popular Right to Information law offers potential insight from government sources. Finally, India has experienced an explosion of government-led disruptions in the past three years, with a very high degree of decentralization (regional shutdowns ordered by state authorities).

This initiative is worth exploring to visualize the extent of the damage shutdowns entail in one particular country and to allow others to extrapolate. It can also be carried out in collaboration with India's rich landscape of CSOs, some of which (DEF, SFLC) are already carefully monitoring the topic.

Telecommunications companies have unique qualities that give them the edge in this conversation. They can rely on the vast technical expertise of their teams to educate governments and raise their awareness regarding the consequences of shutdowns without exerting undue pressure.

ENGAGE DIRECTLY WITH GOVERNMENT ACTORS AND SUPPORT TRAINING

Government actors in different countries are often familiar with some aspects of shutdowns (e.g. technical feasibility, impact, or remedy) but do not understand their full scope. The executive and judicial branches of many governments do not have the training that would provide them with this information. This may lead to disproportionate steps being taken to counter a perceived digital threat.

At least one trade association, two telco representatives, and several representatives of international organizations supported one-on-one engagement and various forms of capacity building for government officials. Most agree that reactive pushback in the moment is not enough. Telcos must have proactive conversations with the government outside of crisis situations, e.g., by discussing the implications of proposed legislation. Telecommunications companies have unique qualities that give them the edge in this conversation. They can rely on the vast technical expertise of their teams to educate governments and raise their awareness regarding the consequences of shutdowns without exerting undue pressure. Furthermore, while reports on the economic cost of shutdowns may reach the highest echelons of a national government, they may not find their way to regional or local decision makers.

It is also important to engage with government actors beyond those directly responsible for disruptions (i.e., ministries of interior and/or telecommunications) to ensure that different viewpoints are reflected and impacts internalized in government decision making. Government actors responsible for social services (health, education), and for economic development are likely to recognize and articulate the disproportionate impacts that disruptions can have.

The multiple WhatsApp shutdowns in Brazil and numerous other cases suggest that individual decision-makers often know little about the fallout of their actions. The judiciary should be an entry point, as it often provides, according to one intergovernmental organization official, "one of the few meaningful safeguards against unbridled executive power." Capacity building should also be provided to different agencies, departments, and ministries, as they often do not reflect a coordinated position regarding disruptions (e.g., Egypt in 2011).

Overall, a combination of one-on-one engagement and collaboration seems to spark the most enthusiasm.



CONCLUSION

Network shutdowns and resistance to them on the part of companies, civil society, and civilians are amorphous and rapidly developing topics. Strategies of controlling information flows online are constantly evolving and create challenges for measurement, even among experts in network security. The proliferation of shutdowns in stable democracies, such as India, is particularly concerning. India's growing role as a regional economic power creates the risk that its approach to information control will be used as a petri dish by other developing countries, which may emulate India's penchant for shutdowns, unless such disruptions are proven ineffective. The breadth of the impacts outlined may also bring

[Tackling network disruptions jointly] will help ensure that these black holes of communication do not become the new normal on a global scale.

new arguments to the debate on shutdowns, focusing on their disproportionate impact on vulnerable populations such as individuals with chronic health conditions, marginalized ethnic groups, and women. All of these groups are affected by a digital divide that shutdowns only perpetuate.

As analysts devise new ways of detecting disruptions and tracing them back to the decisions of specific government entities, others can take action:

- **Activists** can broaden their targets to include other government ministries and reach out to leaders of organizations that have suffered shutdowns silently without a global network to magnify their concerns.
- **Large firms** can bring local businesses into the discussion while social media companies can significantly expand efforts to monitor inciteful speech, regardless of the language.
- **Academics and other researchers** can drive forward data collection and analysis on a largely unexplored topic, work across multiple fields of study, and make the data that underlie their findings publicly available.
- **Governments** can work with actors at various levels to develop capacity building opportunities and expand connectivity while ensuring the spread of false content does not incite violence.

None of these groups can address the problem alone. Multistakeholder engagement on issues related to technology and human rights is a proven approach, which has already been applied to network disruptions and can be expanded upon. This discussion should be held parallel and in coordination with greater engagement on problems like disinformation and hate speech, which are often cited as justifications for network disruptions. Whatever mechanisms are used to counteract the alarming trend of network shutdowns, jointly improving our understanding of this phenomenon will help ensure that these black holes of communication do not become the new normal on a global scale.



ANNEX: HOW ARE DISRUPTIONS TYPICALLY EXECUTED?¹⁰³

Large-scale shutdowns typically take place in one of several ways. This appendix aims to summarize some of the mechanisms underlying these disruptions, including both the orders themselves and the technical components of the communication infrastructure that are usually affected. The dynamics of shutdown orders (often broadly referred to as service restriction orders, or SROs) are discussed in the first section below. The next section outlines some of the known technical aspects of disrupting connectivity on a wide scale, focusing on the withdrawal of routes from the global routing table. Two more subsections outline other modes of disruption (infrastructural damage and throttling). While far from exhaustive, this section provides an introduction to some of the mechanics of network shutdowns.¹⁰⁴

SHUTDOWN ORDERS

Mobile and ISP shutdown orders are an accelerating trend, correlating with the vigorous expansion of cellular networks in developing countries, the falling cost of mobile data, the increased use of social media in emerging markets, and the expansion of submarine and terrestrial fiber networks routing ever-growing volumes of data.¹⁰⁵ As a result of increasing coverage and strong economic growth in lower- and middle-income states, cell phone subscriptions per 100 individuals reached a global average of 101.5 in 2016, surpassing 100 for the first time that year. However, this growing reliance on mobile devices has made them a primary target for intentional disruption in certain countries. MNOs are typically ISPs, i.e., entities that provide Internet access, usually on a subscription basis. Thus, orders to disconnect telecom services often concentrate on mobile data connectivity.

Mobile shutdown orders are issued by regional or national authorities (executive or judicial) to compel network operators to suspend services, often citing a clause in the country's criminal code or communications law.¹⁰⁶ According to several telco representatives, in extreme cases, the order is issued verbally (by phone) to accelerate the process, followed by a written order, which companies commonly request if it is not attached to the initial demand.

In this scenario, while the actual links connecting Internet service providers to the outside world are not necessarily cut, services such as mobile data, specific communication apps (often instant messaging apps, social media, and VoIP services), calls, and/or SMS (texting) are made unavailable. When a specific app is the target of a suspension order, operators are held responsible for blocking access to specific servers that the app relies on, under threat of punishment or penalty (e.g., Zimbabwe in July 2016¹⁰⁷). Suspension of services provided by an app has also been triggered when a government demanded access to communication channeled through the app but company representatives argued that full encryption did not allow them to present this information. In such cases, governments have occasionally moved to completely block the app in light of their own inability to access or restrict individual pieces of content. Several WhatsApp disruptions in recent years have occurred in this context, e.g., in Burundi (April 2015), Morocco (January 2016), Zimbabwe (July 2016), the Democratic Republic of the Congo (August 2017), and, perhaps most prominently, Brazil (December 2015, May and June 2016).¹⁰⁸ Sri Lanka's blocking of Facebook and other platforms in March 2018 was, in turn, the result of official claims of rampant hate speech and its possible links to violence on the ground.

According to several telco representatives interviewed for this report, a shutdown request and/or the law authorizing it may restrict telcos' ability to publicly acknowledge the existence of the disruption. Consequently, there have been calls for greater transparency from civil society, companies, and governments regarding mobile disruption orders, as well as several notable cases where such orders were anonymously leaked (e.g., DRC 2017). Furthermore, several telcos have corporate social responsibility (CSR) protocols in place when the head of the company or subsidiary receives an order to terminate

connectivity or release customer data. This may involve informing telco peers and CSOs of the order. State-run companies and those operating solely within the country in question seem to be less likely to respond to an informal order by requesting legal justification in writing. They are also less likely to engage with global civil society on the matter.

Fixed Internet shutdown orders are occasionally issued in tandem with mobile orders. While the overwhelming majority of service restriction orders targets mobile networks, a small percentage of them also entail the suspension of fixed Internet access. In India, only 10 of the 73 shutdowns registered by SFLC by mid-July 2017 were confirmed to have included fixed-line service offered by certain providers, and none had focused on fixed lines exclusively. DSL broadband access was also limited in recent disruptions in Duraz (Bahrain) in 2016 and Togo in 2017.¹⁰⁹ Disruptions of fixed and leased¹¹⁰ lines are less common than mobile data shutdown orders, possibly given government offices' dependency on the former.

TECHNICAL ASPECTS OF LARGE-SCALE SHUTDOWNS

In order to understand some of the technical means that are used to execute shutdowns, we must first briefly describe some of the network architecture that governments disrupt. Global Internet traffic is routed by the **Border Gateway Protocol (BGP)**. Manipulating or hijacking BGP routes can significantly disrupt Internet access in a country and inflict collateral damage outside its borders. The BGP acts as a road map to **autonomous systems (AS)** and their respective identifying numbers (ASNs).¹¹¹ An autonomous system is a self-contained collection of routers that groups one or more blocks of IP addresses (prefixes) under (typically) a single operator. Operators (companies or their branches, groups of companies, universities) determine a routing protocol, akin to directing traffic among nodes in the Internet. Routing protocols provide routers with information on the topology of their network. BGP routers can announce routes (make changes to existing routes or create new routes) or withdraw them, informing receivers that the routes in question no longer exist. BGP routers continually exchange routing tables consisting of all of their active routes. The receiving router incorporates new information from its neighbor into its routing table.¹¹² BGP routes are responsible for directing international traffic to and from a country. The number of routes differs by country.¹¹³

As a network, BGP is founded on trust. The information transmitted through it is generally believed to be accurate. Consequently, both deliberate and unintentional disruptions can have broad impact zones.¹¹⁴ When ISPs receive a shutdown order, they typically withdraw routes from the global routing table. Internet performance services use BGP analysis to investigate incidents in which BGP routes are withdrawn. Manipulating routing tables allows an ISP to send IP addresses down a path to nowhere, much like fabricating a map with false trails and dead ends. BGP routes to a country's IP space thus disappear from its upstream providers, culminating in a large-scale shutdown. This is commonly called a **BGP outage**. During the Arab Spring, for instance, Egypt initially withdrew about 3,500 routes, accounting for 88 percent of Egypt's Internet traffic, while Libya briefly withdrew all 14 of its own, supplementing the process with satellite signal jamming and packet filtering.¹¹⁵ A cascading or simultaneous series of withdrawals by multiple ISPs signals a likely explicit order issued to these providers.

The number of **border providers** in each country contributes to a country's risk of disconnection. Border providers are domestic network providers (i.e. ASes) with direct connections to international providers.¹¹⁶ The more of these entities exist in a country, the greater the network's overall resilience — and resistance to large-scale shutdowns. Additional risks include the centralization of institutional power in a state-run telecom (e.g., in Ethiopia), a laissez-faire approach of central governments to regional security (e.g., shutdowns implemented by state governments in India), and a limited number of fiber links carrying traffic internationally.

It is important to note that erratic network behavior can be caused by other processes that result from interference with BGP routing. Inadvertent misconfigurations can result in **routing leaks**, i.e., illegitimate announcements of blocks of IP addresses. Traffic is then often diverted and sent through the misconfigured router, which may cause widespread instability in critical services if providers propagate it without validation.¹¹⁷ Route hijacks, BGP hijacks, and BGP man-in-the-middle attacks are all related categories of incidents, but differ from route leaks in malicious intent. Governments sometimes use hijacks to enforce censorship regulations or block a service. This, however, may extend the disruption beyond country borders, as was the case when Pakistan attempted to block YouTube domestically in 2008.¹¹⁸

SABOTAGE OF INFRASTRUCTURE AND CABLE CUTS

In very specific instances, access to networks can be disrupted by shutting down traffic at a cable landing or via physical damage to cables. The government of Iraq, for example, shut down access to the Internet at the Gulf Bridge International (GBI) cable landing and a terrestrial waypoint on the Iraqi-Jordanian border in 2013.¹¹⁹ Armed groups have occasionally forced disruptions by cutting or bombing cables (e.g. Libya in 2013¹²⁰), and a 2014 incident involving the Shabwa cable in Yemen was attributed by national media to a conflict with local tribesmen.¹²¹ However, the inherent resilience of the Internet renders this tactic futile in many cases, particularly when the infrastructure that provides the country with Internet access extends beyond a single access point. For cable damage to trigger an outage on the national level, all of the terrestrial and submarine cables that provide international connectivity to the country have to be cut simultaneously.¹²² Governments almost never intentionally damage the Internet's support infrastructure in the country, as such a tactic would quickly prove self-defeating.

However, governments do occasionally use cable damage to justify severe disruptions, not always providing evidence for these claims. For instance, in June 2017, the administration of Denis Sassou Nguesso in the Republic of the Congo claimed accidental cable damage caused by a shipping vessel had severed the country's connection through the West Africa Cable System (WACS) (parliamentary elections were to be held the following month.)¹²³ Similarly, following the ouster of Zimbabwean President Robert Mugabe in November 2017, twin cable cuts reportedly brought down most of Zimbabwe's connectivity, additionally affecting that of Zambia and the DRC, in early December. MNOs attributed the outages in both Congo and Zimbabwe to accidents, and this explanation has been corroborated by Internet performance analysts. The same defense has been used by the Syrian government in that country's civil war, typically without external corroboration. Damage to infrastructure is often difficult to verify given the use of government vessels to conduct inspections and repairs. This can create confusion during armed conflicts and enable governments to falsely attribute disruptions to technical faults.

Deliberate, coordinated targeting of one or multiple cables is not generally considered a feasible strategy in international conflict. Nonetheless, states that rely on a small number of 'chokepoint' cables or contain a high concentration of cables that serve as hubs for international connectivity also constitute areas of heightened risk.¹²⁴

BANDWIDTH THROTTLING

Throttling refers to the intentional slowdown of network traffic, sometimes to the point where it is rendered unusable. As of late 2017, throttling has been used in at least ten countries: Bahrain, China (in the Tibet Autonomous Region), Gabon, India, Iran, Iraq, Myanmar, Syria, Turkey, and Uzbekistan.¹²⁵ Turkey is the state actor that perhaps most prolifically resorts to throttling, which has occurred during or in the wake of, protests, terrorist attacks, violent clashes, and the July 2016 coup attempt.¹²⁶ Iran rolled out similar measures to stifle electoral protest or anticipate it ahead of key dates (e.g., the anniversary of the Islamic Revolution and of the contested 2009 Presidential election).¹²⁷

OONI regularly investigates disruptions via throttling. A particularly prevalent method is **packet dropping**, in which packets of data sent across a network fail to reach their destination. OONI has identified the throttling of encryption protocols in Iran in conjunction with sensitive occasions such as protests and elections, as well as similar incidents in Egypt and Turkey.¹²⁸

As a censorship measure, throttling is more sophisticated in execution, but less dramatic in scope and potential consequences. It is also less detectable by outside parties and offers more flexibility for communication among government and security actors, as vital communication links remain open.

Beyond the measures mentioned above, governments often impose more targeted restrictions to access, including IP blocking, DNS filtering and redirection, URL filtering, or any combination thereof. Researchers and activists are also detecting emerging patterns of DDoS attacks by governments, particularly during periods of political contention such as elections. These measures can be interpreted as censorship, but they generally do not fulfill the inclusion criteria of a shutdown as framed in this report, and they do not always aim to undermine multilateral communication, coordination, and organization.

EXTERNAL RESOURCES

- Anderson, C. (2013). Dimming the Internet: Detecting throttling as a mechanism of censorship in Korea. Retrieved from <https://arxiv.org/abs/1306.4361>.
- Asal, V., J. Mauslein, A. Murdie, J. Young, K. Cousins, and C. Bronk (2016). Repression, education, and politically motivated cyberattacks. *Journal of Global Security Studies*, 1(3), 235-247.
- Audu, O. (2013). Borno residents want phone network restored as Boko Haram gets deadlier. *Premium Times*. Retrieved from <https://www.premiumtimesng.com/news/145640-borno-residents-want-phone-network-restored-boko-haram-gets-deadlier.html>.
- Aydin, D. (2016). The laws that let internet shutdowns happen. *Access Now*. Retrieved from <https://www.accessnow.org/laws-let-internet-shutdowns-happen/>.
- Balakrishnan, H. (2009). Wide-area Internet routing. Overview paper. Massachusetts Institute of Technology. Retrieved from <http://web.mit.edu/6.033/2017/wwwdocs/papers/InterdomainRouting.pdf>.
- Bariyo, N. (2015). Democratic Republic of Congo extends internet blockage. *Wall Street Journal*. Retrieved from <http://www.wsj.com/articles/congo-blocks-internet-access-amid-protests-against-president-kabila-1421938042>.
- Belson, D. (2017). The migration of political internet shutdowns. *Oracle Internet Intelligence*. Retrieved from <https://blogs.oracle.com/internetintelligence/the-migration-of-political-internet-shutdowns>.
- Brown, M. A. (2008). Pakistan hijacks YouTube. *Renesys Blog*, February 24. Retrieved from <https://dyn.com/blog/pakistan-hijacks-youtube-1/>.
- Bushell-Embling, D. (2017). Viettel plans to expand to Indonesia, Nigeria. *TelecomAsia*. Retrieved from <https://www.telecomasia.net/content/viettel-plans-expand-indonesia-nigeria>.
- Cakebread, C. (2017). Google received a record-breaking number of government data requests. *Business Insider*. Retrieved from <http://www.businessinsider.com/google-reports-record-number-of-government-data-requests-chart-2017-9>.
- Carter, B. L. (2017). Something is happening in Congo-Brazzaville. *African Arguments*. Retrieved from <http://africanarguments.org/2017/06/20/something-is-happening-in-congo-brazzaville/>.
- CCG [Center for Communication Governance] (2018). Incidents of Internet shutdown in India (2010 onwards). Retrieved from <https://drive.google.com/file/d/0BwkVG7IkYz7Ac0ZMZMHhCeUc3Nkt0d0U4cURvY0hRTkxLY3pj/edit>.
- Chaabane, M. (2017). Les sujets du bac publiés sur Facebook, une demi-heure après le démarrage des épreuves. *Webdo.tn*. Retrieved from <http://www.webdo.tn/2017/06/08/tunisie-sujets-bac-publies-facebook-demi-heure-apres-demarrage-de-lepreuve/>.
- CIPESA (2017a). The growing trend of African governments' requests for user information and content removal from internet and telecom companies. *CIPESA Policy Brief*, July 2017. Retrieved from https://cipesa.org/?wpfb_dl=248.
- CIPESA (2017b). A framework for calculating the economic impact of internet disruptions in Sub-Saharan Africa. Retrieved from <https://cipesa.org/2017/09/economic-impact-of-internet-disruptions-in-sub-saharan-africa/>.
- Committee to Protect Journalists (2016). Indian authorities shut down media outlets in Jammu and Kashmir. Retrieved from <https://cpj.org/2016/07/indian-authorities-shut-down-media-outlets-in-jamm.php>.
- Cowie, J. (2013). Iraqi government tries, fails to shut down Internet. *Dyn Research*. Retrieved from <http://research.dyn.com/2013/10/iraqi-government-tries-fails-shut-internet/>.
- Dada, T., & P. Micek (2017). Launching STOP: The #KeepItOn internet shutdown tracker. Retrieved from <https://www.accessnow.org/keepiton-shutdown-tracker/>.
- Dahir, A. L. (2017). Reeling from an internet shutdown, startups in Cameroon have created an "internet refugee camp." *Quartz Africa*. Retrieved from <https://qz.com/942879/an-internet-shutdown-in-cameroon-has-forced-startups-to-create-an-internet-refugee-camp-in-bonako-village/>.
- Dainotti, A., et al. (2011). Analysis of country-wide Internet outages caused by censorship. Presented at Internet Measurement Conference 2011, Nov 2-4, Berlin, Germany.
- Deloitte (2016). The economic impact of disruptions to internet connectivity: A report for Facebook. Deloitte. Retrieved from <http://globalnetworkinitiative.org/sites/default/files/The-Economic-Impact-of-Disruptions-to-Internet-Connectivity-Deloitte.pdf>.

- Dyn Research (2013). Twitter post on Silphium cable attack in Libya. Retrieved from <https://twitter.com/DynResearch/status/375992351925080064>.
- ESAT News (2017). Ethiopia: Regime blocks social media, jams ESAT satellite as protest intensifies. ESAT. Retrieved from <https://ethsat.com/2017/12/ethiopia-regime-blocks-social-media-jams-esat-satellite-protest-intensifies/>.
- Forden, E. (2015). The undersea cable boom in Sub-Saharan Africa. USITC Executive Briefing on Trade. United States International Trade Commission. Retrieved from https://www.usitc.gov/publications/332/executive_briefings/forden_submarine_cables_june2015.pdf.
- Fowler, T. (2015). Why a blanket ban on the Internet in troubled Manipur is not a good idea. Scroll.in. Retrieved from <http://scroll.in/article/753108/why-a-blanket-ban-on-the-internet-in-troubled-manipur-is-not-a-good-idea>.
- Franceschi-Bicchierai, L. (2015). Congo government allegedly shuts off internet service to squash protests. VICE Motherboard. Retrieved from https://motherboard.vice.com/en_us/article/kb7ew9/congo-government-allegedly-shuts-off-internet-service-to-squash-protests.
- Freedom House (2017). Freedom of the Net 2017. Retrieved from <https://freedomhouse.org/report/freedom-net/freedom-net-2017>.
- Gambanga, N. (2016). Here's the Zimbabwean government's warning against social media abuse. TechZim. Retrieved from http://www.techzim.co.zw/2016/07/heres-zimbabwean-governments-warning-social-media-abuse/#.V-7BQ_ArLIU.
- Global Network Initiative (2016a). GNI condemns Election Day shutdowns of social media in Uganda. Global Network Initiative. Retrieved from <http://globalnetworkinitiative.org/news/gni-condemns-election-day-shutdowns-social-media-uganda>.
- Global Network Initiative (2016b). Extremist content in the ICT sector. Research report (November 2016). Retrieved from <http://globalnetworkinitiative.org/sites/default/files/Extremist-Content-and-the-ICT-Sector.pdf>.
- Global Network Initiative (2018a). GNI Principles on freedom of expression and privacy. Retrieved from https://globalnetworkinitiative.org/sites/default/files/GNI-Principles-on-Freedom-of-Expression-and-Privacy_0.pdf.
- Global Network Initiative (2018b). The consequences of network shutdowns and service disruptions: A one-page guide for policymakers. Retrieved from <https://globalnetworkinitiative.org/the-consequences-of-network-shutdowns-and-service-disruptions-a-one-page-guide-for-policymakers/>.
- Gohdes, A. R. (2015). Pulling the plug: Network disruptions and violence in civil conflict. *Journal of Peace Research*, 52(3), 352-367.
- Greenwald, G., & A. Fishman (2016). WhatsApp, used by 100 million Brazilians, was shut down nationwide by a single judge. *The Intercept*. Retrieved from <https://theintercept.com/2016/05/02/whatsapp-used-by-100-million-brazilians-was-shut-down-nationwide-today-by-a-single-judge/>.
- GSMA (2017). The mobile economy: Sub-Saharan Africa 2017. Retrieved from <https://www.gsmainelligence.com/research/?file=7bf3592e6d750144e58d9dcfac6adfab&download>.
- Guled, A. (2017). Somalia's internet returns after 3-week outage caused outcry. *Phys.org*. Retrieved from <https://phys.org/news/2017-07-somalia-internet-week-outage-outcry.html>.
- Hassanpour, N. (2017). *Leading from the Periphery and Network Collective Action*. Cambridge: Cambridge University Press.
- Hern, A. (2017). Ethiopia turns off internet nationwide as students sit exams. *The Guardian*. Retrieved from <https://www.theguardian.com/technology/2017/may/31/ethiopia-turns-off-internet-students-sit-exams>.
- Hindustan Times (2017). Mobile internet to remain suspended in Punjab, Haryana; likely to resume in Chandigarh tonight. *Hindustan Times*. Retrieved from <http://www.hindustantimes.com/punjab/mobile-internet-services-likely-to-resume-in-chandigarh-tonight/story-UGXVgdWetlRJEde4jBJQAN.html>.
- Howard, P. N., S. Agarwal, & M. Hussain (2011). When do states disconnect their digital networks? *The Communication Review* 14 (3): 216-232.
- IHRB [Institute for Human Rights and Business] (2015). *Security v Access: The Impact of Mobile Network Shutdowns. Case Study: Telenor Pakistan*. Institute for Human Rights and Business. Retrieved from <http://www.global.asc.upenn.edu/app/uploads/2015/09/2015-09-Telenor-Pakistan-Case-Study.pdf>.
- Indian Express (2015a). Ban on mobile Internet likely to continue in Ahmedabad. *The Indian Express*. Retrieved from <http://indianexpress.com/article/cities/ahmedabad/ban-on-mobile-internet-likely-to-continue-in-ahmedabad/>.
- Indian Express (2015b). Internet services restored in Ahmedabad at midnight. *The Indian Express*. Retrieved from <http://indianexpress.com/article/india/gujarat/internet-services-to-be-restored-in-ahmedabad-at-midnight/>.
- ITU [International Telecommunications Union] (2017). *The State of Broadband: Broadband Catalyzing Sustainable Development*. ITU / Broadband Commission report. Retrieved from https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.18-2017-PDF-E.pdf.
- Jeffrey, J. (2016). Internet blackout forces young Ethiopians to go retro. *Deutsche Welle*. Retrieved from <http://www.dw.com/en/internet-blackout-forces-young-ethiopians-to-go-retro/a-36490982>.

Karanja, M., M. Xynou, & A. Filastò (2016). How the Ethiopia protests were stifled by a coordinated internet shutdown. Quartz Africa. Retrieved from <http://qz.com/757824/how-the-ethiopia-protests-were-stifled-by-a-coordinated-internet-shutdown/>.

Kedzie, C. (1997). Communication and democracy: Coincident revolutions and the emergent dictators. Washington, DC: RAND.

Krebs, B. (2017). Who is Anna-Senpai, the Mirai worm author? Krebs on Security. Retrieved from <https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author>.

Kuran, T. (1995). Private Truths, Public Lies: The Social Consequences of Preference Falsification. Cambridge, MA: Harvard University Press.

Macha, N. (2016). #ShutDownZim: Will Social Media Protests Drive Zimbabwe to Build a 'Great Firewall'? Global Voices. Retrieved from <https://advox.globalvoices.org/2016/07/11/shutdownzim-will-social-media-protests-drive-zimbabwe-to-build-a-great-firewall/>.

MacKinnon, R. (2012). Consent of the Networked: The Worldwide Struggle for Internet Freedom. New York, NY: Basic Books.

Madory, D. (2017). Telecom heroics in Somalia. Oracle Internet Intelligence blog post. Retrieved from <https://dyn.com/blog/telecom-heroics-in-somalia/>.

Maqbool, M. (2017). Frequent Internet bans are slowly choking Kashmir's online businesses. The Wire. Retrieved from <https://thewire.in/158719/internet-shutdowns-kashmir-business-start-up/>.

Marczak, B. (2016). "Time for some Internet problems in Duraz": Bahraini ISPs impose internet curfew in protest village. Bahrain Watch. Retrieved from <https://bahrainwatch.org/blog/2016/08/03/bahrain-internet-curfew/>.

Margetts, H., P. John, S. Hale, & T. Yasseri (2015). Political Turbulence: How Social Media Shape Collective Action. Oxford: Oxford University Press.

Mawii, Z., R. Srivastava, S. Lal, & B. P. Abraham (2018). Kept in the dark: Social and psychological impacts of network shutdowns in India. Digital Empowerment Foundation. Retrieved from <http://defindia.org/wp-content/uploads/2018/02/Kept-in-the-Dark.pdf>.

Micek, P. & D. Olukotun (2016). Internet Disrupted in Bahrain around Protests as Wrestling Match Sparks Shutdown in India. Access Now. Retrieved from <https://www.accessnow.org/internet-disrupted-bahrain-around-protests-wrestling-match-sparks-shutdown-india/>.

Mishral, P. (2015). Mobile internet shut down: Over Rs 7000 crore losses to banks in Gujarat. The Times of India. Retrieved from <http://timesofindia.indiatimes.com/city/ahmedabad/Mobile-internet-shut-down-Over-Rs-7000-crore-losses-to-banks-in-Gujarat/articleshow/48760311.cms>.

Ngassa, S. (2017). The damage caused by the 93-day Internet blackout in Cameroon. Slate Future Tense. Retrieved from http://www.slate.com/blogs/future_tense/2017/08/17/the_damage_caused_by_cameroon_s_93_day_internet_blackout.html.

Onuch, O. (2014) Social Networks and Social Media in Ukrainian 'Euromaidan' Protests. The Washington Post. Retrieved from <https://www.washingtonpost.com/news/monkey-cage/wp/2014/01/02/social-networks-and-social-media-in-ukrainian-euromaidan-protests-2/>.

Owono, J. (2016). Internet bandwidth limited by the government in Gabon? Internet Sans Frontières. Retrieved from <https://internetwithoutborders.org/fr/internet-bandwidth-limited-by-the-government-in-gabon/>.

Raj, R. (2015). Mobile Internet & SMS services ban in Gujarat disrupts startup ecosystem in the State. Inc42. Retrieved from <https://inc42.com/buzz/mobile-internet-ban-affects-startups-gujarat/>.

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

Maigron, P. (2017). Regional Internet Registries Delegations / ASN Statistics. Retrieved from https://www-public.tem-tsp.eu/~maigron/RIR_Stats/RIR_Delegations/World/ASN-ByNb.html.

Mauldin, A. (2017). Frequently asked questions: Submarine cables 101. TeleGeography. Retrieved from <http://blog.telegeography.com/frequently-asked-questions-about-undersea-submarine-cables>.

PRI (2013). Pakistanis question government's use of bans on cell phones, other tech. PRI's The World. Retrieved from <https://www.pri.org/stories/2013-01-03/pakistanis-question-governments-use-bans-cell-phones-other-tech/>.

Prince, M. (2012). How Syria turned off the Internet. Cloudflare blog. Retrieved from <https://blog.cloudflare.com/how-syria-turned-off-the-internet/>.

Qureshi, A. (2017). The new normal of living with no Internet in Kashmir. Feminism in India. Retrieved from <https://feminisminindia.com/2017/06/06/living-no-internet-kashmir/>.

Ravelo, J. L. (2014). Some aid groups affected by mobile Internet shutdown in Somalia. Devex. Retrieved from <https://www.devex.com/news/some-aid-groups-affected-by-mobile-internet-shutdown-in-somalia-82875>.

RIPE NCC [RIPE Network Coordination Centre] (2017). RIPEstat country routing statistics. Retrieved from <https://stat.ripe.net/widget/country-routing-stats>.

Rogoff, Z., & A. Li (2017). Dispatches from an internet shutdown – Togo. Acces Now. Retrieved from <https://www.accessnow.org/dispatches-internet-shutdown-togo/>.

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

Rydzak, J. (2016). Now Poland's government is coming after the Internet. *Foreign Policy*. Retrieved from <https://foreignpolicy.com/2016/06/10/now-polands-government-is-coming-after-the-internet/>.

Singel, R. (2011). Report: Egypt shut down Net with big switch, not phone calls. *Wired*. Retrieved from <https://www.wired.com/2011/02/egypt-off-switch/>.

SFLC [Software Freedom Law Centre] (2018). Internet Shutdown Tracker – India (2012-2018). Retrieved from <https://internetshutdowns.in/>.

Starosielski, N. (2015). *The Undersea Network*. Durham, NC: Duke University Press.

Steinert-Threlkeld, Z. C., D. Mocanu, I. Vespignani, & J. Fowler (2015). Online social networks and offline protest. *EPJ Data Science* 4:19.

Telecommunications Industry Dialogue (2015). Democratic Republic of the Congo: Legal frameworks pertaining to freedom of expression and privacy in telecommunications. Retrieved from <https://www.telecomindustrydialogue.org/resources/drcongo/>.

Telenor Group (2015). Authority requests for access to electronic communication – legal overview. Myanmar Country Report. Telenor Group. Retrieved from http://www.telenor.com/wp-content/uploads/2015/05/GOVERNMENT-ACCESS-REPORT_05.pdf.

The Citizen (2016). Internet remains cut in Chad after tense elections. The Citizen (Tanzania). Retrieved from <http://www.thecitizen.co.tz/News/Internet-remains-cut-in-Chad-after-tense-elections/-/1840340/3156880/-/1331m1f/-/index.html>

Times of India (2016). To beat exam cheats, Gujarat to block mobile internet today. The Times of India. Retrieved from <http://timesofindia.indiatimes.com/india/To-beat-exam-cheats-Gujarat-to-block-mobile-internet-today/article-show/51173461.cms>.

Tucker, J. A., J. Nagler, M. MacDuffee Metzger, P. Barberá, D. Penfold-Brown, and R. Bonneau (2016). Big data, social media, and protest: Foundations for a research agenda. In Alvarez, M. R. (ed.) *Computational Social Science: Discovery and Prediction*. Cambridge: Cambridge University Press.

Tufekci, Z. (2017). *Twitter and Tear Gas: The Power and Fragility of Networked Protest*. New Haven & London: Yale University Press.

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

UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 30 March 2017, A/HRC/35/22, paragraphs 31, 49, and 79, retrieved from: <http://undocs.org/A/HRC/35/22>

United Nations General Assembly Human Rights Council (2016). The Promotion, protection and enjoyment of human rights on the Internet, A/HRC/32/L.20, 30 June 2016. Retrieved from https://www.article19.org/data/files/Internet_Statement_Adopted.pdf.

Vargas-León, P. (2016). Tracking Internet shutdown practices: Democracies and hybrid regimes. In F. Musiani, D. L. Cogburn, L. DeNardis, & N. S. Levinson (Eds.). *The Turn to Infrastructure in Internet Governance*. New York: Palgrave Macmillan, 167-188.

Weidmann, N. B., Benitez-Baleato, S., Hunziker, P., Glatz, E., & Dimitropoulos, X. (2016). Digital discrimination: Political bias in Internet service provision across ethnic groups. *Science*, 353(6304), 1151-1155.

West, D. (2016). Internet shutdowns cost countries \$2.4 billion last year. Washington, D.C.: Brookings Institution. Retrieved from <https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf>.

West, S. M. (2015). Worrying trend of internet shutdowns in countries with limited connectivity. Electronic Frontier Foundation. Retrieved from <https://www.eff.org/deeplinks/2015/06/worrying-trend-shutting-internet-access-countries-limited-connectivity>.

Wilson, S. L. (2015). How to Control the Internet: Comparative Political Implications of the Internet's Engineering. *First Monday*. Retrieved from <http://firstmonday.org/ojs/index.php/fm/article/view/5228/4204>.

World Bank (2016). *World Development Report 2016: Digital Dividends*. Washington, D.C.: The World Bank.

World Bank (2017). *Migration and remittances: Recent developments and outlook*. Migration and Development Brief 27. Washington, DC: IBRD / The World Bank.

Yaacoub, K. (2016). Algeria reconsiders blocking social media to prevent cheating on exams. SMEX. Retrieved from <http://www.smex.org/algeria-reconsiders-blocking-social-media-to-prevent-cheating-on-exams/>.

Xynou, M., A. Filastò, M. Alimardani, S. Kouhi, K. Bowen, Vmon, & A. Sabeti (2017). Internet censorship in Iran: Network measurement findings from 2014-2017. Open Observatory of Network Interference (OONI).

Yaguez, B. R. (2017). How throttling Internet has become a way of censorship in Turkey. Journalism Festival Web Magazine. Retrieved from <http://magazine.journalismfestival.com/how-throttling-internet-has-become-a-way-of-censorship-in-turkey/>.

Yemen Times (2014). Tribesmen sabotage Internet cable in Shabwa. Yemen Times. Archived at <https://www.thefreelibrary.com/Tribesmen+sabotage+Internet+cable+in+Shabwa.-a0367494794>.

Young, L. E. (2016). Did protests in Zimbabwe really go from 'tweets to streets'? The Washington Post. Retrieved from <https://www.washingtonpost.com/news/monkey-cage/wp/2016/07/15/did-recent-protests-in-zimbabwe-really-go-from-tweets-to-streets/>.

ENDNOTES

- 1 However, it is not a golden key. The Google tool's methodology represents the ratio of a country's traffic to global traffic at any given moment. This means that smaller-scale local and regional disruptions will not be clearly highlighted in the traffic charts, and caution must be exercised in interpreting the sudden drop-offs that do appear.
- 2 Available at <https://globalnetworkinitiative.org/gni-id-statement-network-shutdowns/>.
- 3 Deloitte (2016).
- 4 Global Network Initiative (2018b).
- 5 This definition draws from and mirrors (to some extent) digital rights organization Access Now's definition of the term "Internet shutdown": "an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information." However, it differs in a number of respects. First, it avoids using the term "Internet shutdown," as the disruptions in question may cover other forms of communication (e.g., cell phone service) in addition to the internet, and do not always constitute full communication blackouts (e.g., throttling or disabling only some autonomous systems). Second, it does not include language on the purpose of the disruption, as disruptions can plausibly serve multiple purposes. With that said, the available universe of cases does confirm that controlling the flow of information is a top priority for governments and other actors in disrupting digital communication.
- 6 Dada & Micek (2017). Several additional cases have been documented since then.
- 7 Accurately estimating the total number and duration of shutdowns is difficult due to widely varying measurement tools, criteria, detection accuracy, reporting, and governments' transparency regarding each incident. It is highly likely that even the most liberal compilation of disruptions would be incomplete.
- 8 Hern (2017), Micek & Olukotun (2016).
- 9 Rydzak (2016).
- 10 Vargas-León (2016)
- 11 In Turkey, for instance, approximately 116,000 cases of website blocking have been documented since 2008, according to Efe Kerem Sözeri, editor-in-chief of Dekadans.co (Yaguez 2017).
- 12 Asal et al. (2017).
- 13 Krebs (2017).
- 14 Cakebread (2017).
- 15 CIPESA (2017a). Note that these are not removal requests.
- 16 An early example preceding the smartphone era is the July 2005 suicide bombings in London, which were followed by a cell phone signal blackout in the area surrounding the affected Tube station. This measure was roundly condemned in the UK and reflects an approach used more widely in non-democratic countries.
- 17 IHRB (2015).
- 18 Hassanpour (2017).
- 19 Gohdes (2015).
- 20 Belson (2017).
- 21 Howard et al. (2011).
- 22 Rød & Weidmann (2015).
- 23 MacKinnon (2012), Steinert-Threlkeld et al. (2015), Ruijgrok (2017).
- 24 Young (2016), Macha (2016).
- 25 Gambanga (2016). Little work has social media has reined in or accelerated the underlying dynamics of information flows in a country (particularly rumors), and how this contributes to censorship and shutdowns. This is a vital topic, as it highlights the pace of technological change and allows the public and NGOs to understand the social and cultural context of shutdowns.
- 26 Kashmiri journalist Aakash Hassan underscored this point at a conference organized by MediaNama in December 2017: "Nobody takes Internet as a reliable source in Kashmir now because you never know when it will be snapped."
- 27 Howard et al. 2011
- 28 E.g., the expansion of Viettel, Vietnam's military-owned telecommunications company, into developing markets has entailed a rapid buildup of telecom infrastructure, primarily terrestrial cables (see Bushell-Embling 2017). Emerging markets in which Viettel has recently begun operations include Tanzania (2015) and Myanmar (2017), with future expansion to include Nigeria and Indonesia.
- 29 TeleGeography, a leading source of expertise on the subject, estimates that there are 428 submarine cables in operation worldwide as of early 2017 (Mauldin 2017).
- 30 The UN Special Rapporteur on freedom of expression has noted and condemned these threats. See, UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 30 March 2017, A/HRC/35/22, paragraphs 31, 49, and 79, retrieved from: <http://undocs.org/A/HRC/35/22>
- 31 Karanja et al. (2016).

- 32 Madory (2017).
- 33 See, e.g., A/HRC/35/22.
- 34 A useful one-page summary of shutdown impacts, published by GNI, can be found at http://globalnetworkinitiative.org/sites/default/files/Impacts-Shutdowns-Disruptions-EN_0.pdf.
- 35 Freedom of expression is set out in Article 19 of the UDHR and ICCPR; freedom of association in Article 20 of the UDHR and Article 22 of the ICCPR; and freedom of peaceful assembly in Article 20 of the UDHR and Article 21 of the ICCPR.
- 36 United Nations General Assembly Human Rights Council (2016)
- 37 Committee to Protect Journalists (2016)
- 38 Freedom House (2017)
- 39 The Citizen (2015)
- 40 Global Network Initiative (2016a)
- 41 Bariyo (2015)
- 42 Al Jazeera (2016)
- 43 Owono (2016)
- 44 Software Freedom Law Centre (2016), Fowler (2015)
- 45 nuch (2014)
- 46 Tucker et al. (2016)
- 47 Margetts et al. (2015)
- 48 Tufekci (2017)
- 49 Interview with #BringBackOurInternet activist, April 2017.
- 50 Research has called attention to the existence of 'preference falsification' – a situation in which privately held views are self-censored due to the assumption that they do not command enough support among the general public, that they would violate a social norm, or that they would encourage punishment and reprisal (Kuran 1995). The sudden removal of nodes through that facilitate information flows may exacerbate this effect (Tufekci 2017)
- 51 The right to equality before and equal protection under the law is set out in Article 7 of the UDHR and Article 26 of the ICCPR.
- 52 Weidmann et al. (2016)
- 53 Karanja et al. (2016)
- 54 ESAT News (2017)
- 55 Article 18 of the UDHR and the ICCPR articulate the “freedom of thought, conscience, and religion”
- 56 See, e.g., Global Network Initiative, “Extremist Content in the ICT Sector,” November 2016, available at: <http://globalnetworkinitiative.org/sites/default/files/Extremist-Content-and-the-ICT-Sector.pdf> (Global Network Initiative 2016b)
- 57 The right to life, liberty and security of person is set out in Article 3 of the UDHR and Articles 6 and 9 of the ICCPR.
- 58 Hindustan Times (2017).
- 59 Gohdes (2015).
- 60 West (2015)
- 61 Franceschi-Bicchierai (2015)
- 62 Audu (2013)
- 63 Dahir (2017)
- 64 Gabon's 'Internet curfew,' which featured 23 days of nightly shutdowns, is another example.
- 65 A good example of work along these lines is the recent report by GNI member Digital Empowerment Foundation (Mawii et al. 2018)
- 66 Article 25 of the UDHR and Articles 6 and 11 of the ICESCR recognize the right to an adequate standard of living for themselves and their family.
- 67 Singel (2011)
- 68 Mishral (2015)
- 69 Indian Express (2015b)
- 70 Raj (2015)
- 71 Indian Express (2015a)
- 72 Cowie (2013)
- 73 Rogoff & Li (2017)
- 74 World Bank (2016)
- 75 CIPESA (2017b), GSMA (2017)
- 76 GSMA (2017)
- 77 GSMA (2017)
- 78 According to media reports, up to 7,000 of the 14,000 individuals employed in the IT sector in Kashmir lost their jobs in 2016 in the aftermath of a prolonged shutdown implemented in response to the killing of an Islamist militant commander (Maqbool 2017)
- 79 Digital rights organization Bahrain Watch released estimates of the economic costs of a shutdown in the village of Duraz (Bahrain) in the first five months of disruption. The estimate – at least \$265,000 – was based on a back-of-the-envelope calculation of Internet and mobile data penetration and the lowest price of a data plan.
- 80 Deloitte (2016). The study was conducted by Deloitte and commissioned by Facebook.
- 81 West (2016)
- 82 CIPESA (2017b)
- 83 World Bank (2017)
- 84 Article 12 of the ICESCR establishes “the right of everyone to the enjoyment of the highest attainable standard of physical and mental health.
- 85 PRI (2013)
- 86 Guled (2017)
- 87 MediaNama #NAMAPolicy Conference on Impact of Internet Shutdowns, Delhi, December 6, 2017.
- 88 Mawii et al. (2018), pp. 36-40.
- 89 The right to education is set out in Article 26 of the UDHR and Article 13 of the ICESCR
- 90 Qureshi (2017), Jeffrey (2016)
- 91 Robertson, A. (2015). Can online classrooms help the developing world catch up? The Verge. Retrieved from <http://www.theverge.com/2015/2/11/8014563/bill-gates-education-future-of-online-courses-third-world>.
- 92 Ngassa (2017)

- 93 In early 2017, announced new measures to combat cheating in national exams; these measures are to reduce the disproportionate footprint of large-scale Internet disruptions. While these measures are likely to include localized signal jammers and “600 anti-fraud devices that cover all examination centers,” in the most recent round of high school exams, exam questions were photographed, published on Facebook, and solved within the first hour of the exam (Chaabane 2017)
- 94 The right to take part in cultural life and benefit from scientific progress is set out in Article 27 of the UDHR and Article 15 of the ICESCR.
- 95 Ravelo (2014)
- 96 Civil society is assumed to represent the interests of society at large, and the rights of average citizens.
- 97 Global Network Initiative (2018a)
- 98 Email correspondence with a member of OONI (Aug–Sep 2017) and others.
- 99 CCG (2018)
- 100 Exceptions include Hassanpour (2017), Gohdes (2015), and Tufekci & Wilson (2012)
- 101 Kedzie (1997)
- 102 The second implication is that governments will find new modes of information control in ways that do not sacrifice growing connectivity. This trend is widely observable today.
- 103 Many thanks to Arturo Filastò (OOONI) and Doug Mado-ry (Oracle Internet Intelligence) for valuable feedback on this section.
- 104 In some of the instances below, limited Web-based access to online services, as well as access via Virtual Private Networks (VPNs) and anonymity networks such as Tor, remain possible. VPNs and anonymity networks provide an avenue for circumvention during many shutdowns, and the use of these services spikes in the midst of disruption.
- 105 ITU (2017). For instance, the inauguration of the West Africa Cable System (WACS) in 2012 was followed by spikes in connectivity as multiple West African countries supplemented the single existing undersea fiber-optic connection with a system that offered more than five times the capacity provided by the older, tenuous link. Vastly increased bandwidth led to price drops in costs of monthly access and stimulated the telecommunications market. Elsewhere, new undersea cables have prompted the growth of intercity and cross-border networks (e.g., in Tanzania) (Forden 2015)
- 106 Telecommunications Industry Dialogue (2015), Aydin (2016). The mere existence of specific regulations does not seem to curb the precipitous pace of shutdowns. In August 2017, for instance, India’s Ministry of Communications issued rules outlining new procedural requirements for a shutdown to be put in place. Among others, these guidelines restrict the authority to order a shutdown to a small number of state- or national-level officials, and introduce boards of civil servants reviewing these orders. By April 2018, however, the number of shutdowns in India had already surpassed the total for all of 2016 and exceeded half the total for 2017 (SFLC 2018)
- 107 Young (2016)
- 108 Greenwald (2016)
- 109 Marczak (2016), Rogoff & Li (2017)
- 110 Leased lines are sometimes used by businesses and government entities to connect distant offices.
- 111 As of late 2017, there are more than 82,000 autonomous systems in the world; however, there is no one-to-one geographical correspondence between ASs and national borders. Thus, a single ASN can, in the case of some large companies, announce prefixes in multiple countries. ASNs are vital in identifying paths via BGP.
- 112 Balakrishnan (2009)
- 113 Maignon (2017)
- 114 E-mail correspondence with Arturo Filastò, November 2017
- 115 Dainotti et al. (2011)
- 116 Belson (2017)
- 117 Major incidents of this kind have occurred consistently over the last several years, recently disrupting the Internet for millions of users in Japan (August 2017) and the U.S. (November 2017). Several other countries were affected by the second incident.
- 118 Brown (2008)
- 119 Cowie (2013)
- 120 Dyn Research (2013)
- 121 Yemen Times (2014)
- 122 Prince (2012)
- 123 Carter (2017)
- 124 Starosielski (2015). In addition, unconventional methods such as intercepting fuel or energy deliveries are sometimes reported, albeit very rarely. Only non-governmental actors are known to have used this method.
- 125 Anderson (2013), Dada & Micek (2017), Yaguez (2017).
- 126 Yaguez (2017)
- 127 Anderson (2013)
- 128 Xynou et al. (2017)