International Journal of Communication 14(2020), 4327–4342 1932–8036/20200005

A Spectrum of Shutdowns: Reframing Internet Shutdowns From Africa

ELEANOR MARCHANT[1]
NICOLE STREMLAU[2]
University of Oxford, UK

This article explores the prevailing ways Internet shutdowns are currently understood and makes the case for a new conceptualization—one that recognizes the inherent diversity of cases and how and why they are employed. To do so, we focus on Internet shutdowns in Africa, drawing on data collected during our ongoing research into the politics and practice of social media and conflict in Africa. Though Africa is not the only continent on which Internet shutdowns are taking place, it provides a landscape where the presence of various alternative versions of shutdowns produces important reactions and policy outcomes. A spectrum approach allows for more nuanced conceptualization rather than thinking of shutdowns as a homogeneous technique. This recognizes the variations—both subtle and extreme—among different aspects of Internet shutdowns, including their frequency, duration, breadth, depth, and speed. It also helps to situate this practice more clearly within the wider landscape of other approaches to censorship and offers indications as to how Internet shutdowns might evolve in the future.

Keywords: Internet shutdown, social media, Internet policy, Africa, hate speech, misinformation

What actually constitutes an Internet shutdown, and how to identify one in practice, can be deceptively complex and far more varied than most prevailing definitions indicate, as the articles in this Special Section have explored.[3] The main advocacy organizations involved in drawing attention to Internet shutdowns have taken the lead in defining them and tend to adopt categorical definitions, drawing a stark line between what they are and what they are not. For example, Access Now defines an Internet shutdown

Eleanor Marchant: eleanor.marchant@csls.ox.ac.uk
Nicole Stremlau: nicole.stremlau@csls.ox.ac.uk
Date submitted: 2020–04–06

[1] This research has been funded by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation program (Grant Agreement No. 716686, ConflictNET).
[2] Nicole Stremlau is also with the University of Johannesburg, South Africa.
[3] The technical processes behind how shutdowns are implemented, including switching off critical exchange points or changing routing tables, have been extensively outlined elsewhere (Internet Society, 2019b; Wolchover, 2011).

as "an *intentional* disruption of *Internet or electronic communications*, rendering them inaccessible or *effectively unusable*, for *a specific population* or within *a location,* often to exert control over the flow of information" (Taye & Access Now, 2019, sec. 1.1, para. 1, emphasis added). Other definitions from the Internet Society (2019a) and the Software Freedom Law Centre, India (2019), which tracks Internet shutdowns in India, emphasize similar characteristics, but also refer to the government as the primary perpetrator and the closing off of the Internet as a whole (as opposed to certain platforms or websites). These definitions can be helpful for identifying cases, but they also suggest significant ambiguity about how information flows and Internet infrastructures are understood by different stakeholders.

This ambiguity is amplified by the ways in which related terms—like blackouts, disruptions, Internet kill switches, or network shutdowns—are often used interchangeably. As a result, some scholars have chosen to adopt other terms, intentionally avoiding the ambiguity debate around Internet shutdowns. For example, Rydzak (2019) and Purdon, Ashraf, and Wagner (2015) use the term "network shutdown" to include bans on social media networks but exclude more targeted censorship, like individual website filtering, in their analyses. In this piece, we take a different approach, engaging with the ambiguity to better understand and account for the diversity of causes, effects, and perceptions around Internet shutdowns. This reveals a great deal about the nature of the blunt instruments that are various forms of shutdowns and the diversity of ways that they might evolve in the future.

We begin by interrogating definitions of Internet shutdowns, arguing for a conceptualization of shutdowns along a spectrum rather than as a homogenous technique or a single event. This spectrum approach builds on the definitional work done by advocacy organizations, but rather emphasizes the diversity of how and why shutdowns are employed and experienced, laying the groundwork for future conversations about the nature of shutdowns and their relationship to other forms of censorship.

The article then introduces elements such as the frequency, duration, breadth, depth, and speed of access to information and the modes of communication that contribute to a spectrum approach. Considering these factors encourages debate along the boundaries of what shutdowns are, what their impact is, and how they fit into the wider landscape of other related activities, such as censorship and the curtailment of media and Internet freedoms.

A spectrum approach also highlights the many tools that actors are attempting to employ to address hate speech and misinformation online. Increasingly frustrated with the inability of social media companies such as Facebook to effectively regulate harmful content, some governments feel they have few avenues for recourse and for addressing such speech in a more targeted way. Increased encryption of messaging services, such as WhatsApp and Facebook Messenger, only elevate and escalate the use of shutdowns. In short, shutdowns are likely to evolve as governments find more targeted ways of dealing with harmful content, or content that they may not like, but shutdowns are unlikely to go away in the near future.

This article furthers our argument about framing shutdowns through the lens of spectrums by drawing on data collected during our ongoing research into the Internet and conflict in Africa, including interviews with technologists, human rights activists, and humanitarians working on Internet connectivity in Africa in the context of the European Research Council project, ConflictNET (The Politics and Practice of Social Media and

Conflict in Africa).[4] We also draw on the articles presented in this Special Issue that highlight the diversity of shutdowns on the continent. Africa is certainly not the only continent in which Internet shutdowns are taking place, but it is home to a notably wide variety of cases—from those targeting subnational groups during the regional shutdown in Cameroon, to those blamed on the accidental severing of cables in Zimbabwe, to the drawn-out shutdowns specifically targeting social media platforms in Chad. This diversity of cases is useful for examining what tools and approaches comprise different types shutdowns.

Ambiguity in Shutdowns

One way of diagnosing the ambiguity about what constitutes a shutdown is through unpacking the expected causes and effects that are included in many definitions. In terms of causes, most definitions, like Access Now's, specify that an Internet shutdown must be intentional, not the result of an accident that affects the technical systems.[5] Similarly, many definitions are explicit that the government is necessarily the actor that orders an Internet shutdown. Private sector Internet service providers and mobile network operators, as managers of a country's Internet network, are typically the actors that must carry out a shutdown of a country's Internet network. But for many existing definitions, if these private sector actors decide themselves to block access to the Internet rather than being ordered to do so by a government, it would not amount to an Internet shutdown. For example, the Software Freedom Law Centre, India (2019) offers a definition which specifies that "an Internet shutdown is always Government-imposed" (FAQ sec., para. 1). When intentionality is made an integral aspect of what constitutes a shutdown, some leave a bit of room in their understanding of what motivated this choice of tactic, mentioning, as the Internet Society (2019b) does, that they are conducted "to exert control over the flow of information" (para. 5). In terms of effects, definitions differ in how specific they have chosen to be. Access Now is quite broad, saying that an Internet shutdown disrupts "Internet or electronic communications, rendering them inaccessible or effectively unusable" (Taye & Access Now, 2019, sec. 1.1, para. 1), whereas the Software Freedom Law Centre, India (2019) takes a more limited approach, arguing that an Internet shutdown "always imposes a blanket ban on Internet access" (para. 6).

Causes

There are, of course, many examples of times when access to the Internet goes down without an explicit decision to turn it off. In Kenya, for example, connectivity is frequently lost due to unintentional technical challenges. Kenya's mobile telecom provider, Safaricom, for example has suffered from accidentally severed cables as well as software issues at a data center that have caused short blackouts. In Liberia, a cyberattack on one of the country's main mobile operators carried out by a British hacker, and paid for by a rival Internet company, took down Internet access in Liberia for a full day (Casciani, 2019). Although the cyberattack had been planned, its widespread near total impact on the country's Internet was certainly not. And in Somalia, Internet services were unavailable for nearly a month after a ship severed an undersea fiber optic cable ("Somalia Internet," 2017).

---

[4] For more information, see https://pcmlp.socleg.ox.ac.uk/conflictnet/. This Special Section draws on a conference on Internet Shutdowns held in Johannesburg (Marchant & Stremlau, 2019).

[5] Others have also focused on the centrality of intentionality. See, for example, Wagner (2018).

Such disruptions are not uncommon, and they also offer opportunities for governments to obfuscate the intentionality behind some Internet shutdowns. In Zimbabwe, when the Internet and phone lines went down for a day, the government and the ISPs said it had been caused by a tractor severing a cable in South Africa ("Internet Shuts Down in Zim," 2017). Although many accepted this technical explanation, some observers suspected government involvement (Thulin, 2017). But experiences like the one at Safaricom, or similar technical network disruptions, imply that the unintentional technical explanation is at least plausible. Government decision making, particularly in more authoritarian regimes, can be notoriously opaque, and without an inside view into this process, it can be difficult to determine the intentionality behind a network disruption, particularly when government officials deny responsibility.

Governments are often the primary perpetrator in Internet shutdowns, and government-led shutdowns also make up the majority of the news coverage of the topic. But nonstate actors—from militant groups and hackers to foreign governments and tech companies—muddle the lines of responsibility for shutdowns. In some cases, a nonstate actor may be acting on behalf of a government, other authority, or independently. There have been regular instances in which the insurgent group Al Shabaab shut off Internet access in parts of Somalia and northern Kenya by attacking network towers, banning certain telecom providers, and prohibiting the use of smart phones. In these instances, they make their intention to shut off connectivity clear and offer justifications ranging from reducing the ability of government and African Union troops to communicate and coordinate, implicating the use of smartphones by government security services to spy, and asserting that the Internet was promoting immoral behavior (Wakama, 2014). In many respects, Al Shabaab acts like a state in the territories it controls—it runs the schools, hospitals, and provides security. Telecom companies that provide mobile Internet are "taxed" by Al Shabaab and operate only with their patronage, giving them little choice but to comply with the varying dictates (Stremlau, 2018a; Stremlau, Fantini, & Gagliardone, 2015).

A distributed denial-of-service (DDoS) attack is another example of a way in which Internet access may be interrupted by actors other than governments, though it is not often discussed in the same context as Internet shutdowns. DDoS attacks are "an explicit attempt to prevent the legitimate use of a service" (Mirkovic & Reiher, 2004, p. 40) by intentionally flooding a particular target with traffic that its servers cannot handle. They are a particularly common form of cyberattacks on telecom companies in Africa (Mataranyika, 2016). They are most often associated with narrower targets, like websites, banks, or IT companies, rather than nationwide Internet access we more commonly associate with an Internet shutdown. South Africa, for example, has experienced a wave of such attacks in recent years, as banks have repeatedly been targeted in DDoS attacks as part of a campaign to extort ransom payments (Ikeda, 2019). The City of Johannesburg has also been subjected to ransom driven attacks with its websites and online government services shutdown (Moyo, 2019). In both instances, the public-facing Internet services have been disabled, resulting in significant financial loss.

However, less well-known but relevant to the present discussion is the ways in which DDoS attacks can be broad and result in widespread Internet shutdowns. Such an event occurred in the United States in 2016, when hackers, using a DDoS attack aimed at an Internet infrastructure company, were able to take down a large portion of the Internet for most of the East Coast (Newman, 2016). While DDoS attacks are most known for targeting individual websites, when pursuing a company that provides the domain name system

(DNS) services that we use to access the Internet, a DDoS attack can restrict the ability to access the Internet for any user whose traffic routes through that DNS service. In the case of DDoS attacks, the perpetrators can range from independent hackers, to private companies targeting the competition, to states targeting one another. But from the perspective of the end user, the experience is the same regardless of who orchestrated the attack, and it is not dissimilar to the experience of a more overt Internet shutdown. This diversity of actors instigating Internet shutdowns is only likely to increase in the future and suggests the importance of ensuring that consideration of intentionality encompasses a wide range of actors and motivations.

Government intentionality is coupled, in many definitions, with motivations rooted in things like a government's desire to control the flow of information. Although it is difficult to verify the real motivations behind any effort to restrict Internet access, let alone within governments, examining some of the justifications given by government officials gives some indication as to what government officials believe are acceptable reasons for shutdowns. Two of the key themes that emerge are protecting public security and controlling the spread of misinformation (Iazzolino & Stremlau, 2017).

The Togolese government, for example, used the public safety justification during the 2017 elections (Y-Kollektiv, 2018), whereas officials from the Democratic Republic of Congo (DRC) have used it numerous times, including during a shutdown that same year when the ICT Minister of the DRC, Emery Okundji, argued that "there are very ill-intentioned guys who have been organizing to make blood run during this festival period at the end of the year" ("RDC," 2018, para. 2). In a subsequent shutdown in 2018, the country's Minister of Communication, Lambert Mende Omalanga, asked the public, "What is more important? Our comfort or our security? I think we need to understand that it concerns the security of all Congolese" ("La République," 2019, para. 1). Because of such perceived security risks, during the 2018 shutdown, Minister Mende went so far as to say that Internet shutdowns should be an accepted cost for a smooth election period:

> An Internet shutdown is a thing we do during election periods; it's once every 5 years. We need to understand that everything has a price. Dignity has a price. The sovereignty and integrity of the electoral process also has a price. I ask the Congolese to consider this to be the price to pay to maintain the integrity of their electoral process. (Tshiamala, 2019, para. 6)

The misinformation justification has also been used frequently during elections. During the 2019 elections in Benin, the Internet was shut down soon after the government's official Twitter account warned about the problems of misinformation on social media (NetBlocks, 2019). Similarly, in Cameroon, in 2017, the communication minister said that the country's Internet shutdown had been triggered in response to the spread of misinformation on social media that was inciting violence (Mukeredzi, 2017). And during the 2018 shutdown in the DRC during elections, Communication Minister Mende pointed to "sneaky guys who wanted to use social networks to replace CENI [their electoral commission] by publishing false figures, false data, and so it was necessary to deprive them of this instrument" (Tshiamala, 2019, para. 2).

Regardless of the justifications governments give publicly, many of those who closely monitor Internet shutdowns believe they are false narratives used to hide the overriding objectives to curtail opposition activity, demonstrations, or critical voices. Although this may be the case in some circumstances, at the same time, in

certain circumstances, misinformation and the threat of violence pose real challenges that governments need to address (Stremlau, 2018b). As one technologist and human rights practitioner in Uganda argued, "sometimes certain governments do have legitimate security concerns" (personal interview, August 1, 2019). She provided the example of Ethiopia, where she described a civil society focused on keeping the Internet on amid concerns about a real threat of physical violence: "If there's men in the streets with machetes mobilizing," she explained, "then yes, shut off social media." In a similar vein, another human rights practitioner in Cameroon described how misinformation on social media began as a mere justification the government was giving, but that it had since become a "real problem that everyone has to contend with" (personal interview, September 5, 2019). The purpose here is not to validate government justifications for extreme actions like shutting off the Internet, but to draw attention to the complex array of factors with which leaders are confronted and the lack of information that exists about how these decisions are really made.

Effects

Fundamental to the prevailing definitions of an Internet shutdown is that it is an act that has the effect of rendering the Internet "inaccessible or effectively unusable" (Taye & Access Now, 2019, sec. 1.1, para. 1). Yet while rendering the Internet inaccessible is certainly the most obvious effect of an Internet shutdown, it is not the most important, and it tells us nothing about the lived experiences of those targeted by an Internet shutdown. As a result, many writing about Internet shutdowns focus on other effects, most notably the effects on communities, on economies, and on protests.

Coverage of the effects of Internet shutdowns range from stories of individual struggles to adapt to the new restrictions, to broader nationwide effects on the economy and human rights. There are anecdotes of those who have crossed borders to access their e-mail (Kingsley, 2019), or those who have not been able to withdraw money from their bank to pay vital health expenses (Muperi & Brown, 2019), or those who felt silenced, frustrated by being cut off from their tool of choice for expressing their political opinions publicly (Internet Society, 2019b).

Some of the most significant studies that attempt to detail the impact of shutdowns have focused on the economic effects that Internet shutdowns have reportedly had, ranging from small businesses to overall GDP (CIPESA, 2017; West, 2016). Although such efforts to focus on the economic effects are notable attempts to shift the debate and advocate against Internet shutdowns, the claims they make are difficult to verify. This is, in part, due to challenges in quantifying some of the cost implications of lost economic activity, but it is also difficult to determine whether a shutdown may have also temporarily reduced violence, which can have economic impacts that may be even more severe than the shutdown itself. The evidence base for the relationship between online incitement and off-line harms remains weak or mixed and misunderstood. Although economic analysis documents some very real effects of Internet shutdowns, it is also necessary to look at the ways in which an Internet shutdown might have less of an effect than expected, such as when Internet penetration rates are particularly low. It is also necessary to consider other practices—such as taxation or deliberate efforts to slow down the Internet—that can have similar effects as Internet shutdowns, particularly on the individual level.

Internet penetration rates in Africa continue to rise, but just under 40% of the 1.3 billion people on the continent have access to the Internet. This is in contrast to more than 60% for the rest of the world (Internet World Stats, 2020), and this 40% is not spread evenly around the continent. Of the 10 African countries in which Access Now recorded an event that met their definition of Internet shutdowns (Taye & Access Now, 2019), the majority have far lower Internet penetration rates than the continental average. Chad and the DRC both have less than 10%, for example (6% and 8%, respectively). At the same time, three—Cote d'Ivoire, Mali, and Nigeria—all have penetration rates over the average, with Nigeria's and Mali's 61% and 63% (respectively) being higher than the average for the rest of the world. Penetration rates provide some indication of the impact or disruption a shutdown might cause. If an individual has no Internet access to begin with—whether because of poor infrastructure or prohibitive costs—an Internet shutdown is less likely to have a direct impact on their life than, for example, the forced closure of a local radio station. This is particularly the case in rural areas, especially in Africa, where Internet access is far more limited than in urban areas. In places where network connectivity is already poor, and residents are accustomed to periodic blackouts, a shutdown may not seem as severe as it might appear. As one interviewee from Zimbabwe argued, "If you're accustomed to unreliable Internet, then you don't always know a shutdown is happening" (personal interview, July 28, 2019). This can be the case in urban environments where Internet access may be unreliable for other reasons. For example, in the London Underground, the public WiFi administered by the London Transport Authority is known to offer variable access across platforms and stations. As a result, when the London Transport Authority shut off the WiFi in April 2019 to inhibit an environmental protest movement from Extinction Rebellion, many Underground users were unperturbed. As one Twitter user posted at the time of the shutdown, the WiFi in the Tube is "so intermittent it's generally useless anyway" (Hills, 2019, para. 1). Where Internet is unavailable, unreliable, or people have otherwise refrained from integrating it into their lives, the effects of an Internet shutdown may be less.

In contrast, in places where the Internet has penetrated deeply into people's lives the effects can be significantly increased. For example, a recent piece from Shandler, Gross, and Canetti (2019) used an experiment to look at the impact of being disconnected from the Internet on people's ability to engage in political activity in Israel. They found that "Internet deprivation substantially negates civic participation for political expression and association, but not yet in relation to the acquisition of political information" (Shandler et al., 2019, p. 8). In many countries like Israel, where Internet access is more than 80%, it is not just that the Internet has become a part of daily life, but that it also has often replaced its analogue counterparts. As is the case for many media markets in Europe, and North America, one result of the Internet upending the business model of traditional media, is that many newspaper outlets, particularly small local ones, are no longer available in print but can only be accessed online. To achieve a more holistic, but less quantifiable, understanding of the effects of Internet shutdowns, the context in which the Internet is experienced by citizens and the ways it has, or has not, been integrated into people's lives and the lives of the cities they live in, has to be considered.

At the same time, other practices—mostly national policies—that do not get the same attention as outright shutdowns, but that nonetheless have a dramatic and tangible effect on an individual's ability to get online, are becoming more prevalent. One example of this is the rise in taxation, particularly of social media platforms (Bergère, this Special Section). Uganda is most notable for its adoption of this tactic. In July 2018, Uganda adopted a new tax of 200 Ugandan shillings per day (the equivalent of 5 cents in the

United States) to access more than 60 online platforms, including Facebook, WhatsApp, and Twitter. One interviewee described how this policy was having a particularly significant impact on South Sudanese refugees living in Uganda, saying that it directly affected their ability to receive mobile money transactions, an important lifeline for them (personal interview, January 23, 2019). For refugees and others who cannot afford to pay the tax, the experience of a tax—which standard definitions would not consider to be an Internet shutdown—may be similar to a full Internet shutdown in practice. Lisa Parks and Rachel Thompson provide a useful illustration of this in the context of Tanzania in their article in this Special Section.

In contrast to the prevailing debates about "effects" of shutdowns, which tend to focus on what is most easily identifiable, or quantifiable (such as economic impact, or some social impacts), there is a need to expand understanding about the effects of shutdowns in very different contexts. There is a similar need to consider when different policy choices—a tax versus a full Internet shutdown, for example—have the same impact in practice for many individuals. Similarly, at the moment, too little data exists to make claims about the impact of shutdowns on other issues, such as political decision making or the persistence of unrest (Jacob & Akpan 2015; Rydzak 2019), though Rydzak, Karanja, and Opiyo's piece in this Special Section suggests that it is worth exploring further the possibility that Internet shutdowns could actually increase certain protest movements. Even in Kenya, which has one of the highest Internet penetration rates on the continent, broadcast television is still more influential than social media as a tool for disseminating new and information. Many governments choosing to target social media platforms argue that such platforms breed a particular type of hate and incite violence (Gagliardone et al., 2016). Discerning the impact of access to social media or access to the Internet as a whole on different populations is complex, regardless of context.

A Spectrum Approach

Prevailing definitions of Internet shutdowns serve an important role in the advocacy community for rallying actors around the cause of challenging government action. But there are gray areas—nuances, uncertainties, and variations—among Internet shutdowns, particularly around what or who caused the disruption, and why it was done. This suggests that there is a need to situate shutdowns in broader debates about the relationship between security and censorship, or online discussions and off-line harms. A full nationwide Internet shutdown is an extreme act. But it is not necessarily isolated from less extreme forms of censorship and intimidation, like targeted website takedowns, national Internet "firewalls," or imprisonment of journalists and bloggers. Key advocacy groups such as Access Now agree that Internet shutdowns are not isolated incidents (Kingsley, 2019), but placing shutdowns along a spectrum helps to more accurately situate them in relation to these other forms of censorship. In addition to considering the nuances and acknowledging the unknowns in the causes and effects of different kinds of Internet shutdowns or related policies, as we discussed above, situating a particular case within other dimensions—including frequency and duration, depth, breadth, and speed—offers greater opportunities for understanding the diversity of shutdowns. We illustrate these below.

Frequency and Duration

Frequency and duration most often appear in news coverage of Internet shutdowns, representing how often and for how long the Internet is shut off in a particular place. India is the country most often

pointed to for its extreme approach to frequency, with an estimated 380 separate shutdowns between 2014 and early 2020. However, a quarter of these shutdowns lasted less than 24 hours (Software Freedom Law Centre, India, 2020). In contrast, some countries in Africa have had some of the longest Internet shutdowns on record, most notably Cameroon and Chad, with 230 days and 480 days, respectively (Dahir, 2019). In Cameroon, the shutdown was focused on the Northwest and Southwest regions of the country; in Chad, the shutdown blocked access to all social media platforms rather than the Internet as a whole. These are important nuances and differences that can have significant impact on what implementers are trying to achieve with an Internet shutdown.

Depth

Depth refers to the type of content that is targeted, ranging from a full Internet blackout, to a particular platform, or even the targeting of an individual blogger or another kind of user. Many, though not all, of the prevailing definitions make a distinction between switching off access to the Internet as a whole and switching off access to social media or to individual platforms. For example, much of the coverage of the "shutdown" in Chad referred to it as a "social media shutdown" rather than an Internet shutdown. The Software Freedom Law Centre in India even refers to a block placed on particular kinds of content or a service as a "surgical ban" rather than an Internet shutdown (Software Freedom Law Centre, India, 2019). Although the extreme end of the depth dimension—the "deep" end, as it were—is a complete Internet blackout, a social media shutdown moves us further up the spectrum. Further up still are relatively "shallower" methods, like freedom of speech restrictions, including taking down individual blogs and online newspapers, or jailing journalists. These methods are only shallow in the sense that they are narrower in the type of content they are restricting; it is not intended to reflect their severity.

There is, however, a gray area between these different kinds of bans and shutdowns, considering the impact on individual users. Although restricting a shutdown to social media may seem to limit, for example, the economic impact of a shutdown—by allowing banks to continue to wire money or corporations to continue to use e-mail—for many ordinary users it is experienced in the same way as a full shutdown. In many African countries, blocking Facebook means blocking the Internet. For some African countries—including Somalia, Liberia, Guinea, the Republic of Congo—Facebook penetration among Internet users is more than 80% (Internet World Stats, 2020). This suggests that, in such cases, a social media shutdown may be experienced in a similar way to a full Internet shutdown for many individuals. In this context, the impact of a social media shutdown can vary significantly depending on the information environment and the norms of Internet use in particular areas.

Breadth

Breadth refers to how many people are affected or how geographically dispersed a shutdown is. Many shutdowns are targeted and localized, but the breadth will also be affected by how densely populated an area is. Shutting down the Internet in the Afar region of northern Ethiopia would only affect 1.6 million people, whereas the multiple shutdowns that have been imposed in the Oromio region of Ethiopia may have affected 35 million, the equivalent of more than half the population of the UK. Thus, while a nationwide shutdown seems to sit at the extreme "wide" end of the breadth dimension, there is more variation in the

"narrow" end than looking exclusively at geography would indicate. The example of the shutdown in the London Underground, in 2019, is an instance of an extremely narrow shutdown affecting a small geographic area, though with an impact for a larger population than the authorities were intending to target. The severity of the effect of this particular shutdown was also lessened because of the ease of movement between where the shutdown was in effect—the Underground—and the rest of London, and the poor quality of the Internet in the Underground to begin with.

In some cases, however, a more targeted narrow shutdown might actually be just as concerning as a nationwide shutdown, if not more so. For example, in many refugee camps and settlements in Africa, there have been attempts by humanitarian organizations and mobile network operators (MNOs) to increase refugee access to the Internet, but this policy has not always been embraced by host governments. Since September 2019, following protests against attempts to repatriate some of the 750,000 Rohingya refugees currently living in camps in Bangladesh (UNHCR, 2020), the government of Bangladesh ordered the Internet to be shut off in the camps, which they said was for "security reasons" (Paul, 2019). They began by implementing a mandatory curfew between 5 p.m. and 6 a.m. and gave instructions for the authorities to confiscate SIM cards that the Rohingya were using (Paul, 2019). This is a troubling example of a case in which an Internet blackout was targeted at a particular ethnic group rather than the population as a whole, and as a result does not fall under conventional definitions of an Internet shutdown. Bangladesh is not the only case in which a government has decided that refugees—a population with the least ability to advocate for their rights—should be targeted for exclusion from the Internet. The Jordanian government has taken a similar approach, banning Internet access for the residents of refugee camps that house Syrian refugees over concerns that Internet access would lead to their radicalization (personal interview, January 9, 2019). While refugees have not yet been intentionally excluded in this way in the African context, some of the shutdowns that have occurred on the continent have targeted particular subnational groups. For example, the cases of Cameroon or Ethiopia's regional shutdowns can be seen as attempts to restrict access for particular communities. This kind of targeting, while limiting the effect of a shutdown on the general population, is a worrying trend with broader implications for the relationship between states and subgroups that requires further unpacking.

Speed

Speed refers to the range of techniques available to implement shutdowns—from a slowdown of the network all the way to a full blackout. In a slowdown, Internet bandwidth is throttled to reduce the speed at which data is transmitted, and can be targeted even at an individual user or a larger geographic area. Although a slowdown may not seem as egregious as a full shutdown, in practice, an extreme slowdown may render the Internet so slow as to be unusable in practice. In many parts of Africa, network slowdowns happen unintentionally all the time when bandwidth demands reach the limits of a network's capacity, due to insufficient infrastructure or an unreliable power supply. However, sometimes a network provider will also intentionally slow a connection down, limiting, for example, access to high-bandwidth streaming services to maintain moderate service across their network (personal interview, January 9, 2019). At other times, when individual users are using a disproportionately high proportion of the available bandwidth, many ISPs will throttle the bandwidth allowance for that user to free up space for others. These kinds of network maintenance decisions are regularly made by ISPs around the world. But there are also times when a

network slowdown is a result of an intentional order from public authorities. It can be difficult to distinguish among these three kinds of slowdowns—unintentional, ordered by ISPs, or ordered by the government—or even to confirm when a slowdown is happening. For Internet shutdowns, organizations like NetBlocks and the Open Observatory of Network Interference (OONI) have developed tools that can identify when a network has gone down entirely and an Internet shutdown has taken place (although these tools still cannot identify whether such a shutdown was intentional or not). A serious slowdown can, in practice, have a similar effect on many users as a full Internet shutdown, and it can simultaneously be harder to detect making them more problematic.

Conclusion

At this point, the wide variation among cases of Internet shutdowns along each of these five dimensions—frequency, duration, depth, breadth, and speed—should be self-evident. So, too, should be the ambiguity at their tail ends. Although a full Internet blackout carried out across an entire country for a long period of time may be the most obviously egregious case, situations in which network slowdowns or taxes have the same practical effect as full shutdowns or where a particular ethnic group is targeted for exclusion make clear how complicated the boundaries are between Internet shutdowns and other forms of censorship and how context dependent the impact of various kinds of shutdowns can be. When cases of Internet shutdowns or Internet shutdown-adjacent events arise, situating them along a spectrum can help to better understand their nuanced characteristics and where they are in relation to other cases and in relation to other forms of censorship or information control like taxation, surveillance regulations, website takedowns, or banning live television broadcasts.

As technologies continue to change, it is likely that Internet censorship will not look like the Internet shutdowns we know today. In particular, as governments gain technological expertise and surveillance capabilities improve, it is likely that there will be a move away from the particularly blunt instrument of Internet shutdowns—whether national or local, with governments instead choosing from an array of tactics that vary more greatly in depth, breadth, speed, and perhaps along other unforeseen dimensions.

Public discourse on shutdowns in the media and by advocacy groups tends to present them as a mechanism detached from other, more moderate forms of information control. And with the perceived severity of the impact of a full Internet blackout, shutdowns may deserve to be treated as such. However, doing so risks removing shutdowns from ongoing and quickly evolving debates about the impact of pressing concerns such as hate speech, incitement to violence, and misinformation online and its connection with violence off-line. It also isolates less obvious stakeholders such as ISPs, social media networks, traditional media outlets, and businesses from debates on government techniques for information control.

Analyzing Internet shutdowns as existing on a spectrum—varying along dimensions such as duration, breadth, depth, speed, and frequency—allows that discussion to stay engaged with changing debates about the evolving and competing norms governing the Internet that may shape the forms shutdowns take in the future and the ways in which they are both justified and legitimized.

At present, there is little evidence about the underlying policy debates that occur at a national level when a state decides to implement a shutdown. Questions remain about the technological developments enhancing the ability and willingness for actors to resort to shutdowns, the role played by international and nonstate actors, and the legal and political processes that both enable and legitimize certain shutdowns, the latter of which De Gregorio and Stremlau explore in great detail in their piece in this Special Section. In popular debates about the causes of Internet shutdowns, governments are almost always seen as the perpetrators; they are framed as the villains restricting freedoms. Yet existing research show how varied the causes can be—from the unintentional, including severe weather and accidentally severed cables, to the intentional but nongovernmental, such as foreign government attacks, rogue hackers, or ISP-led slowdowns. Although many definitions of what constitutes an Internet shutdown expressly exclude unintentional shutdowns from the list, it is more difficult than it may seem to tell the difference, and it is important to find ways to accurately and reliably distinguish between them.

Even where governments are responsible, greater consideration of the other actors involved may enhance understanding of why they make the choices they make. This includes, for example, research looking at the role and power of a range of different stakeholders, from the courts to mainstream journalists, government officials to political candidates, domestic publics to foreign publics, and ISPs and MNOs, terrorist organizations and the military. Focusing on the kinds of power relations that exist and how power is exerted between them could provide productive insights into opaque government decision-making processes.

There is a need for more dialogue that includes as many of the diverse stakeholders involved in Internet access as possible. International policy discussions addressing Internet shutdowns (and freedom of speech more broadly) are rarely attended by those within government who are either tasked with restricting certain types of content or managing elections, protests, or other events that are often associated with Internet shutdowns. As a result, there is a gap in discussions about the adoption of particular forms of shutdowns. Engaging with government officials—though difficult—as well as international social media networks like Facebook and Google, and local MNOs is a necessary step toward finding a balance between the need to reduce the potential for violence and access to the Internet. Adopting a spectrum framing of Internet shutdowns, and one that draws attention to the nuances of the causes and effects of shutdowns or shutdown-adjacent policies, may facilitate greater dialogue in those spaces.

References

Casciani, D. (2019, January 11). Briton who knocked Liberia offline jailed. *BBC News*. Retrieved from https://www.bbc.com/news/uk-46840461

CIPESA. (2017). *A framework for calculating the economic impact of Internet disruptions in sub-Saharan Africa.* Retrieved from https://cipesa.org/?wpfb_dl=252

Dahir, A. L. (2019, January 22). *Chad Republic has kept social media shut for 300 days and counting*. Retrieved from https://qz.com/africa/1530071/chad-republic-blocks-social-media-for-300-days-sparking-campaign/

Gagliardone, I., Pohjonen, M., Beyene, Z., Zerai, A., Aynekulu, G., Bekalu, M., . . . Taflan, P. (2016). *Mechachal: Online debates and elections in Ethiopia—From hate speech to engagement in social media.* Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2831369

Hills, M. [@mikewhills]. (2019, April 17). Yeah, definitely. It's so intermittent it's generally useless anyway. Trying to download Brexitcase on the tube is not fun! [Tweet]. Retrieved from https://twitter.com/mikewhills/status/1118438899557253120

Iazzolino, G., & Stremlau, N. (2017). New media and governance in conflict. *Third World Quarterly*, *38*(10), 2242–2257.

Ikeda, S. (2019, November 4). *Sustained DDoS attack on South African banks accompanied by ransom notes*. Retrieved from https://www.cpomagazine.com/cyber-security/sustained-ddos-attack-on-south-african-banks-accompanied-by-ransom-notes/

Internet shuts down in Zim. (2017, December 5). *NewsdzeZimbabwe.* Retrieved from http://www.newsdzezimbabwe.co.uk/2017/12/internet-shuts-down-in-zim.html

Internet Society. (2019a, December 17). *Internet society position on Internet shutdowns.* Retrieved from https://www.internetsociety.org/resources/doc/2019/internet-society-position-on-internet-shutdowns/

Internet Society. (2019b, December 18). *Policy brief: Internet shutdowns.* Retrieved from https://www.internetsociety.org/policybriefs/internet-shutdowns

Internet World Stats. (2020, March 31). *Africa Internet users, 2020 population and Facebook statistics.* Retrieved from https://www.internetworldstats.com/stats1.htm

Jacob, J. U. U., & Akpan, I. (2015). Silencing Boko Haram: Mobile phone blackout and counterinsurgency in Nigeria's Northeast region. *Stability: International Journal of Security and Development*, *4*(1), Art. 8, 1–17.

Kingsley, P. (2019, September 2). Life in an Internet shutdown: Crossing borders for email and contraband SIM cards. *The New York Times*. Retrieved from https://www.nytimes.com/2019/09/02/world/africa/internet-shutdown-economy.html

La République démocratique du Congo privée d'Internet [The Democratic Republic of Congo deprived of Internet]. (2019, January 17). *France 24*. Retrieved from https://www.francetvinfo.fr/monde/afrique/republique-democratique-du-congo/la-republique-democratique-du-congo-privee-dinternet_3149065.html

Marchant, E., & Stremlau, N. (2019). *Africa's Internet shutdowns: A report on the Johannesburg workshop* (Programme in Comparative Media Law and Policy [PCMLP], University of Oxford). Retrieved from http://pcmlp.socleg.ox.ac.uk/wp-content/uploads/2019/10/Internet-Shutdown-Workshop-Report-171019.pdf

Mataranyika, M. (2016, May 27). *Hackers increase their attacks on Africa*. Retrieved from https://www.news24.com/fin24/tech/cyber-security/hackers-increase-their-attacks-on-africa-20160527#:~:text=The%20most%20common%20form%20of,that%20can%20knock%20out%20services

Mirkovic, J., & Reiher, P. (2004, April). A taxonomy of DDoS attack and DDos defense mechanisms. *ACM SIGCOMM Computer Communications Review, 34*(2), 39–54.

Moyo, A. (2019, October 25). *City of Joburg hit by cyber attack*. Retrieved from https://www.itweb.co.za/content/dgp45qaG8gZ7X9l8

Mukeredzi, T. (2017, October 24). Uproar over Internet shutdowns. *Africa Renewal, 31*(2), 32–34. doi:10.18356/64c24ec4-en

Muperi, W., & Brown, R. L. (2019, January 23). *As more Africans reach for Web, more leaders reach for "off" switch*. Retrieved from https://www.csmonitor.com/World/Africa/2019/0123/As-more-Africans-reach-for-web-more-leaders-reach-for-off-switch

NetBlocks. (2019, May 1). *New Internet disruption in Benin amid riots following elections*. Retrieved from https://netblocks.org/reports/new-internet-disruption-in-benin-amid-riots-following-elections-W80ZKLBK

Newman, L. H. (2016, October 21). *What we know about Friday's massive East Coast Internet outage*. Retrieved from https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/

Paul, R. (2019, September 3). Bangladesh blocks Internet services in Rohingya refugee camps. *Reuters*. Retrieved from https://www.reuters.com/article/us-bangladesh-rohingya-idUSKCN1VO1WQ

Purdon, L., Ashraf, A., & Wagner, B. (2015). *Security v. access: The impact of mobile network shutdowns, case study Telenor Pakistan*. Philadelphia: University of Pennsylvania, Center for Global Communication Studies.

RDC: Internet et SMS seront débloqués à partir de ce lundi 23h00 [DRC: Internet and SMS will be unblocked from 11pm this Monday]. (2018, January 1). Retrieved from https://www.mediacongo.net/article-actualite-33897_rdc_internet_et_sms_seront_debloques_a_partir_de_ce_lundi_23h00.html

Rydzak, J. (2019). *Of blackouts and bandhs: The strategy and structure of disconnected protest in India*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3330413

Shandler, R., Gross, M. L., & Canetti, D. (2019). Can you engage in political activity without Internet access? The social effects of Internet deprivation. *Political Studies Review,* 1-10. Advance online publication.

Software Freedom Law Centre, India. (2019). *About.* Retrieved from http://internetshutdowns.in/about

Software Freedom Law Centre, India. (2020). *Internet shutdowns in India.* Retrieved from https://internetshutdowns.in

Somalia Internet returns after three-week blackout. (2017, July 18). *Al Jazeera*. Retrieved from https://www.aljazeera.com/news/2017/07/somalia-internet-returns-week-blackout-170718070256586.html

Stremlau, N. (2018a). Governance without government in the Somali territories. *Journal of International Affairs*, *71*(2), 73–89.

Stremlau, N. (2018b). *Media, conflict, and the state in Africa*. Cambridge, UK: Cambridge University Press.

Stremlau, N., Fantini, E., & Gagliardone, I. (2015). Patronage, politics and performance: Radio call-in programmes and the myth of accountability. *Third World Quarterly, 36*(8), 1510–1526.

Taye, B., & Access Now. (2019, July). *The state of Internet shutdowns around the world: The 2018 #KeepItOn Report.* Retrieved from https://www.accessnow.org/cms/assets/uploads/2019/07/KeepItOn-2018-Report.pdf

Thulin, L. (2017, December 6). *Zimbabwe's Internet went down for about five hours. The culprit was reportedly a tractor*. Retrieved from https://slate.com/technology/2017/12/zimbabwe-s-internet-outage-was-reportedly-due-to-a-tractor-that-cut-the-cables-of-a-major-internet-provider.html

Tshiamala, S. B. (2019, January 2). *Lambert Mende: Coupure Internet et SMS: Je demande aux Congolais de considérer cela comme le prix à payer pour l'intégrité du processus électoral* [Lambert Mende: I ask the Congolese to consider this as the price to pay for the integrity of the electoral process]. Retrieved from https://actualite.cd/2019/01/02/coupure-internet-et-sms-je-demande-aux-congolais-de-considerer-cela-comme-le-prix-payer

UNHCR. (2020). *Joint government of Bangladesh–UNHCR population map as of 15 March 2020.* Retrieved from https://data2.unhcr.org/en/documents/details/74675

Wagner, B. (2018). Understanding Internet shutdowns: A case study from Pakistan. *International Journal of Communication, 12*, 3917–3938.

Wakama, A. (2014, January 9). Al-Shabaab bans mobile Internet in Somalia. *IT News Africa*. Retrieved from https://www.itnewsafrica.com/2014/01/al-shabaab-bans-mobile-internet-in-somalia/

West, D. M. (2016). *Internet shutdowns cost countries $2.4 billion last year*. Retrieved from https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf

Wolchover, N. (2011, January 28). *How do you shut down the Internet in a whole country?* Retrieved from https://www.livescience.com/32965-how-do-you-shut-down-the-internet-whole-country.html

Y-Kollektiv. (2018, October 11). *Internet-shutdown—Wenn die Regierung das Internet abschaltet* [Internet shutdown—When the government turns off the Internet] [Video file]. Retrieved from https://www.youtube.com/watch?v=4FwVQV8FpFk