

# ePub<sup>WU</sup> Institutional Repository

Benjamin Wagner

Understanding Internet Shutdowns: A Case Study from Pakistan

Article (Published)  
(Refereed)

*Original Citation:*

Wagner, Benjamin (2018) Understanding Internet Shutdowns: A Case Study from Pakistan. *International Journal of Communication*, 12 (1). pp. 3917-3938. ISSN 1932-8036

This version is available at: <http://epub.wu.ac.at/6661/>

Available in ePub<sup>WU</sup>: November 2018

ePub<sup>WU</sup>, the institutional repository of the WU Vienna University of Economics and Business, is provided by the University Library and the IT-Services. The aim is to enable open access to the scholarly output of the WU.

This document is the publisher-created published version.

## Understanding Internet Shutdowns: A Case Study from Pakistan

BEN WAGNER<sup>1</sup>

Vienna University of Economics and Business, Austria

This article provides an overview of Internet shutdowns in Pakistan, which have become an increasingly common phenomenon, with 41 occurring between 2012 and 2017. It argues that to understand how shutdowns became normalized in Pakistan, it is necessary to look at the specific dynamics of how the shutdowns take place. In doing so, the concept of communicative ruptures develops to better understand intentional government shutdowns of communications. The article argues that strategic prevention of mobilization is key for short-term shutdowns, whereas long-term shutdowns can be better explained by looking at disciplinary mechanisms and denying the existence of “others.” The article then discusses Internet shutdowns in the wider context of authoritarian practices before concluding with the urgent need for further research on this topic, both in Pakistan and beyond.

*Keywords: Internet shutdowns, human rights, telecommunications policy, Internet access, technology regulation, authoritarian politics*

On August 14, 2014, the “Interior Ministry . . . ordered mobile phone services to be shut down in several parts of Islamabad for an indefinite period” (Bhatti, 2014, para. 1). For three days, large parts of the Pakistani capital were disconnected from mobile phone voice and data connectivity. Citizens in these areas were not able to use their phones, not able to access mobile Internet (by far the most common form of Internet connectivity in Pakistan), and were not able to call emergency services. Why would a government suppress all digital communications across a whole city for days on end?

The five-day telecommunications and Internet services shutdown in Egypt in 2011 cost Egypt’s economy at least US\$90 million, excluding secondary costs, as well as its “reputation among technology firms as a stable place for investment” (Howard, Agarwal, & Hussain, 2011b, p. 231; see also OECD, 2011).

---

Ben Wagner: ben@benwagner.org

Date submitted: 2017–12–07

<sup>1</sup> This research project was conducted in close collaboration with the Pakistani NGO Bytes for All in Islamabad and the Institute for Human Rights and Business (IHRB) in London. In particular, Arsalan Ashraf and Shahzad Ahmad from Bytes for All and Lucy Purdon from IHRB provided invaluable support, without which this research project would not have been possible.

Copyright © 2018 (Ben Wagner). Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at <http://ijoc.org>.

Internet shutdowns in Pakistan during Eid in 2012 caused an estimated loss of 507 million Pakistani rupees (US\$49 million) to the exchequer, and November 2012 shutdowns during Ashura caused losses of 500 million rupees (US\$49.02 million; Purdon, Ashraf, & Wagner, 2015). These high costs would suggest that it is almost impossible for shutdowns to be a regular and ongoing occurrence; yet they still happen in Pakistan numerous times a year. This leads to the research question: Why are Internet shutdowns so frequent in Pakistan?

Internet shutdowns are a surprisingly common phenomena, having occurred in at least 23 countries over the past 10 years, including Syria (Gohdes, 2015), Nepal (Ang, Tekwani, & Wang, 2012), the Democratic Republic of Congo, Burundi, Ethiopia, Iraq, Kazakhstan, Pakistan, Sudan, Uzbekistan, Yemen, China, India,<sup>2</sup> Zimbabwe (Purdon, Ashraf, & Wagner, 2015), North Korea, Uganda, Bahrain, Bangladesh, Egypt, Turkey, Cameroon, Gambia (Micek & Access Now, 2017), and Myanmar (Howard, Agarwal, & Hussain, 2011a; Nizza, 2007),<sup>3</sup> with the best known being in Egypt in 2011 (OECD, 2011).

Although these are typically justified as security or public order measures, many of the shutdowns occur in the context of political rallies, elections, and public assemblies. Although there are clear security risks associated with such events, it remains an open question: What is being secured, and from whom? There are doubtless considerable elevated security concerns in Pakistan, but the timing of the shutdowns and the broad scale through which they are implemented suggests that governance measures are being implemented that go beyond reasonable security considerations alone.

Yet despite considerable interest in the case of Egypt in 2011, almost all shutdowns of communications—with the exception of Syria (Gohdes, 2015) and Nepal (Ang et al., 2012)—have frequently been ignored in the academic literature. The only publication that looks at an extended period before 2011 (Howard et al., 2011a) mainly lists incidents such as journalist's harassment or the shutdown of specific Internet sites or platforms rather than the shutdown of whole communications networks. Of the 606 incidents cataloged by Howard et al. (2011a), only four would constitute the kind of Internet shutdowns discussed in this article. The countries in which these shutdowns were conducted are Pakistan, blocking access in Balochistan; China, blocking access in the Xinjiang region; and Myanmar and Nepal, shutting down Internet access across the whole country.

### **Conceptualization: Defining Internet Shutdowns and Communicative Ruptures**

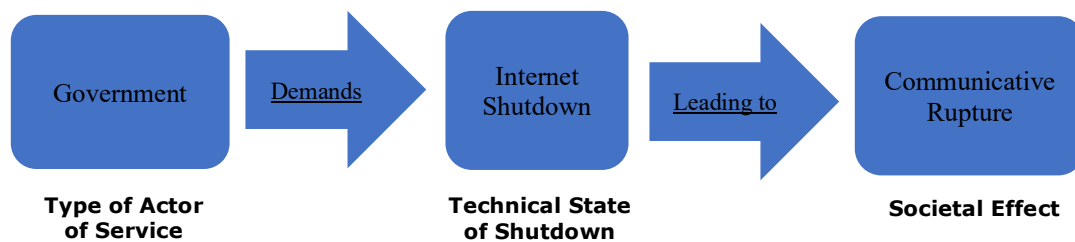
To understand why Internet shutdowns are so frequent in Pakistan, it is important to first clearly define them. In the context of this article, Internet shutdowns are defined as intentional disconnections of digital communications by government authorities. Such shutdowns frequently include shutting down the Internet and mobile phone services as well.

---

<sup>2</sup> See also <https://sflc.in/internet-shutdown-tracker-india-20132016>

<sup>3</sup> Within the context of the data from the Shutdown Tracker Optimization Project, only data that fit into the category shutdown type "full network" were considered, to ensure that they are congruent with the definition of Internet shutdowns used in this article.

However, in contrast to other definitions of shutdowns developed by Howard et al. (2011a) or Micek and Access Now (2017), the definition used here does not include the shutting down of large Internet platforms such as Facebook or YouTube. This definition is thus focused on the suppression of most digital communications mechanisms in a specific geographic area. To more accurately conceptualize the effects of Internet shutdowns, this article proposes the concept of communicative ruptures to help understand this relatively novel social phenomenon. Communicative ruptures are the intended effects of a shutdown; they are what happens in a society when communications networks are intentionally disconnected. Ruptures are not identical to the disconnection of Internet or mobile phone connectivity but instead are separate social phenomena that need to be studied in their own right (see Figure 1).



**Figure 1. Overview of definition of key concepts by the author.**

Importantly, what differentiates communicative ruptures from a simple technical failure is the intent of a governmental actor to disconnect networks. This intent is important, as it has specific effects on the way in which shutdowns affect local populations. Internet shutdowns are usually instituted by government actors in very specific contexts such as mass demonstrations, elections, perceived security threats, or counterterrorism operations. However, they also take place preemptively around events perceived as sensitive, such as mass public gatherings around national holidays or visits of high-ranking state officials.

Notably, societies across the world are increasingly dependent on communications infrastructure. Telecommunications, the Internet, and other information services have become critical social infrastructures (de Bruijne, van Eeten, Roe, & Schulman, 2006), woven into the communicative fabric of societies to the point that many citizens find it difficult to imagine living without them (Bank of America & Braun Research Inc, 2014; Tyers, 2013; York, 2010). In the context of postmodernity, space and place are increasingly in flux—not only condensed but also conditioned by communication (Harvey, 1993). At the same time, media communications are a key “locus of power and a contested political space” (Wagner, 2016, p. 4), which have historically been extensively governed by the state (Green & Karolides, 2005; Hoffmann-Riem, 1996). Governing the public sphere is seen as a key part of building nation states (Bhabha, 1990), but frequently leads to censorship and highly restrictive control of communications (D. Jones, 2001). Although Internet shutdowns are typically portrayed primarily as a means of censorship (Howard et al., 2011a), this portrayal may not entirely be accurate. Indeed, as the work of Gohdes (2015) and Purdon et al. (2015) suggests, Internet shutdowns serve numerous purposes beyond the suppression of information alone. Thus, it is important to study Internet shutdowns as a distinct phenomenon, separate from Internet censorship. The

main existing literature on Internet censorship was developed by the OpenNet Initiative, which has developed a concept of "generations" of Internet censorship, which they define as follows:

1. The first generation focused on "filtering systems at the backbone of the country's Internet . . . represents the first generation of Internet control techniques" (Deibert & Rohozinski, 2010a, p. 4).
2. The "second-generation controls aim to create a legal and normative environment and technical capabilities that enable state actors to deny access to information resources as and when needed" (Deibert & Rohozinski, 2010b, p. 24).
3. "The key characteristic of third-generation controls is that the focus is less on denying access than successfully competing with potential threats through effective counterinformation campaigns that overwhelm, discredit, or demoralize opponents" (Deibert & Rohozinski, 2010b, p. 27).
4. The "fourth phase . . . we call 'access contested.' Although the central characteristics of the previous phases remain relevant, the key notion of this phase . . . is that the contest over access has burst into the open" (Deibert, Palfrey, Rohozinski, & Zittrain, 2011, p. 14).

These approaches focus on influencing what information can be accessed and what information in the public sphere will be widely read. These forms of Internet censorship could therefore be surmised as a form of public sphere curation, as a specific authoritarian practice. By limiting access to specific content or specific websites or discrediting citizen journalism, Internet censorship is trying to shift and shape the public sphere.

By contrast, Internet shutdowns, as defined here as intentional blocking of almost all forms of digital communications, are very different phenomena. They differ from Internet censorship in several different ways:

1. Internet shutdowns do not discriminate regarding content. Instead, they block all content and do not attempt to discriminate what kind of content they block, whereas Internet censorship targets specific items or types of content.
2. Internet shutdowns encompass all forms of digital communication. Although Internet censorship only affects Internet communications, Internet shutdowns typically also directly affect mobile phone and sometimes even other forms of telephony. This makes the scope of communications affected significantly broader.
3. Internet shutdowns have different effects than Internet censorship, as they have an entirely different scope and the focus of the measure is different. Although in the context of Internet censorship some digital communication is still possible, and some

access to uncensored content exists, this is not the case during Internet shutdowns. As a result, communicative ruptures can only meaningfully be discussed in the context of Internet shutdowns and not in the context of Internet censorship.

4. Internet shutdowns have a different intent than does Internet censorship, as their focus is not on a specific piece of content but rather on the act of communication itself.

Thus, in the context of studying authoritarian governance mechanisms, it is important to differentiate between the two mechanisms, which are highly distinct and need to be studied accordingly.

Internet shutdowns should thus be considered a distinct phenomenon and are worthy of further study for several additional reasons. Politically, they are closely connected to human rights violations and threats to democracy and freedom. They are typically used in times of crisis and often deprive protestors of key means of communication and organization as well as depriving the surrounding society of associated services (Perera, 2015). They are also often used before elections to limit mobilization ability of certain political parties or social groups (Julliard, 2011). Sometimes governments will even try to hide their shutdown requests and claim that digital communications have failed because of a technical error (da Silva, 2015).

### **Internet Shutdowns as an Authoritarian Practice**

To say that Internet shutdowns manifest existing societal conflict is not to say that they take place without intent, however. If anything, the intent is crucial for understanding the phenomenon that is taking place. The authoritarian intent around shutdowns is also what differentiates shutdowns from simple technical errors. Rather—following Glasius's concept of authoritarian practices<sup>4</sup>—they are a measure that has a specific repressive effect on the population and attempts through its implementation to limit transparency and accountability. Importantly, communicative ruptures are not the same thing as Internet censorship, a similarly complex and important phenomenon. This is reinforced by the frequent linkage between communicative ruptures and mobile phone disconnections, heavily influencing the lifeworlds of individuals and the way they are able to interact with each other digitally as a society.

Building on the definition of authoritarian practices by Glasius and Michaelsen (2018), it is important to acknowledge the differences between the approach of this text and Glasius and Michaelsen's definition of authoritarian practices. Specifically, the suggestion that authoritarian practices "disable access to information and disable voice" (Glasius & Michaelsen 2018, p. 2) is an important but insufficient for conceptualizing Internet shutdowns. Rather they attack the fabric of society itself and attempt to prevent communicative interaction. This is not merely about preventing information getting out, but rather about preventing information from existing at all. Thus, this text proposes to extend that definition to encompass not just the disabling of access to information or voice but the active attack on the existence of voice

---

<sup>4</sup> See the Introduction of this Special Section.

(Michaelsen, 2016; O'Donnell, 1986). In this definition, the social effect of shutdowns is adequately reflected and integrated into a wider context of authoritarian practices.

However, this fits well into Glasius and Michaelsen's (see this Special Section) definition of "sabotaging of accountability" (p. 3). Both in their implementation and in their effects, shutdowns are actively constructed to limit the accountability of government in that they prevent political mobilization and public protest, prevent information about human rights violations from being documented and actively repress digital community relations in remote regions. As will be explained in greater detail below, the process that leads to shutdowns also actively hampers accountability by ensuring that it is essentially impossible to question or challenge the process. It is also possible to suggest that regular shutdowns make living in the affected areas more difficult, raising the likelihood of exit (i.e., leaving from the regions most affected by ruptures or even the whole country; Michaelsen, 2016; O'Donnell, 1986). However, this suggestion was not sufficiently studied within this article to make a definitive claim about its veracity.

Finally, there is a last important distinction in the way Glasius and Michaelsen (see this Special Section) use authoritarian practices and the way it is used here. In their definition, there is a "digital realm [where] illiberal practices typically constitute interferences with freedom of expression or the right to privacy" (p. 4). As I do not believe it is possible to meaningfully differentiate between digital and physical realm, I would argue instead for focusing on sociotechnical lifeworlds (Kitchin & Dodge, 2011) in which socially constructed technologies reside (Brey, 2005). Moreover, in this sociotechnical world, effects on lifeworlds are not just related to freedom of expression or privacy, but rather encompass all rights and all imaginable effects on human beings. In the specific case of Internet shutdowns, freedom of assembly and freedom of movement are heavily affected, but there will also be many other examples of authoritarian practices where both intent and effect are not primarily oriented on freedom of expression. Thus, this article argues instead for considering authoritarian practices—whether digitally mediated or otherwise—as having a considerable intentional effect on human rights in a manner that actively sabotages accountability.

### **Case Selection and Methodology**

Within this context, Pakistan is by far the most interesting case internationally. No other country can even come close to the 41 Internet shutdowns Pakistan has witnessed in the past five years. Shutdowns have become so common that they are an established part of precautionary measures taken within the security apparatus. For example, to prepare for celebrations around Defense Day in Pakistan on September 6, 2016, the government decided to shut down communications in the capital city not just on the day itself but also as a precaution during the preparations on September 5, 2016. Similar precautions were taken for the ceremony celebrating the Change of Command for the chief of the Army staff in Rawalpindi on November 29, 2016, where mobile phone and Internet services were shut down in the entire city as a security precaution. Thus, Pakistan represents a particularly interesting case that is worthy of further study.

Having selected Pakistan as a case, the field research consisted of several research trips to Pakistan, from November 10 to 19, 2014, and from February 2 to March 1, 2015. During these field trips, 23 expert interviews (Mason, 2002, p. 231) were conducted using nonprobability chain sampling (Tansey, 2007) with current and former government officials, members of civil society, NGOs, and representatives of

private sector companies. The purpose of these interviews was to understand the actual decision-making process behind Internet shutdowns in Pakistan, as well as the motivations of actors involved in the shutdown process.

Studying this phenomenon is relatively difficult in Pakistan, as it is a highly sensitive matter that is frequently discussed in terms of national security, and most interview partners were only willing to speak on condition of anonymity. As a result, details were removed from interviews that would allow for the names, identities, or professional positions of interviewees to be identified.

Because of the sensitivity of the questions being asked, it was often necessary to contact interviewees through trusted intermediaries. Access to these interviews was typically made possible either through collaboration with Bytes for All or IHRB, who were crucial in helping to set up interviews. Although this brings with it issues related to the role of these organizations as gatekeepers (Parsons, Johnson, Warnecke, & Kaluzny, 1993), no issues related to their role as a gatekeeper transpired during the interview process. Through conducting these interviews, it was possible to build an accurate picture of the decision-making process around Internet shutdowns in Pakistan.

Based on data from media reports and individual reports collected in Pakistan, Bytes for All was able to document 41 Internet shutdowns between 2012 and 2017, which it has published on <http://www.killswitch.pk/>. These data from Pakistan are also included as part of the international KeepItOn campaign by the NGO AccessNow, which has developed its own shutdown tracker.<sup>5</sup> The Bytes for All database was used as the basis for the data used in this article about the frequency of and reasoning for Internet shutdowns in Pakistan. Together with the Bytes for All data and additional publicly available online media sources used to corroborate the data provided by Bytes for All, a time series of all 41 shutdowns from 2012 to 2017 was developed and can be seen below.

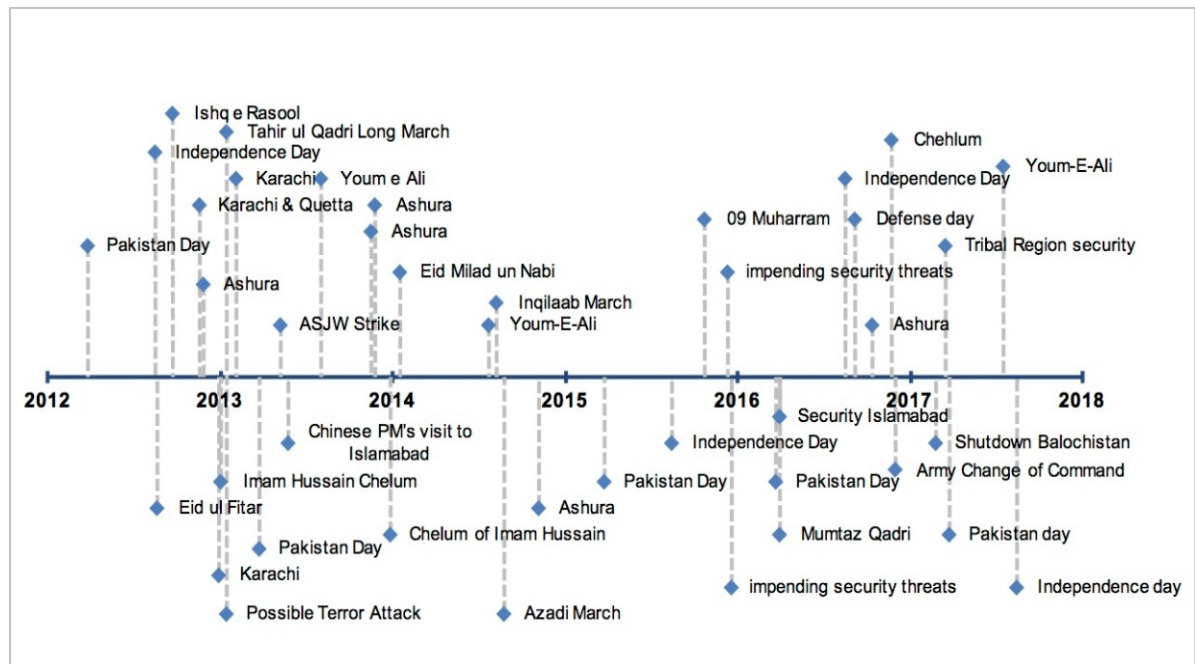
### ***Internet Shutdowns in Pakistan***

Internet shutdowns first took place in Pakistan in 2005 as part of a wider military and anti-insurgency campaign in Balochistan (El-Khawas, 2009, p. 103). However, similar ruptures did not take place in the rest of Pakistan until 2012, when the Interior Minister Rahman Malik began ordering mobile network shutdowns. Since then, they have remained a relatively consistent occurrence in Pakistan and continue to this day. The frequency of these shutdowns varies but has remained relatively consistent in the past five years, as shown in Figure 2.

---

<sup>5</sup> See <https://www.accessnow.org/keepiton-shutdown-tracker/> for further details.





**Figure 2. Overview of Internet shutdowns in Pakistan from 2012 to 2017.**<sup>6</sup>

The scope of the shutdowns is also extremely variable and ranges from parts of Islamabad to the entire country. Some requests for shutdowns are also extremely diverse in their effects, "impact[ing] a total of 56 cities and towns in the regions of Punjab, Sindh, Khyber Pakhtunkhwa, Balochistan, Gilgit-Baltistan and Azad Kashmir" (Purdon et al., 2015, p. 18). However, there are certain patterns that emerge when looking more closely at the data of shutdowns. They can broadly be categorized into short term shutdowns (up to one week) and long-term shutdowns (several weeks or months).

Within the short-term shutdowns, these generally fall into the following five categories:

1. Celebrations around national political holidays, like Pakistan Day or Independence Day.
2. Celebrations around religious holidays, like Ashura or Eid ul-Fitar.

<sup>6</sup> The overview is based on data from <http://www.killswitch.pk/>, which is collected and published by Arsalan Ashraf at Bytes for All. Based on previous collaboration with Bytes for All, which include research and data collection trainings conducted by the author in Islamabad, the author is confident that the data collected is sound.

3. Large political marches, strikes, or sit-ins, typically in the capital city Islamabad or Rawalpindi (which are both very close to each other and are often considered to be twin cities in one large metropolitan area), but also elsewhere in the country.
4. High-level political events, such as the visit of the Chinese prime minister or the Change of Command in the Armed Forces.
5. Perceived security threats, typically unspecified, which require shutdowns as a precaution.

The above Internet shutdowns typically take place for one day, although they are sometimes extended for up to a week. Such short-term shutdowns need to be seen in a distinct context from long-term shutdowns that take place for longer periods of weeks or months. These types of shutdowns typically take place in remote parts of Pakistan, such as Balochistan or the tribal region ("Suspension of Mobile Phone Services," 2017). To provide just two of the most recent examples:

- On March 15, 2017, the Pakistani government "suspended all mobile phone services throughout the entire tribal [region] without any notice and unknown reason at once" ("Suspension of Mobile Phone Services," 2017, para. 1). The disconnected mobile phone networks had not been restored almost four months later on July 9, 2017, as "mobile phone services remained suspended" ("Mobile Phone Services," 2017, para. 1).
- In February 2017, the Pakistani government suspended Internet services in Dalbandin, a city in the Balochistan region. Six months later, on August 19, 2017, the shutdown was still in place, and it was unclear when Internet connectivity would be restored.

The above overview was meant to provide a more general picture of Internet shutdowns in Pakistan without going into too much detail about the reasons for shutdowns. How and why short-term and long-term shutdowns take place will be explained in greater detail in the following sections.

### ***The Process That Leads to Shutdowns in Pakistan***

The process of shutdowns within Pakistan needs to be seen within the context of the overall political system there. The Pakistani civilian government is relatively weak and faced with a strong military, which has far greater power (Idris, 2016). Like other countries that have exemplified similar politically powerful military forces like Turkey, the Pakistani military enforces its power through regular coups to topple unfriendly civilian governments, which were conducted in 1958, 1977, and 1999 (Narli, 2000). Communications shutdowns are one of the examples of such engagement, with strong suggestions in the interviews conducted in Pakistan that a considerable proportion of shutdown orders stem directly from the Pakistani military.

These shutdown orders from the military and other security agencies are sent to the National Crisis Management Cell (NCMC), a unit within the interior ministry responsible for liaising between military and civilian agencies. The NCMC typically makes a determination on shutdowns, although one interviewee with experience working in the Pakistani government described the process of issuing a shutdown order as "mechanical."<sup>7</sup> Because the issue of Internet and mobile phone shutdowns "relates to national security,"<sup>8</sup> there is an unwillingness among political parties and parliamentarians to challenge the measure or even talk about them widely.

Beyond this, it seems that Internet shutdowns as a precautionary measure had already, at the end of 2014, become "part of the standard operating procedures"<sup>8</sup> of the NCMC in various situations that were perceived as relevant to national security. This mechanical and standardized approach to decision making around shutdowns would help to explain considerably why shutdowns are so frequent and seem to have become so "normal" in Pakistan. There are some examples where the decision is also taken by another specialized unit within the Ministry of Interior, such as the National Counter Terrorism Authority (NCTA; Bhatti, 2014), but in the majority of cases, the decision for shutdowns is taken within the NCMC.

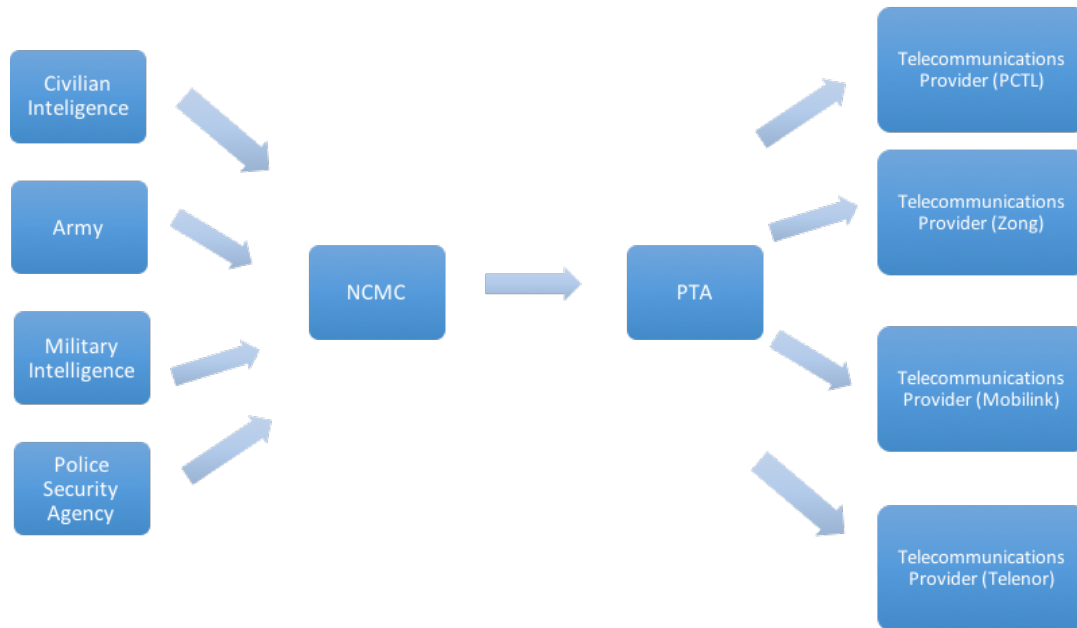
The decisions made by the NCMC or other units within the Ministry of Interior are then sent to the Pakistan Telecommunication Authority (PTA). The PTA is a classic telecommunications regulator, similar to those that exist in many different countries, and is responsible for implementing government telecommunications policy in numerous different areas, for example, by licensing telephone and Internet providers in Pakistan. It is also responsible for enforcing Internet censorship decisions, with 597 links required to be removed by the PTA from 2006 to 2013.

Although the PTA is the "enforcement agency," it does not have the capability to question the decision or the manner of its enforcement. It simply has to ensure that the shutdowns take place and has the ability to fine telecommunications operators that do not comply, and in the most extreme cases it could theoretically withdraw their telecommunications license. The orders are issued by the PTA under section 54 of the 1996 Pakistan Telecommunications (Re-organization) Act. As noted by an interviewee who runs a leading telecommunications company in Pakistan, NCMC has "no public interface,"<sup>8</sup> and its determinations of a national security threat cannot be contested. As a result, it is impossible for telecommunications companies to challenge decisions of the NCMC, as their decisions cannot be scrutinized. This is particularly the case as there is no formal legal process to authorize shutdowns, but rather an established practice over time that the NCMC will typically take responsibility. But sometimes shutdown orders will also be issued by another unit within the Ministry of Interior, such as the NCTA (see Figure 3).

---

<sup>7</sup> Interview with former senior Pakistani government official, November 12, 2014.

<sup>8</sup> Interview with head of large communications company in Pakistan, November 13, 2014.



**Figure 3. Process of decision making about Internet shutdowns in Pakistan.**

The result is a lack of accountability of decisions on Internet shutdowns, within which both the providers who have to implement the shutdowns as well as the citizens affected by it have no form of legal recourse to challenge the decision. This ambiguity in which authority is even responsible for issuing shutdown orders further challenges even basic accountability, with decisions frequently made by the NCMC but sometimes also authored by the NCTA. Moreover, the decisions are publicly justified on such a vague basis, such as “impending security threats,”<sup>9</sup> that they are very difficult to contest politically. The nature of the decisions made is thus evidently constructed in a manner to evade accountability and can thus be considered an authoritarian practice.<sup>9</sup> This is particularly the case given the military–civilian imbalance in Pakistan, where the military wishes to influence everyday politics, but is often unable to do so overtly.

This unaccountable decision-making process is also evident in the vague public statements made by public authorities when shutting down communications; for example, the “mobile phone service in the region was suspended owing to security reasons. It was meant to further improve law and order in the agency especially in the border areas” (“Mobile Phone Service Suspended,” 2016, para. 6).

The current system of lacking accountability and unclear authorship shields both the Pakistani military from having to publicly take responsibility for a shutdown as well as the responsible agency within the Ministry of Interior from having to justify its choices and the intelligence these choices are based on to

<sup>9</sup> See Glasius and Michaelsen’s contribution to this Special Section.

the general public. While they can of course benevolently choose to do so as they see fit, this process neither promotes accountability nor provides checks and balances to limit or prevent shutdowns within the existing process of governance.

### ***How Did the Concept of Internet Shutdowns Reach Pakistan?***

It is hard to say for certain where Internet shutdowns as a policy measure originally come from. The following paragraphs are thus an attempt to understand plausible paths of development and the dissemination of authoritarian practice.

As there is a considerable body of military literature on “disrupting enemy communications” (Royal Institute of International Affairs, 1944, p. 558), and many of the earliest Internet shutdowns were employed as an anti-insurgency or antiterror tactic, it seems plausible that the origins of such shutdowns may be in military circles. The origin of Internet shutdowns may be in Northern Ireland, where communications jamming was commonly used to prevent the detonation of bombs and to prevent oppositional radio broadcasts (Oppenheimer, 2009). It would be plausible that such tactics could conceivably have traveled from Northern Ireland to Afghanistan and Iraq, where in both countries providing mobile connectivity was a central part of anti-insurgency military strategies (Shapiro & Siegel, 2015). However it should be noted that while in Afghanistan mobile phone towers were actively attacked by the Taliban—leading new towers to be primarily built on U.S. military bases for protection (Glanz & Markoff, 2011)—access to the Internet was far more heavily contested in Iraq, where providing or removing Internet access was a key part of the anti-insurgency strategy of the military coalition there (Shapiro & Siegel, 2015).

From Iraq and Afghanistan, it is plausible that the strategy of shutdowns could then have traveled to Balochistan, where it was first employed by the Pakistani government in 2005. In Balochistan and in the tribal regions primarily, long-term shutdowns were common until 2012, when shutdowns began to spread to other parts of the country. It is quite possible that the reason for this spread was not an internal Pakistani but rather an external event: the shutdowns of mobile and Internet communications in Cairo and other parts of Egypt during the Arab uprisings. Before this event in Cairo—which was the highest profile shutdown event up until then—shutdowns were a relatively uncommon event at a global level. This is not to say that Cairo was necessarily a successful event of a shutdown—far from it. Rather, the events around the Internet and telephone shutdown in Cairo exemplified to a global audience that shutdowns were possible. It thus serves less as a good example of effectiveness and rather as a proof of concept that governments have the capacity to take such measures.

### **Why Are Shutdowns So Frequent in Pakistan?**

When asking why shutdowns are so frequent in Pakistan, security threats alone do not seem to be a sufficient explanation. While Pakistan doubtless faces numerous security threats, so do many other countries. As noted by one of the interviewees with experience of working in government, “many countries face terrorism . . . they don’t block . . . why do we?” Because of the secretive nature of national security justifications, it is impossible to assess the actual effectiveness of shutdowns in increasing security and

preventing terrorism effectively. In the context of promoting security, two arguments are typically made in favor of Internet and mobile phone shutdowns.

First, it is typically suggested that mobile phones can be used as a trigger for explosive devices. While this is certainly true, there are numerous other trigger mechanisms for explosive devices, and shutting down communications across a whole country for hours, days, or weeks does not seem like a particularly effective mechanism to prevent the usage of explosive devices. Indeed, it seems that terrorist groups in Pakistan have adapted to use numerous forms of explosive devices going beyond mobile-phone triggers alone (Barker, 2011; S. G. Jones & Johnston, 2013).

Second, Internet communications can be used to spread information swiftly. In politically tense situations, it is argued that the swift spread of information can have harmful side effects, such as political violence or social unrest. Although there are some cases where this has happened,<sup>10</sup> the core of the latter argument seems to be to prevent political mobilization. Although disrupting communications may be one way of doing this, it is by no means the only way and has considerable side effects. Moreover, the propensity of misuse of these types of shutdowns is high, particularly in the context of mass mobilization and political events such as rallies or elections. A particular likelihood of violence is easy to construct around large groups, and doing so—if preventing the mobilization is successful—can change the course of a demonstration or an election.

### ***Strategic Prevention of Political Mobilization***

This also seems to be the context of numerous shutdowns within Pakistan. When the government felt threatened by large rallies by political opposition, particularly in the capital city Islamabad or the surrounding area of Rawalpindi, there is a strong tendency to shut down mobile and Internet communications, often for several days. Here, the strategic implementation of shutdowns is less linked to preventing violence and more to suppression of political opponents. Shutdowns are used during political demonstrations, at rallies, or at large mass protests.

The most obvious example of shutdowns being used to prevent political mobilization is during the Azadi and Inqilab marches of 2014, which were, for a while, suspected to topple the Pakistani government with their demands for the resignation of then Prime Minister Nawaz Sharif due to irregularities in the national elections (Idris, 2016; Tariq, 2014). In response, the government shut down mobile phone and Internet communications for several days, and in some cases up to a week in many of the places where the march took place, such as Islamabad (August 13–14, 2014; August 23–27, 2014) and Lahore (August 8–13, 2014).

An even more obvious example of preventing political mobilization is the Internet shutdowns during the Tahir ul Qadri Long March, which took place to “protest government’s corruption” (Attaa, 2013). During the march from Lahore to Islamabad, communications were shut down in every location through which the March passed. Thus, shutdowns took place in mid-January 2013 in Karachi, Sindh, Islamabad, Faizabad,

---

<sup>10</sup> See <https://dangerousspeech.org/> for further details.

Shahdara, Punjab, Shahdra, Minar-e-Pakistan, Lahore, Do Moria Pull, Garhi Shahu, Dharampura, Shahrah-e-Quaid-e-Azam, and Ichhra (Attaa, 2013). The Pakistani government even went as far as shutting down communications on specific roads that the March was passing through, as such the Imamia Colony Road and the Ravi Bridge. Although ostensibly to protect the security of those marching, the intended effect was evidently to prevent the mobilization of additional Pakistani citizens in close proximity to those marching.

### ***Communicative Ruptures: A Punitive Disciplinary Tool***

Notably, these kinds of shutdowns around political marches or mass demonstrations are limited in time to a maximum of a week. They are thus in contrast to some of the long-term shutdowns that take place in some of the more fringe parts of Pakistan, such as Balochistan or the tribal region. This distinction in the approach to shutdowns is important, as it suggests that there may be different intent involved. As will be argued here, the month-long shutdowns common in Balochistan and the tribal region follow a different logic, which is less about strategically preventing mobilization and more a disciplinary tool of authoritarian repression.

To understand why such shutdowns take place, it is important to understand the role of remote regions like Balochistan in Pakistan. The shutdowns can be seen part of a wider struggle between Balochistan and the national Pakistani government for greater recognition and more political independence (Wirsing, 2008). The increasing relevance of Balochistan energy resources and networks for national Pakistani strategic interests is evident, as "sprawling, mineral-rich Balochistan is the largest province of Pakistan and constitutes approximately 44% of the country's total land mass" (Ahmad & Dad, 2011, para. 1).

These conditions have led the Pakistani government to employ a policy of "zero tolerance and ruthless crushing of the insurgency" (Wirsing, 2008, p. vi). Within this context, frequent, long-term communications shutdowns were exceedingly common since 2005. Although it has not been possible to document the exact number of communicative ruptures, individuals familiar with the matter suggest that they are both common and very extensive, lasting for weeks or months, and taking place many times per year. Similarly,

the Federally Administered Tribal Areas (FATA) has for many decades been marginalized. . . . Furthermore, prior to . . . August 2011 no political representation was allowed to function in the tribal areas. In the absence of a vibrant political process, there has been no platform to address grievances or to contribute to local or national affairs. (Shinwari, 2012, pp. 17–19)

Much like Balochistan, there are ongoing struggles between the central political administration and remote region for recognition and agency within the Pakistani process of governance. Shutdowns thus need to be seen in this context, within which specific remote regions experience long-term punitive shutdowns that are difficult to explain, other than as a repressive measure.

### ***Denying the Existence of "Others" Over Extended Periods***

However, simply describing such measure as punitive, repressive, or disciplinary does not fully do them justice. It is important to note in this context that this is not just any form of disciplinary interaction, but rather one that specifically targets everyday societal communications. In Pakistan, government actors frequently initiate network disconnections to target the activities of specific, often-marginalized groups. Social life for large portions of the population can be considerably slowed and reduced to in-person encounters or one-to-many communication through TV or radio. Space and "symbolic proximity" (Wurtzel & Turner, 1976) are also significantly expanded, as the distance becomes far more difficult to traverse. In Pakistan, conflicts between groups in society manifest themselves both through forms of physical conflict and through the configuration of technological infrastructure. Thus, communications shutdowns serve—to a certain degree—to define who is part of Pakistani society and who is not.

Those who are disconnected are quite literally unable to speak in digital form, both to each other and to the outside world. This behavior suggests that the Pakistani government does not consider political protestors or ethnic minorities, such as the Balochs or those inhabiting the tribal region, full parts of Pakistani society. Thus, their disconnection from the communicative interaction is not just a technical but also a symbolic act, serving both as a way to discipline a group and define their identity as "others" within society.

This form of exclusion is a more extreme form of what scholars have found to be a prevalent link between communications access and the exclusion of specific ethnic groups (Weidmann, Benitez-Baleato, Hunziker, Glatz, & Dimitropoulos, 2016). The exclusion of such ethnic groups from Internet service provision is suggested to be a result of political bias by Weidmann et al. (2016), an assumption that also holds true in Pakistan. Indeed, it may be that the effects of a lack of Internet services provisions are amplified by the frequent disconnections for which little Internet service exists. However, it can be also be argued that the lack of Internet penetration has a different symbolic effect on the affected population than the forcible removal of Internet and mobile phone connectivity over a specific period of time.

Although a lack of access is likely to have longer term structural effects, the latter is likely to be more symbolically violent in separating parts of a society from others. It can also be seen as a mechanism for preventing communicative interaction between members of a community over an extended period of time, essentially a way to "atomise" (Glasius, 2012, p. 362) individuals digitally and separate them from other individuals within their society. Glasius suggests that many Latin American and Eastern European activists conceive of this atomization of individuals as a key form of authoritarian rule, as authoritarian regimes aspire "to freeze and 'atomise' society in order to rule for ever" (Glasius, 2012, p. 362). In this context, long-term communicative ruptures could be seen as a similar authoritarian mechanism to atomize society to prevent the creation of civil societies. At the same time, ruptures have direct effects on the ability of a subaltern population to speak for themselves (Spivak, 1988). This is particularly the case in FATA, which has more limited political agency than other parts of the country, and the people living in these areas are still, in many cases, quite literally "spoken for" by the FATA administration.

Importantly, communications shutdowns are a key tool to restrict information about the conflict and the demands of people in Balochistan reaching the outside world:



Baloch groups have been waging a nationalist insurgency to protest against the province's underdeveloped conditions; state security forces have tried to suppress this insurgency through the abduction, torture, and extrajudicial killings of Baloch separatists and human rights activists, and have successfully censored most mainstream media coverage of the province. To counter the media vacuum, Baloch activists have launched online newspapers, blogs, Facebook groups, and video-sharing channels to facilitate communication, document human rights violations, and share photographs of missing persons believed to have been abducted by state security forces. (Yusuf, 2013, p. 43)

Thus, not only does shutting down communications make the everyday lives of marginalized groups more difficult, it also prevents them from "existing" in a communicative digital context. They are unable to document their existence online and make the outside world aware of human rights violations (unrelated to the Internet) taking place within their region. Through shutting down the Internet, they have far greater difficulty making their voices heard to the national and international communities. Here, too, shutting down the Internet serves to prevent transparency and accountability of government action in the tribal areas, as the shutdown serves to hide information that would otherwise exist both about a part of the population living in a remote area and their specific struggles and conflicts.

Of course, this denying the existence of "others" could also be interpreted as a form of strategic prevention of the sharing of information about human rights violations. In this sense, these measures also have a strategic component in that they prevent voice and agency for the affected populations. The point of the tactics described here is not about denying their strategic component, but rather to argue that the motivation goes deeper than just preventing information getting out or preventing political mobilization.

### **Internet Shutdowns as an Authoritarian Practice**

Communications technologies play an important role in society, and as their importance grows, so too does the interest in misusing as the basis for authoritarian practices. They extend the reach of the state even more deeply into the communicative lifeworlds of individuals.

Having put forward several theories on why shutdowns happen in Pakistan and how they became normal, this article argues that there are strong reasons for the Pakistani state to shut down the Internet that have little to do with security or public order. Instead, Internet shutdowns are a strategic measure to prevent mobilization and prop up the state, as well as a disciplinary measure to prevent marginalized "others" from taking part in the national political debate and documenting their grievances. This separation quite literally creates digital boundaries not just to the outside world but within communities themselves, limiting their ability to communicate among themselves. As such, it is a much more repressive authoritarian practice governance mechanism than simply censoring certain websites or denying a community access to the Internet.

As noted above, the intention of sabotaging accountability runs through both intended effects of the shutdowns and their implementation. By (a) preventing the contestation of shutdowns by providing an untransparent and incontestable process around the decision to shut down communications, and (b) shutting

down communications in Balochistan over an extended period of time, making it far more difficult to document the violent anti-insurgency campaigns there, both mechanisms serve to sabotage accountability for the actions of the Pakistani government and, in particular, its military and security services.

Although some attempts were made to trace the process around the development of Internet shutdowns as a political measure, further work is still clearly required in this area. Although the ideas of a military origin of Internet shutdowns in Northern Ireland seem plausible, they require further documentation and research to clarify the exact causal mechanism. What is clear, however, is the highly political usage of shutdowns within the context of a political struggle. It seems relatively clear that this concept became popular after the shutdown events in Cairo and has since been commonly used throughout Africa and Asia. Most recently, Cameroon has begun to emulate Egypt and Pakistan and conducted a shutdown for more than three months in the English-speaking part of an otherwise French-speaking country (Kazeem, 2017). While the English-speaking part of Cameroon is not as heavily marginalized as Balochistan is in Pakistan, similar dynamics of disconnecting the region from the national political debate, punishing them for protesting the national government, demanding greater independence, and preventing further political mobilization are also evident in Cameroon.

Beyond Cameroon and Pakistan, there is an urgent need for scholars not just to look at Internet shutdowns technically from afar but to engage with the local political dynamics of how shutdowns happen. Only when the authoritarian dynamics of shutdowns and communicative ruptures are better understood will it be possible to meaningfully understand and respond to both.

### **Epilogue**

On the February 26, 2018, as this article was being finalized, the Pakistan High Court declared Internet shutdowns in Pakistan "as illegal and disproportionate response to security threats" (Bytes for All, 2018, para. 1). The judgement suggests that the concept of national security is being overextended and that justifying Internet shutdowns using "apprehensions relating to public safety, law and order or the happening of an untoward incident" (Minallah, 2018, p. 12) can be justified by "by no stretch of the imagination" (Minallah, 2018, p. 12). Internet shutdowns could only be justified under a national state of emergency following an official "Proclamation of Emergency by the President of Pakistan" (Minallah, 2018, p. 13). Although the High Court decision was able to hold the PTA accountable as the actual author of legal requests to Internet providers, it does not even mention the NCMC or their decision-making process. Thus, while the High Court was able to prevent civilian authorities to account, whether this constitutes actual accountability remains to be seen.

### References

- Ahmad, S., & Dad, N. (2011). *Pakistan: Internet rights and democratisation*. Retrieved from <https://www.giswatch.org/en/country-report/freedom-expression/pakistan>
- Ang, P. H., Tekwani, S., & Wang, G. (2012). Shutting down the mobile phone and the downfall of Nepalese society, economy and politics. *Pacific Affairs*, 85(3), 547–561.
- Attaa, A. (2013, January 13). *Mobile phone services to remain blocked during Qadri's Long March*. Retrieved from <https://propakistani.pk/2013/01/13/mobile-service-blocked-qadri-long-march/>
- Bank of America, & Braun Research Inc. (2014). *Trends in consumer mobility report 2014*. Charlotte, NC: Bank of America.
- Barker, A. D. (2011). Improvised explosive devices in southern Afghanistan and western Pakistan, 2002–2009. *Studies in Conflict & Terrorism*, 34(8), 600–620.
- Bhabha, H. K. (1990). DissemiNation: Time, narrative and the margins of the modern nation. In H. K. Bhabha (Ed.), *Nation and Narration* (p. 333). Abingdon, UK: Routledge.
- Bhatti, S. I. (2014). Mobile phone services being suspended in parts of Islamabad: PTA. *Dawn*. Retrieved from <http://www.dawn.com/news/1124907>
- Brey, P. (2005). Artifacts as social agents. In H. Harbers (Ed.), *Inside the politics of technology: Agency and normativity in the co-production of technology and society* (pp. 61–84). Amsterdam, Netherlands: Amsterdam University Press.
- Bytes for All. (2018, February 26). *Verdict: Islamabad high court declares network disconnections as illegal*. Retrieved from <https://bytesforall.pk/post/verdict-islamabad-high-court-declares-network-disconnections-illegal>
- da Silva, I. S. (2015). DRC govt cuts Internet, SMS to quell deadly protests. *Biztech Africa*. Retrieved from <http://www.biztechafrika.com/article/drc-govt-cuts-internet-sms-quell-deadly-protests/9574/#.VhzgaxPzquV>
- de Bruijne, M., van Eeten, M., Roe, E., & Schulman, P. (2006). Assuring high reliability of service provision in critical infrastructures. *International Journal of Critical Infrastructures*, 2(2), 231–246.
- Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (2011). Access contested: Toward the fourth phase of cyberspace controls. In R. Deibert, J. Palfrey, R. Rohozinski, & J. Zittrain (Eds.), *Access contested security, identity, and resistance in Asian cyberspace information revolution and global politics* (pp. 3–20). Cambridge, MA: MIT Press.

- Deibert, R., & Rohozinski, R. (2010a). Beyond denial. In R. Deibert, J. G. Palfrey, R. Rohozinski, & J. Zittrain (Eds.), *Access controlled: The shaping of power, rights, and rule in cyberspace* (pp. 3–14). Cambridge, MA: MIT Press.
- Deibert, R., & Rohozinski, R. (2010b). Control and subversion in Russian cyberspace. In R. Deibert, J. G. Palfrey, R. Rohozinski, & J. Zittrain (Eds.), *Access controlled: The shaping of power, rights, and rule in cyberspace* (pp. 15–34). Cambridge, MA: MIT Press.
- El-Khawas, M. A. (2009). Musharraf and Pakistan: Democracy postponed. *Mediterranean Quarterly*, 20(1), 94–118. doi:10.1215/10474552-2008-037
- Glanz, J., & Markoff, J. (2011). US underwrites Internet detour around censors. *The New York Times Reprints*, p. 1. Retrieved from <https://commotionwireless.net/files/U.S.%20Underwrites%20Internet%20Detour%20Around%20Censors.pdf>
- Glasius, M. (2012). Dissident writings as political theory on civil society and democracy. *Review of International Studies*, 38(02), 343–364. doi:10.1017/S0260210511000155
- Glasius, M., & Michaelsen, M. (2018). Prologue: Illiberal and authoritarian practices in the digital sphere. *International Journal of Communication*, this Special Section.
- Gohdes, A. R. (2015). Pulling the plug: Network disruptions and violence in civil conflict. *Journal of Peace Research*. doi:10.1177/0022343314551398
- Green, J., & Karolides, N. J. (2005). *The encyclopedia of censorship*. New York, NY: Facts on File.
- Harvey, D. (1993). From space to place and back again: Reflections on the condition of post-modernity. In J. Bird (Ed.), *Mapping the futures: Local cultures, global change* (pp. 3–29). London, UK: Routledge.
- Hoffmann-Riem, W. (1996). *Regulating media: The licensing and supervision of broadcasting in six countries*. New York, NY: Guilford.
- Howard, P. N., Agarwal, S. D., & Hussain, M. M. (2011a). *The dictators' digital dilemma: When do states disconnect their digital networks?* Retrieved from [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2568619](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2568619)
- Howard, P. N., Agarwal, S. D., & Hussain, M. M. (2011b). When do states disconnect their digital networks? Regime responses to the political uses of social media. *The Communication Review*, 14(3), 216–232.

- Idris, S. (2016). Challenge of democracy and local governance in Pakistan. In U. Sadioglu & K. Dede (Eds.), *Comparative studies and regionally-focused cases examining local governments* (pp. 259–279). Hershey, PA: IGI Global.
- Jones, D. (2001). *Censorship: A world encyclopedia*. London, UK: Fitzroy Dearborn.
- Jones, S. G., & Johnston, P. B. (2013). The future of insurgency. *Studies in Conflict & Terrorism*, 36(1), 1–25. doi:10.1080/1057610X.2013.739077
- Julliard, J.-F. (2011). *Government lifts three-week-old ban on texting*. Retrieved from <http://en.rsf.org/democratic-republic-of-congo-after-disputed-election-sms-22-12-2011,41597.html>
- Kazeem, Y. (2017). *The Internet shutdown in English-speaking parts of Cameroon is finally over*. Retrieved from <https://qz.com/964927/caemroons-internet-shutdown-is-over-after-93-days/>
- Kitchin, R., & Dodge, M. (2011). *Code/space software and everyday life*. Cambridge, MA: MIT Press.
- Mason, J. (2002). Qualitative interviewing: Asking, listening and interpreting. In T. May (Ed.), *Qualitative research in action*. London, UK: SAGE Publications.
- Micek, P., & Access Now. (2017). *Shutdown tracker optimization project here*. Retrieved from <https://www.accessnow.org/cms/assets/uploads/2017/09/Shutdown-Tracker-Optimization-Project.xlsx>
- Michaelsen, M. (2016). Exit and voice in a digital age: Iran's exiled activists and the authoritarian state. *Globalizations*, 1–17. doi:10.1080/14747731.2016.1263078
- Mobile phone service suspended in Bajaur. (2016, March 16). *Dawn*. Retrieved from <http://www.dawn.com/news/1245999>
- Mobile phone services remain suspended in Mohmand Agency. (2017, July 9). *Tribal News Network*. Retrieved from <http://www.radiotnn.com/mobile-phone-services-remain-suspended-in-mohmand-agency/>
- Minallah, A. (2018). F.A.O. 42-2016. Islamabad High Court, Islamabad Judicial Department [Judgment sheet]. Retrieved from <http://mis.ihc.gov.pk/attachments/judgements/F.A.O.%2042-2016%20Against%20Order%20-finalFAONo.42of2016.CMPakLimitedv.ThePTA,etc.636552442049031490.pdf>
- Narli, N. (2000). Civil-military relations in Turkey. *Turkish Studies*, 1(1), 107–127.

- Nizza, M. (2007). Burmese government clamps down on Internet [Web log post]. Retrieved from <https://thelede.blogs.nytimes.com/2007/09/28/burmese-government-clamps-down-on-internet/>
- O'Donnell, G. A. (1986). *On the fruitful convergences of Hirschman's exit, voice, and loyalty and shifting involvements: Reflections from the recent Argentine experience*. Notre Dame, IN: Helen Kellogg Institute for International Studies, University of Notre Dame.
- OECD (Organization for Economic Cooperation and Development). (2011). *The economic impact of shutting down Internet and mobile phone services in Egypt*. Retrieved from <http://www.oecd.org/countries/egypt/theeconomicimpactofshuttingdowninternetandmobilephoneservicesinegypt.htm>
- Oppenheimer, A. R. (2009). *IRA, the bombs and the bullets: A history of deadly ingenuity*. Dublin, Ireland: Irish Academic Press.
- Parsons, J. A., Johnson, T. P., Warnecke, R. B., & Kaluzny, A. (1993). The effect of interviewer characteristics on gatekeeper resistance in surveys of elite populations. *Evaluation Review, 17*(2), 131–143. doi:10.1177/0193841X9301700201
- Perera, S. M. (2015). *Accessing the inaccessible: The uses and abuses of crowdsourcing in gathering data in the eastern Democratic Republic of Congo*. New Orleans, LA: International Studies Association.
- Purdon, L., Ashraf, A., & Wagner, B. (2015). *Security v access: The impact of mobile network shutdowns*. London, UK: Institute for Human Rights and Business.
- Royal Institute of International Affairs. (1944). Outline of military operations. *Bulletin of International News, 21*(14), 555–563.
- Shapiro, J. N., & Siegel, D. A. (2015). Coordination and security: How mobile communications affect insurgency. *Journal of Peace Research, 52*(3), 312–322.
- Shinwari, N. A. (2012). *Understanding FATA: Attitudes towards governance, religion and society in Pakistan's Federally Administered Tribal Areas* (Vol. 5). Islamabad, Pakistan: CAMP.
- Spivak, G. C. (1988). Can the subaltern speak? In R. C. Morris (Ed.), *Can the subaltern speak? Reflections on the history of an idea* (pp. 21–78). New York, NY: Columbia University Press.
- Suspension of mobile phone services creates problems for tribesmen. (2017, June 18). *Tribal News Network*. Retrieved from <http://www.radiotnn.com/suspension-of-mobile-phone-services-creates-problems-for-tribesmen/>
- Tansey, O. (2007). Process tracing and elite interviewing: A case for non-probability sampling. *PS: Political Science & Politics, 40*(4), 765–772.

- Tariq, F. (2014). Pakistan: Right-wing protests aim for military coup. *Green Left Weekly*, (1023), 13. Retrieved from <https://search.informit.com.au/documentSummary;dn=584488859033083;res=IELHSS>
- Tyers, A. (2013). Without a mobile phone, you basically don't exist. *The Telegraph*. Retrieved from <http://www.telegraph.co.uk/men/thinking-man/10399971/Without-a-mobile-phone-you-basically-dont-exist.html>
- Wagner, B. (2016). *Global free expression: Governing the boundaries of Internet content*. Cham, Switzerland: Springer International.
- 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. doi:10.1126/science.aaf5062
- Wirsing, R. (2008). *Baloch nationalism and the geopolitics of energy resources: The changing context of separatism in Pakistan*. Carlisle, PA: Strategic Studies Institute, U.S. Army War College.
- Wurtzel, A., & Turner, C. (1976, April 2). *Latent functions of the telephone: What missing the extension means*. Paper presented at the Fourth Annual Conference on Telecommunications Policy Research, Arlie, VA.
- York, J. C. (2010). Policing content in the quasi-public sphere. *Open Net Initiative Bulletin*. Retrieved from <https://opennet.net/sites/opennet.net/files/PolicingContent.pdf>
- Yusuf, H. (2013). *Mapping digital media: Pakistan*. New York, NY: Open Society Foundations.