The Effects of Internet Shutdowns on Societies: Lessons for SADC Member States

Admire Mare, PhD
Senior Lecturer: Namibia University of Science and Technology

Abstract
This paper critically discusses the effects of internet shutdowns on societies based on concrete examples from the African continent. Internet shutdowns have become normalized as evidenced by the rate at which these communicative raptures and disruptions have been used by both democratic and autocratic governments to stifle the free flow of information, freedom of assembly and freedom of expression. Whilst most studies on the impacts on internet shutdowns have been conducted by CIPESA, Brookings Institution and Deloitte from a quantitative research perspective, there is need to highlight that the effects of these disruptions are far much broader. They encompass political, social, technical and personal impacts. Besides the short-term effects, there are also long-term impacts which persist long after the restoration of internet and social media services. In countries, where most people rely on social media internet and mobile payment systems, the effects of network disruptions are very dire. These disruptions affects the overall investment image of a country, slows down economy growth, disrupts the value chain of the digital economy, lead to political demobilization and self-censorship. It affects job application, submission of assignments, transfer of remittances, and the smooth operations of technology-based transportation systems like Uber, Taxify and Vaya. Internet shutdowns also affect the attainment of the Sustainable Development Goals (SDGs).

Introduction and background to the study
The internet and its ancillary digital media technologies have become increasingly embedded in people’s everyday lives. As a result, it has become a key intermediary for economic, social and political transactions. The internet has also expanded economic
activities by providing a platform for buyers and sellers who are spatially removed from each other to be able to transact businesses (AFEX, 2017). Because of its ability to close up geographical gaps, the internet and digital media platforms have become useful tools for connecting people for reasons other than political action and economic transactions. It is therefore unsurprising that the United Nations Human Rights Council (UNHRC) passed a resolution on the promotion, protection and enjoyment of human rights on the internet. The resolution specifically expresses concern about measures aiming to or that intentionally prevents or disrupts access to or dissemination of information online. At the basic level, the internet is consists of a network of devices such as computers whose data can move over a wide range of channels including telephone wires, fibre-optic cables, satellites and wireless connections (KictaNet, 2017). It is used for a wide range of purposes including for obtaining information, sending important documents, applying for jobs, making mobile and online payments, organizing political protests and engaging in political participation and discussions (see Mare, 2016; 2018; Castells, 2010). The internet has made possible innovative contacting practices and interface between government and citizens. For most citizens, the internet and digital media platforms have facilitated easier engagement with the state, and also enabled citizens to speak truth to power (Mare, 2016).

In many ways, the early constructions of the internet and digital media technologies were couched within the realm of the concept of the “dictator’s dilemma”. This refers to the balance between authoritarian governments’ use of information communication technology for economic development with their need to control the democratizing influences of this technology. Based on this logic, ICTs were viewed as dramatically lower the costs of networked communication, favoring civil society over repressive governments (Diamond, 2010). It was believed that dictators would eventually succumb to these technological advances that undermine their political control. Conversely, it has been found that authoritarian regimes are finding increasingly sophisticated ways to counter the political impact of ICTs while simultaneously exploiting their commercial benefits. As intimated above, the internet has always been presented as “open, minimalist, and neutral” (Goldsmith and Wu, 2006: 23). It was open in that almost any computer or network could join it; it was minimalist because it required very little of the computers that wanted to join; and it was neutral between applications because it treated e-mail, downloads, and every other type of application the same (Goldsmith and Wu, 2006, 23). It was also depicted as the “electronic
“frontier” as a borderless “place” that could be protected and separated from territorial government (Goldsmith and Wu, 2006: 19; Drezner, 2010). In many cases, it was assumed that because of the decentralised design of the internet, it was inherently resistant to state control. In this vein, Diamond argues that it is not merely the structure of the Internet, but the scale of content generated that makes censorship difficult if not impossible (2010, 74).

However, as the various examples of internet shutdowns show, regulation has caught up with this technology. Goldsmith and Wu (2006) observe that, despite the early claims of internet idealists, geographic borders have become highly relevant to the development of the internet. This has not only been a result of authorizations by national governments, but rather an organic development from user demand, as “internet users around the globe demanded different internet experiences that corresponded to geography” (Goldsmith and Wu, 2006: 49). Internet intermediaries also rely on the legal authority of governments – backed by the threat of coercion or imprisonment – to maintain rule of law within internet communities. Overall, the internet’s architecture of links has proven to be far less decentralised than initially believed because, in part, internet access depends on physical connections which can be compromised to facilitate surveillance or censorship (Farrell, 2011: 15). For authoritarian regimes intent on maintaining power, the cost of controlling information may be less of an issue than the need for maintaining political power.

Despite its invaluable role in individuals and businesses’ day-to-day activities, some governments across the world have resorted to shutting down the internet in times of elections, protests and civil wars as a way of disrupting the normal flow of information. These practices have institutionalised what MacKinnon (2011) calls ‘networked authoritarianism’ especially in China, Iran and Russia. In this age of interconnected devices, throttling and shutting down the internet has the same effect as pulling the plug on a machine (Gohdes, 2015). It also has the net effect of limiting the opportunities for people and businesses, and hampering the general health status of the economy.

\[1\] There is no guarantee of individual rights and freedoms. People go to jail when the powers-that-be decide they are too much of a threat – and there’s nothing anybody can do about it. Truly competitive, free and fair elections do not happen. The courts and the legal system are tools of the ruling party.
Shutdowns can inhibit social interactions especially in societies where families have been dislocated by international and regional migration. Disruptions have widespread impacts on people and the economy with even partial disturbances affecting productivity, souring business confidence, and leading to lost opportunities (Wagner, 2018). Most of the shutdowns recorded thus far have arisen from political compulsions (CIPESA, 2017; Deloitte, 2016). For instance, during the Arab Spring—wave of protests that engulfed the Middle East and North Africa between 2011 and 2012, the internet was shut down as a means of demobilizing cyber-movements and disrupting the coordination of protests via digital media platforms.

Most research (Deloitte, 2016; CIPESA, 2017; AFEX, 2017) thus far has focused on the impact of internet shutdowns on the economy. Studies (see CIPESA, 2017; KictaNet, 2017; Wagner, 2018; AFEX, 2017) also suggest that limiting the functions of the internet can materially affect productivity in both short and longer-term horizons. Several African countries have experienced different forms of internet shutdowns since 2011. These include: Cameroon, Gabon, Democratic Republic of Congo, Chad, Gabon, South Sudan, Ethiopia, Egypt, Tunisia and Zimbabwe. Several governments (Somalia, Ethiopia, Uganda, DR Congo, Cameroon, Zimbabwe, Liberia, Togo and Nigeria) resorted to Internet shutdowns or content censorship as a means to disrupt anti-government protests and check the spread anti-government content. The most publicized case in the last two years has been that of Cameroon where the government of Paul Biya shut down internet access to the North-west and South-west regions in an attempt to stifle protests against political and economic discrimination. Authoritarian governments across the African continent appear threatened by the robust access to information that is enabled by the internet, and are resorting to controlling the flow of such information for several reasons, among them public order, protection of state leaders and institutions, and protection of state processes and national security (KictaNet, 2017).

Notwithstanding these important quantitative studies foregrounding the economic, costs of internet shutdowns, there are is a disconcerting dearth of qualitative research on political, social, technical and personal costs of these disruptions. As discussed above, governments have been turning to network shutdowns with increasing frequency to quell unrest and suppress the spread of rumors and fake news. But there is no
empirical evidence that proves this tactic is effective, and activists and journalists alike have raised concerns over the catastrophic side effects these shutdowns often have on communities. Below I look at the concept of internet shutdowns before proceeding to discuss briefly about the literature review.

**Conceptualizing Internet Shutdowns**

It is important to problematize the concept of internet shutdowns given its contextualized usage. Shutdowns are also sometimes described as “blackouts” or slowdowns or “kill switches” (Gerbaudo, 2013). Internet shutdowns refers to 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, are a type of online censorship (Access Now, 2017). It happens when a certain actor (government, internet service provider or even third party) intentionally disrupts the internet or social media platforms in order to control what people say or do. However, this definition does not encompass the pricing out of the unconnected from the internet market. The argument of this paper is that there are already people who are shut out of the internet system because of lack of infrastructure, cost and other structural impediments.

Internet shutdowns can be partial or total depending on the context. Partial shutdowns happen when there is a targeted blocking of internet and specific websites or even social media services in a region or a country (KictaNet, 2017). A complete or total shutdown is when all Internet services are blocked without specific targeting of applications or websites. Noteworthy to underscore that internet shutdowns can involve the following elements: a deliberate and complete disruption; throttling of speeds or blocking of specific websites or applications; blockage of fixed line or mobile Internet or both; imposition of intermediary liability and issuance of an order by an authority of the state to telecommunication operators (Wagner, 2018). Shutdowns can be implemented at various layers of the Internet architecture. The most methods employed include: Internet Protocol (IP) address blocking; Deep Packet Inspection (DPI) (where equipment reads data passing through a network and hijacks it through equipment known as a “middlebox”); Border Gateway Patrol (BGP) attacks (where the addresses of certain websites or routes to entire networks are taken over illegitimately) and
Hypertext Transfer Protocol (HTTP) throttling (which is the intentional slowing of bandwidth by a service provider) (see KictaNet, 2017; Wagner, 2018).

A Brief Overview of the Emerging Literature on Internet Shutdowns

Internet shutdowns constitute an emerging means of online censorship, although it can be viewed also as a distinct phenomenon. Scholars (Deibert and Rohozinski, 2010, p. 4) have identified four “generations” of internet censorship or control. First, it was about filtering systems at the backbone of the country’s internet. Second, it creating a legal and normative environment and technical capabilities that enable state actors to deny access to information resources as and when needed. Third, it emphasized less on denying access than successfully competing with potential threats through effective counter-information campaigns that overwhelm, discredit, or demoralize opponents. Fourth, it is more about access contested (see Deibert and Rohozinski, 2010). As Wagner (2018) argues, by limiting access to specific content or specific websites or discrediting citizen journalism, internet censorship aims to reconfigure and shape the public sphere.

It is noteworthy to highlight whilst the literature on the impact of the internet on society and politics have been presented as a binary involving cyber-optimists and cyber pessimists, there is need to underscore the point that the actually existing of state of research in the field points to the existence of spectrum rather than the aforementioned taken for granted dichotomy. Although most scholars (see Castells, 2010; Shirky, 2011; Lim, 2018) tend to gravitate towards the pessimistic and optimistic ends of the debate, there is equally a growing amount of literature that demonstrate the grey areas of this debate on the impact of the proliferation of the internet. In the middle of the spectrum, are cyber-realists (Morozov, 2011; Aouragh, 2013) who adopt a more cautious approach that transcends both the cyber-optimist and cyber-pessimist approaches.

Cyber-optimists view the internet and digital media technologies in the positive light while cyber-pessimists focus on its negative impact on society. Cyber-optimists focus on its positive transformative impact on facets like political, social and economic activities (Castells, 2010). Platforms like Facebook, WhatsApp and Twitter are being appropriated for business, social and political transactions. In repressive regimes,
digital media platforms have become the mainstream alternative media. Dominant
debates have overly emphasized the positive impact of social media as means for
protest mobilization (see for example Shirky, 2011; Lim, 2018). Social media networks
have also enabled civil society to coordinate and gather voices of dissent like never
before, crucial to the functioning of a democracy. It has given rise to new forms of
political parties and social movements. Whilst cyber-optimists focus on the
transformative potential of the internet to dismantle authoritarian practices and cultures,
cyber-pessimists focus on how these technologies can be used for autocratic durability.

Cyber-pessimists focus on the negatives like the proliferation of hate speech,
recruitment of terrorists, illicit financial flows, online harassment, spread of fake news
and cyber-propaganda and other forms of dark participation (see Mare, 2016). Bots and
cyber-troops are now being deployed for sole purpose of democratic subversion and
authoritarian survival. This has had deleterious effects on electoral processes and access
to quality information. Social media has also received bad press for its negative role in
the outcomes of elections in the United States of America and the Brexit vote in the
United Kingdom (see Howard, 2017). The internet is not only a force for openness and
transparency, but also a surveillance machine. Twitter and Facebook are also being
used by security and intelligence agencies to identify and locate activists and protesters
(Camninos, 2013). It is within the context of this unending debate about the negative
and positive attributes of the internet that shutdowns and slowdowns have become
normalized and institutionalized especially in authoritarian regimes.

Morozov (2011: 319) puts emphasis on studying the environment in which digital
media operate and rejects the view that the internet has a single preordained outcome.
He critiques cyber-optimism for promoting the gospel of “technological solutionism”
where technical fixes are seen as an answer to democratic challenges (Morozov, 2014).
Aouragh (2012; 2013) views the internet as a double-edged technology with both
empowering and disempowering potentialities. Likening digital media to Damocles’
sword, Aouragh (2013) argues that those who are empowered by taking the seat under
the sword do so haunted by the constant threat of being killed by the same sword,
because slaughter could come at the slightest disruption. This observation dovetails
with Curran’s (2002) view that media [including digital media] are spaces, where media
power and counter-power are played out.
Ever-since the globalization of protests spawned by the Arab Spring and the Spanish Indignados, internet shutdowns have become the weapons of last resort for authoritarian governments. Reflecting on the Arab Spring, Gerbaudo (2013) conceptualized the ‘kill switch’ in Egypt under Hosni Mubarak in 2011 as a ‘suicide switch’. As Gerbaudo (2013) argues, the ‘kill switch’ turned into a ‘suicide switch’, which ended up giving more energy to the protests that took place on 28 January and on the following days than would have happened otherwise. Instead of deterring people from flooding the streets, the kill switch approach mobilized a huge mass of people to demonstrate in Cairo and other cities (Gerbaudo, 2013). A number of African governments are deploying censorship, criminalization of speech, surveillance and control or closure of media houses as strategies and tactics to throttle the free flow of information (AFEX, 2017).

Beyond the continent of Africa, internet shutdowns have been used to demobilize protestors and citizens in Asia, Europe and South America. Countries like Syria, Nepal, Iraq, Kazakhstan, Pakistan, Uzbekistan, Yemen, China, India, North Korea, Bahrain, Bangladesh, Turkey and Myanmar have been at the forefront of using internet shutdowns as a tactic of paralyzing and demobilizing protestors. Internet shutdowns have generally used especially during important events like elections or protests or during terror attacks or national emergencies to silence dissent and curtail freedom of assembly rights. These shutdowns abrogate human rights such as freedom of expression and assembly, access to information and political rights. Various justifications for shutdowns have been thrown around such as the need to protect state institutions and leaders, managing electoral crises, controlling the spread of propaganda, and mitigating dissent and national security (KictaNet, 2017).
What are the effects of Internet Shutdowns? Political, Social, Economic, Technical and Personal

Research and anecdotal evidence have shown that internet shutdowns have deleterious economic, political, social, personal and technical impacts. Besides affecting directly and indirectly people’s everyday lives, internet shutdowns affect broadly the democratization project. They undermine the rule of law, constrain freedom of expression and disrupt the normal functioning of the economy. There is therefore urgent need for policymakers need to consider the costs alongside security imperatives. Generally, internet shutdowns are disproportionate and discriminate hence fails to meet the necessary and proportionate requirements.

Economic impacts

Internet shutdowns have a huge economic impact because businesses suffer immensely when they cannot communicate. According to the Brookings Institute, internet shutdowns all over the world cost $2.4 billion in 2015-2016. During 2012-2017, 16,315 hours of Internet shutdown cost India’s economy around $3 billion, the 12,600 hours of mobile Internet shutdown about $2.37 billion, and the 3,700 hours of mobile and
fixed-line Internet shutdowns nearly $678.4 million. Internet shutdowns affect economies in numerous ways, disturbing productivity and generating monetary losses in time-sensitive transactions. Businesses that are heavily dependent on electronic transactions are particularly exposed to very serious consequences such as bankruptcy. For example, e-payments are becoming increasingly common not only in the developed world but in many developing countries. There is a real impact of shutdowns on countries’ Gross Domestic Products (GDP) (CIPESA, 2019). Beyond macro-economic impacts, shutdowns also result in loss of earnings in the digital economy and government revenues. It also affects informal economies, worker productivity, supply chains, manufacturers and service providers, investor confidence and foreign direct investment. Even short-lived Internet disruptions affect many facets of the national economy and tend to persist far beyond the days on which access is disrupted. Businesses cannot engage in e-commerce or provide digital products and services. Companies lose access to online information, thereby undermining productivity and potentially costing jobs. The spread of mobile internet has also offered many Africans an opportunity to achieve key development aims, and access education, health services, insurance, and employment opportunities.

### Internet shutdowns continue to cost Africa's economy

<table>
<thead>
<tr>
<th>Country</th>
<th>Cost of disruption/day</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethiopia</td>
<td>$3.5 million</td>
</tr>
<tr>
<td>DR Congo</td>
<td>2</td>
</tr>
<tr>
<td>Uganda</td>
<td>1.76</td>
</tr>
<tr>
<td>Cameroon (Anglophone)</td>
<td>1.67</td>
</tr>
<tr>
<td>Gabon</td>
<td>0.88</td>
</tr>
<tr>
<td>Republic of Congo</td>
<td>0.43</td>
</tr>
<tr>
<td>Niger</td>
<td>0.41</td>
</tr>
<tr>
<td>Burundi</td>
<td>0.16</td>
</tr>
<tr>
<td>The Gambia</td>
<td>0.05</td>
</tr>
</tbody>
</table>
Political Impacts

At a political level, internet shutdowns have the potential to demobilize protestors but also to politicize the bystanders when they feel that they have nowhere to turn to but going to the streets to air their grievances. In such a case, the ‘kill switch’ operations can actually politicize those are considered apolitical and apathetic towards formal politics. Shutdowns also constitute human rights violations because they interfere with the exercising of basic rights like freedom of expression and peaceful assembly. They further contribute to the institutionalisation of the chilling effect which manifests through self-censorship. In the clock of darkness, human rights abuses are often conducted because of limited flow of news and information. Other political effects of shutdowns include the breakdown of rule of law and use of the law as a weapon of repression. It has also been argued that disruptions contribute to technology-enhanced authoritarianism in the digital space.

Technical impact

There are collateral damages associated with network disruptions. These include the form of over-blocking of websites and content that was not intended to be restricted, for example when unrelated websites hosted on the same server as the targeted website are affected by the shutdown. Other collateral damages include exposing users to privacy and security risks, for example when people turn to untrustworthy VPNs in order to route around restrictions. Vaguely worded judicial orders sometimes force ISPs and other network-level operators to assess which content is acceptable or not and, to proceed to remove it. Irrespective of their duty before the law to respond to court orders, such actors are generally not equipped to take on the role of judge and jury, nor should they. Total internet shutdowns have the potential to generate long term systemic risks.

Social Impacts

There are also a number of social impacts. Not only does shutting down the internet affect the smooth running of peoples’ lives, it also impacts on the ability of individuals to complete online job applications, applying for basic identity documents, submitting
school and college assignments and transfer of remittances. In societies where most people rely on social media internet for basic communication, it can affect the smooth running of the family and school runs. It disrupts the transportation system especially ride sharing applications which rely on the internet for geolocation data and online payment systems. In countries, like Zimbabwe, Ethiopia, and Somalia, where locals are very dependent on the transfer of remittances, internet shutdowns can affect the sending and receiving of essential cash supplies. In areas, where the internet has become embedded into the health and education sectors, its absence can disrupt the whole value chain.

Conclusion

This paper has looked at the various impacts of internet shutdowns from an economic, political, social and technical point of view. It has defined the problematic concept of internet shutdowns. Rather than focusing on the intentional disruption of the internet and social media services, the paper has broadened the definition to look at how affordability and accessibility conspire in ways that shut down the internet from the unconnected thereby leaving them behind the information superhighway. The paper has demonstrated that internet shutdowns have short and long term impacts. Besides affecting economic growth, hampering revenue generation and collection, these disruptions negatively affect the overall image of the country. Internet shutdowns tend to attract international attention and create pressure on countries that undertake them. This relates to the so-called “Streisand effect”, where the attempt to silencing voices or hiding information leads to the unintended consequence of bringing more attention to them. It recommends that internet shutdowns must meet the necessary and proportionate test in order for them to be considered justifiable. There must be legitimate aim and valid reasons for carrying out the exercise in the public interest.

References


Goldsmith, J. and Wu, T. @006). Who Controls the Internet? Illusions of a Borderless


