State-Ordered Internet Shutdowns and Digital Authoritarianism in Zimbabwe

ADMIRE MARE

University of Johannesburg, South Africa

This study critically reflects on why and how private telecommunications operators in a militarized authoritarian state comply with government orders to shut down the Internet. It argues that state-ordered Internet shutdowns must be conceptualized as a form of digital authoritarianism. It demonstrates that between 2016 and 2019, the government in Zimbabwe added state-ordered Internet shutdowns to its ever-expanding authoritarian toolkit, thereby negatively impacting the financial sustainability of telecommunications operators. Deploying the critical political economy approach and the metaphor of lawfare, the study demonstrates that the responses of private telecommunications operators to government orders must be understood within the broader context of sociopolitical and economic factors. Although private companies such as Econet Wireless Zimbabwe and Liquid Telecom control a huge chunk of the telecommunications infrastructure, the government often deploys political, regulatory, and lawfare strategies to force through state-ordered Internet shutdowns. The study argues that private telecommunications operators comply with government partly to abide by their licensing obligations, for fear of political harassment and victimization and threats of arbitrary imprisonment.

Keywords: Internet shutdowns, Zimbabwe, political economy, digital authoritarianism, state control, lawfare, and telecommunications.

Over the past decade, Internet shutdowns have become normalized across the globe (see Ayalew, 2019; Freyburg & Garbe, 2018; Hintz & Milan, 2018; Mare, 2019; Glasius & Michaelsen, 2018; Wagner, 2018). Most Internet shutdowns occurred during events such as elections, protests, terror attacks, and public examinations (Access Now, 2017; Ayalew, 2019; CIPESA, 2019). This is despite the

1 I would like to thank Tina Freyburg, Eleanor Marchant, and Nicole Stremlau for the invaluable insights.

2 Internet shutdown refers to the intentional disruption of Internet-based communications, rendering them inaccessible or effectively unusable (Access Now, 2019). There are different types of shutdowns. This study focuses on state-ordered shutdowns: situations in which the government (through ministers or regulatory authorities) orders telcos or ISPs to shut down the Internet and social media services. In most cases, the directives are backed by a warrant or official written or verbal order.

Copyright © 2020 (Admire Mare). Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at http://ijoc.org.
initial celebration of the Internet as a decentralized, democratic, and fluid network structure (Curran, 2012). In view of its assumed empowering potential, Diamond (2010) coined the term *liberation technology* to describe the Internet and its ancillary digital media technologies. As a “citizen-designed, citizen-controlled worldwide communications network” able to “revitalize the public sphere” (Rheingold, 1993, pp. 14–15), scholars expected the Internet to present a silver bullet with the potential to undermine authoritarianism (Howard, Agarwal, & Hussain, 2011). From this optimistic perspective, the Internet can undermine authoritarian tendencies by offering new communication channels that are “fundamentally resistant to state regulation, reducing a state’s capacity for repression by hindering its ability to control the flow of information and political communication” (Garrett, 2006, p. 220).

Yet, scholars such as Freyburg and Garbe (2018) remind us that the Internet relies on a hierarchical physical infrastructure, which provides governments, regulatory authorities, and telecommunications companies (telcos) with control opportunities. These control opportunities manifest themselves at the level of telecommunication infrastructure, including the licensing of operators, ownership of single or multiple international gateway systems, and installation of surveillance infrastructure on telecommunications boosters and networks. Consequently, because of these vulnerabilities, governments—normally through Internet service providers (ISPs)—are capable of switching off the Internet arbitrarily and often on the basis of a wide range of reasons; these include combatting fake news, dealing with hate speech and related violence, securing public safety and national security, and preventing cheating during exams (Access Now, 2017; Ayalew, 2019; CIPESA, 2019; Mare, 2019). Since the former Guinean president Lansana Conte ordered the country’s four main ISPs to shut down the Internet in 2007 following widespread protest action calling for his resignation, the practice has been exported to other countries across the globe (Akunola, 2018). As a demobilizing tool, Internet shutdowns graced international headlines during the Arab Spring (Morozov, 2014; Rød & Weidmann, 2015). Thus, Internet shutdowns are increasingly becoming the “new normal” in a number of countries.

This article aims to demonstrate why and how private telecommunications operators comply with government orders to shut down the Internet and, in particular, social media services in an authoritarian context. This is particularly important in a context in which customers access the Internet on a prepaid basis, making Internet shutdowns extremely costly for telecommunications companies. Drawing on the critical political economy (CPE) approach (Golding & Murdock, 2000; Murdock & Golding, 1973) and the metaphor of “lawfare” (Dunlap, 2017), this article argues that the systemic unequal balance of power between the government and telcos can explain the incidences of state-ordered Internet shutdowns in Zimbabwe between 2016 and 2019. Ownership of backbone infrastructure plays an important economic

---

3 This term refers to any facility that is used to access international cable systems (often submarine) or satellite systems and that manages incoming and outgoing international voice and data traffic by connecting national networks to regional and global systems.

4 The Arab Spring was a wave of protests that engulfed the Middle East and North Africa between 2011 and 2012, leaving a trail of destruction, toppling of undemocratic regimes, and normalization of military violence.

5 This term refers to the ways by which a state uses or misuses the law as an alternative to traditional military mechanisms of war.
role in tilting the balance of power between these state and private businesses. On the one hand, political power denotes the extralegal measures—such as harassment, intimidation, victimization, and threats of arbitrary imprisonment—that can be used by authoritarian governments as part of their repressive state apparatuses to arm-twist telcos to implement their directives. On the other hand, regulatory power manifests itself through the ability of governments to license and regulate the sector through regulatory authorities. While private telcos have economic power by virtue of their financial muscle and ownership of infrastructure, notably fiber cables, authoritarian governments can resort to lawfare to get things done. As Dunlap (2017) argues, authoritarian governments and associated parties weaponize the law and legal institutions, with the intent to weaken or annihilate any resistance from the opposition parties and other nonstate actors. The aim is to subdue the targeted nonstate actor’s resistance without resorting to other lethal and traditional political strategies. Complementing existing literature (e.g., Freyburg & Garbe, 2018), this article demonstrates that although ownership and control of ISPs determine to a large degree whether an Internet shutdown will be successfully implemented, the political economy of the international gateway systems in any given context contributes significantly to the overall objective.

The CPE approach allows examining the structure and properties of the telecommunications industry, with a focus on issues such as ownership, market structure, and commercial support, and how these affect service provision, performance, and impact (McChesney, 2003). Thus, to investigate why and how private telcos comply with government directives to shut down the Internet and social media services, it is imperative to take into account the structural constraints, such as financing, shareholding structure, government policies, and the broader sociopolitical dynamics. One of the major tenets of the CPE approach to the telecommunications sector revolves around the ownership and control of ISPs and the extent to which these telcos operators can keep the Internet on as a public good. As Freyburg and Garbe (2018) show, the government can abuse its direct and indirect influence to coerce the operators into complying with its directives if it is the majority owner of telcos. Because of its concern with ownership and control, the CPE will assist us in analyzing how power and control exercised through direct state ownership of the international gateway systems allow the government of Zimbabwe to undertake state-ordered Internet shutdowns.

Building on the CPE approach, it is the overall proposition of this study that the government of Zimbabwe can make private telcos (e.g., Econet Wireless Zimbabwe, ZOL, and Liquid Telecom) comply with its orders for predominantly two reasons: (1) It has access to traditional state tools of control, notably the threat to withdraw licenses and the ability to pass legally binding laws and policies, as well as its monopoly of weapons of violence, and (2) It is able to press on with Internet shutdowns because of its ownership and control of four critical international gateway systems. This study therefore proposes that private telcos in Zimbabwe are likely to safeguard their long-term commercial interests at the expense of the broader public interest mandate (such as keeping the Internet on). Thus, compliance of private telcos in an authoritarian context must be conceptualized from “the point of view of their inherent nature to pursue and maximize profits sometimes at the expense of promoting public good” (Murdock & Golding, 1973, p. 205).

Using Zimbabwe for empirical illustration, the study provides a rich, contextualized understanding of the intercalary position inhabited by private telecommunications operators in an authoritarian regime.
The country is particularly suited as a case study because of the complex ownership dynamics in the telecommunications sector, where, despite liberalization and privatization of state-owned enterprises (SoEs) in the early 2000s, “elite renewal and continuities” have remained intact (Sparks, 2011). The liberalization drive has been accompanied by a cohort of telecommunications owners, who are mostly aligned to the dominant political party. Even more interesting has been the militarization of politics and the economy, which has culminated in what has been described by some scholars as the “military commercialism” (Moyo, 2016), or the “military-industrial complex”—the informal entanglements of the security services in various facets of the Zimbabwean society. As this article will show later, the expanded involvement of the military in the political economy of Zimbabwe has manifested itself through the ownership of Africom, one of the main ISPs, by the Ministry of Defence. Furthermore, the government has a significant ownership stake in a number of key telecommunications operators.

Between 2016 and 2019, Zimbabwe experienced two major state-ordered Internet shutdowns, which were accompanied by gross human rights violations and a spike in the circulation of misinformation and disinformation (Mpofu & Mare, 2020). The first shutdown focused on the partial closure of a specific social media platform, WhatsApp, for at least four hours in July 2016, while the shutdown in January 2019 was characterized by the total closure of all Internet services for at least 7 days. They occurred at a time when the ruling party, the Zimbabwe African National Union-Patriotic Front (ZANU-PF), was going through some of the most brutal internal fights in its history (Mare, 2019). Both shutdowns also coincided with the resurgence of social and digital activism in response to the worsening socioeconomic crisis and closure of the democratic space (Mpofu & Mare, 2020). The government used a law-and-order approach to fend off the pressure from citizens.

Both shutdowns being investigated were executed based on government directives. This raises a number of scholarly questions, which form the bedrock of the present study: Why did private telcos comply with the government orders? What role did ownership and control of key infrastructure play in the arm-twisting of private telcos? Why did the private telcos fail to push back against the government orders? How did the government use legal and extralegal measures to force telcos to implement its orders?

In this article, I first discuss the nexus between digital authoritarianism and ISP ownership. I then proceed to justify the methods and case selection for this particular study. Thereafter, I look at the political-economic context of the telecommunications sector in Zimbabwe. I move on to present the findings and offer a brief discussion and implications of the study. Last but not least, I present my preliminary conclusions.

**The Nexus Between Digital Authoritarianism and ISP Ownership**

Extant literature on how and why Internet shutdowns are carried out has shifted toward studying ownership and management structures of ISPs, taking into account varying types of political

---

6 This term refers to change that is narrow and self-serving in its manifestation. Such a system ensures that the old order mutates into something in the so-called new order.
regimes, domestic legal architecture, existence of oversight mechanisms, and the management of international gateway systems (Ayalew, 2019; CIPESA, 2019; Freyburg & Garbe, 2018; Gerbaudo, 2013). Most Internet shutdowns have been shown to involve an official order by the government targeted at telcos. Reports indicate that telcos are caught between their legal obligations to regulators on the one hand, and a moral duty to protect customers’ freedom to communicate on the other (Adegoke, 2017; Wilson, 2019). Extant literature (Adegoke, 2017; Southern Africa Litigation Center, 2019) puts the spotlight on the role of telcos in the implementation of government orders. Their findings are that some telcos, such as the MTN Group and Orange, have resorted to complying with government orders so as to avoid heavy penalties on the part of their employees (Adegoke, 2017; Wilson, 2019). However, reports suggest that it may be difficult for telecoms to put up a fight in countries with authoritarian regimes (Access Now, 2017; Wilson, 2019). One of the reasons it is difficult for telcos to push back against government orders is that certain licensing obligations allow regulators to invoke nebulous justifications, such as the need to protect national security.

Using a nonprobabilistic method known as qualitative comparative analysis, Freyburg and Garbe (2018) demonstrate that the involvement of state governments in the ownership structure of Internet-providing companies is positively associated with blockages of access to the Internet or other specific services such as social media. Ownership is considered one of the crucial governance mechanisms. Consonant with the CPE approach, the concept of ownership structure helps explain the occurrence of intentional network disruptions. Eventually, authoritarian governments do not implement shutdowns themselves; rather, they order ISPs and telcos to cut services. Although direct state ownership of telecommunication operators provides a direct way to control infrastructure and traffic, Freyburg and Garbe (2018) show that we can also observe shutdowns “if the state is not the majority shareholder but elections are marked by violence” (p. 3907).

Research has foregrounded the need to critically analyze the terms and conditions of telecommunications licenses, which compel them to become willing “chokepoints” for authoritarian governments (Southern Africa Litigation Center, 2019). Recent studies have shifted focus toward investigating the ways in which telcos can push back against government orders in authoritarian settings. A report published by Access Now (2017) indicated that Kenyan telcos have been making use of strategic litigation, implementing rights-respecting standards, influencing public policy, deploying technical resources, increasing transparency by publishing proactive reports, and working with progressive allies.

While advocacy-oriented literature has dominated earlier discussions on the nexus between digital authoritarianism and Internet shutdowns, it is noteworthy to highlight that academic studies (Ayalew, 2019; Freyburg & Garbe, 2018; Gohdes, 2015; Hintz & Milan, 2018; Marchant & Stremlau, 2019; Rod & Weidmann, 2015; Wagner, 2018) have grown by leaps and bounds over the last few years. Digital authoritarianism is an extension of what MacKinnon (2011) calls “networked authoritarianism.” It consists of practices such as filtering and controlling Internet content that citizens can access, and blocking and

---

7 This term refers to how authoritarian governments can adapt or leverage ICTs to bolster their legitimacy and durability. Networked authoritarianism can take the form of governments tracking, surveilling, and controlling their populations.
shutting down Internet services completely (Hintz & Milan, 2018). Building on the concept of “communicative raptures” (p. 3918), Wagner (2018) argues that state-directed Internet shutdowns can be conceptualized as “intentional disconnections of digital communications by government authorities,” which often include “shutting down the Internet and mobile phone services” (p. 3918). Glasius and Michaelsen (2018) observe that the openness to global digital media technologies presents new opportunities for authoritarian rulers to control and manipulate citizens. These authoritarian practices sabotage accountability and thereby threaten democratic processes (Glasius & Michaelsen, 2018). By limiting access to specific content or specific websites or discrediting citizen journalism, Internet censorship aims to reconfigure and shape the public sphere (Wagner, 2018).

In his study of Internet shutdowns in Ethiopia, Ayalew (2019) notes that blanket shutdowns do not meet the requirements of human rights law (such as legality, legitimacy, necessity, and proportionality). Instead of using law, the government of Ethiopia successfully mobilized narratives such as “economic development” to convince the public of the desirability of Internet shutdowns (Ayalew, 2019). These measures have been deployed as a way of disrupting the normal flow of information. In Cameroon, the government of Paul Biya effectively ordered shutting down Internet access to the North-West and South-West regions in an attempt to stifle protests against political and economic discrimination (Access Now, 2017).

Methods and Case Selection

The two Internet shutdowns—July 2016 and January 2019—in Zimbabwe were chosen as “idiographic case studies” (Gerring & Cojocaru, 2016). An idiographic case is selected “because of the intrinsic or theoretic importance of a case, and usually because they are not (in the author’s view) well understood” (Gerring & Cojocaru, 2016, p. 410). Both Internet shutdowns happened when Zimbabwe was experiencing massive social protests over the worsening economic crisis, shortages of fuel and cash, and a deteriorating human rights record (Mpofu & Mare, 2020). The July 2016 Internet shutdown was peculiar in that it was characterized by the partial blocking of a specific social media platform, WhatsApp. During that incident, private telcos such as Econet, ZOL, and Liquid Telecom were evasive about the reasons for the social media blackout. Even the press statement issued by the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) did not explain the mechanics behind the partial shutdown. The January 2019 Internet shutdown was a complete blocking of Internet and social media services (Mare, 2019). For at least 7 days, the country had no access to the Internet except those relying on satellite connections, such as embassies and nongovernmental organizations. For the first time, the chairman of Econet Global Limited, Strive Masiyiwa, revealed that his company had been forced to shut down the Internet by government authorities.

The political economy of the telecommunications sector in Zimbabwe also makes it an interesting case study because of the monopolistic tendencies of the government. The government of Zimbabwe is a major shareholder in telcos such as Net*One, Tel*One, Africom, and Telecel (see Tables 1, 2, and 3). As far as the market share is concerned, Econet Global Limited has a virtual monopoly in terms of the provision of fixed and mobile Internet through its ownership of Econet Wireless Zimbabwe, Liquid
Telecom, and ZOL Zimbabwe (see Tables 1, 2, and 3). Thus, the government and Econet Global Limited dominate the telco industry in Zimbabwe.

To answer the question of why and how private telecommunications operators in Zimbabwe complied with government orders to shut down Internet services between 2016 and 2019, the article relies extensively on secondary data. Thematic content analysis of ministerial orders, press statements from telcos and regulatory authorities, and reports from media advocacy organizations was also conducted. From a CPE perspective, it is important to understand the complex interactions between the telcos and the broader sociopolitical and economic context of Zimbabwe. Hence, the section that follows discusses the ever-shifting ownership structures and political economic foundation of the telecommunications industry in Zimbabwe.

The Political-Economic Context of the Telecommunications Sector in Zimbabwe

Zimbabwe has experienced unprecedented sociopolitical and economic transformations since the early 2000s, which have laid the foundation for a “militarized” authoritarian regime (Mare, 2018; Masunungure, 2014). The weaponization of the law has been the defining feature of the ZANU-PF regime for the past two decades (Magaisa, 2020). Although Zimbabwe has held periodic elections since the country attained political independence in 1980, the twin processes of militarization of public life and politicization of the military have stood in the way of democratization and good corporate governance (Mare, 2018; Masunungure, 2014). These mutually reinforcing processes also corroded the ownership and corporate governance structures of state-owned telcos. The telecommunications industry does not operate in total isolation from the political environment (Makuvise, 2014). Since the liberalization of the telecommunications industry (punctuated by privatization of state-owned companies, the introduction of competition, the opening of markets to foreign investors, and establishment of procompetitive regulations), which commenced with the passage of the Postal and Telecommunications Act of 2000, the government of Zimbabwe wasted no time in acquiring significant shares in the fixed (Tel*One) and mobile Internet companies (Net*One). This speaks of “elite continuity and renewal” (Sparks, 2011) in the telecommunications sector.

While the 2000 act effectively ended the monopoly of the Post and Telecommunications Corporation, it led to the splitting of the company into three commercial units: the fixed telephone provider Tel*One, the mobile cellular company (Net*One), and the public postal operator ZimPost (Makuvise, 2014). The act also provided for the creation of the POTRAZ, which was mandated to ensure a level playing field in the post and telecommunications sector. The regulator granted licenses to private companies—Econet Wireless Private Limited and Telecel—to operate mobile networks. The liberalization of the telco sector was also accompanied by the emergence of a new cohort of telecommunications owners and companies, mostly aligned to the dominant political elite. Most of the owners are loyal to the incumbent government.

8 The initial intention was to complement secondary data with primary data, but efforts to interview key informants from the telcos failed to yield tangible results.
There are three mobile voice operators in Zimbabwe: one privately owned (Econet Wireless Private Limited) and two state-owned (Net*One and Telecel) enterprises (see Table 1). Econet is owned by Econet Global Limited (with 42.62%), Stanbic Nominees (Private) Limited (NNR; with 16.83%), Stanbic Nominees (Private) Limited (with 9%), and other shareholders (with 31.55%). The government holds 100% shareholding in Net*One (Makuvise, 2014). With regard to Telecel, the government holds 60% shareholding, and the remaining 40% stake is owned by a consortium of local and foreign investors. The acquisition of the 60% stake in Telecel was a well-calculated move by the government to consolidate its control over the telecommunications sector, especially when Econet had a domineering market influence. SoEs, Net*One, and Telecel fall under the Ministry of Information Technology and Courier Services. The board of directors of SoEs is appointed by the line ministry.

<table>
<thead>
<tr>
<th>Company Name</th>
<th>Shareholders and Their Percentages</th>
<th>Market Share %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Econet Wireless Zimbabwe</td>
<td>Econet Global Limited, 42.62%</td>
<td>69.7</td>
</tr>
<tr>
<td></td>
<td>Stanbic Nominees (Private) Limited (NNR), 16.83%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Stanbic Nominees (Private) Limited, 9%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Other shareholders, 31.55%</td>
<td></td>
</tr>
<tr>
<td>Telecel Zimbabwe</td>
<td>Government, 60%</td>
<td>8.9</td>
</tr>
<tr>
<td></td>
<td>Consortium of local and international investors, 40%</td>
<td></td>
</tr>
<tr>
<td>Net*One</td>
<td>Government, 100%</td>
<td>21.4</td>
</tr>
</tbody>
</table>

Source: POTRAZ, 2019

Most Zimbabweans connect to the Internet via mobile phone (Mare, 2018). In terms of mobile market share, Econet enjoys 69.7%, Net*One has 21.4%, and Telecel has 8.9% (POTRAZ, 2019). There are two fixed voice operators in Zimbabwe: Tel*One and TeleAccess. The former is 100% owned by the government, and the latter is a privately owned company. In recent years, Internet access providers (IAPs) were allowed to do both voice and data through the Voice over Internet Protocol, thereby encroaching on the services previously provided by the voice operators. As a result, Africom, Tel*One, Powertel, and Liquid Telecom (a subsidiary of Econet Global Limited) have emerged as big threats to the three mobile service providers (Makuvise, 2014).

There are 18 IAPs with varying degrees of market share (POTRAZ, 2019). Liquid Telecom (owned by Econet Global Limited) has 54.2%, followed by Tel*One with 23.1%, Powertel (owned by government) with 12.8%, Dandemutande (a private firm) with 5.8%, Africom with 2.8%, Telco (a private operator) with 1.1%, and, finally, Aquiva (a private firm) with 0.2% (POTRAZ, 2019). Africom, one of the IAPs, is owned by the Ministry of Defence, Security and War Veterans through its investment arm, Fernhaven Investments (Ndebele, 2016). The National Social Security Authority and a number of “ghost” shareholders—such as Beitast Investments limited, Ramallo Investments (Pvt)
Limited, and Full Wing Investments (Pvt) Limited), which are not registered with the Registrar of Companies of Zimbabwe—also have shares in the company (“Africom’s ‘Ghost’ Shareholders,” 2011).

<table>
<thead>
<tr>
<th>Name</th>
<th>Shareholders</th>
<th>Market Share %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Africom Zimbabwe</td>
<td>Ministry of Defence</td>
<td>2.3</td>
</tr>
<tr>
<td>Afrihost</td>
<td>Private investors</td>
<td>N/A</td>
</tr>
<tr>
<td>A Pics</td>
<td>Private investors</td>
<td>N/A</td>
</tr>
<tr>
<td>Clay Bytes Solutions</td>
<td>Private investors</td>
<td>N/A</td>
</tr>
<tr>
<td>Econet Wireless Zimbabwe</td>
<td>Econet Global Limited and other private investors</td>
<td>Liquid Telecom and Econet are subsidiaries of Econet Global Limited</td>
</tr>
<tr>
<td>FBNet</td>
<td>Private investors</td>
<td>N/A</td>
</tr>
<tr>
<td>Frampol</td>
<td>Private investors</td>
<td>NA</td>
</tr>
<tr>
<td>Liquid Telecom</td>
<td>Econet Global Limited</td>
<td>69.6</td>
</tr>
<tr>
<td>Powertel</td>
<td>Government of Zimbabwe</td>
<td>4.3</td>
</tr>
<tr>
<td>SADACNET</td>
<td>Private investors</td>
<td>N/A</td>
</tr>
<tr>
<td>Telecontract</td>
<td>Private investors</td>
<td>1</td>
</tr>
<tr>
<td>Telecel</td>
<td>Government of Zimbabwe</td>
<td>N/A</td>
</tr>
<tr>
<td>Dandemutande</td>
<td>Private investors</td>
<td>2.4</td>
</tr>
<tr>
<td>YoAfrica</td>
<td>Private Investors</td>
<td>N/A</td>
</tr>
<tr>
<td>ZARNet</td>
<td>Private investors</td>
<td>N/A</td>
</tr>
<tr>
<td>ZOL Zimbabwe</td>
<td>Liquid Telecom</td>
<td>N/A</td>
</tr>
<tr>
<td>Tel*One</td>
<td>Government of Zimbabwe</td>
<td>23.7</td>
</tr>
<tr>
<td>Aquiva</td>
<td>Private investors</td>
<td>0.2</td>
</tr>
</tbody>
</table>

*Note. N/A means that the market share percentage is not provided. Source: POTRAZ, 2019*

It can be deduced from Table 2 that Econet Global Limited, which owns Econet Wireless Zimbabwe, ZOL Zimbabwe, and Liquid Telecom, controls the lion’s share of the Internet market. It is followed by state-owned ISPs, including Tel*One, Africom, Powertel, and Telecel. The third tier is populated by a number of smaller ISPs, which are owned by individuals and foreign investors.

Zimbabwe has five international gateways for both Internet and voice traffic; three of these are operated by SoEs (Telecel, Tel*One, and Net*One), one is operated by Africom (which is owned by the Ministry of Defence, Security and War Veterans), and one is owned by Econet Wireless Zimbabwe. These gateways allow the speed, access, availability, and price of the Internet in a given location to be determined. Although the ownership and control of international gateways are partially liberalized in Zimbabwe, the government, which owns and controls four of five international gateway systems, enjoys a monopoly. A monopoly in the international gateways market enables the government to willingly interrupt international connectivity—voice and data—at the national level. Because of the government monopoly in the international gateways market, it can be argued that authoritarian governments can limit international traffic into a particular region for specific period, as evidenced by Internet shutdowns in July 2016 and January 2019.
Table 3. Ownership and Control of International Gateway Systems in Zimbabwe.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type of company</th>
<th>Number of gateway systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Econet Wireless Zimbabwe</td>
<td>Private</td>
<td>1</td>
</tr>
<tr>
<td>Telecel</td>
<td>State-Owned</td>
<td>1</td>
</tr>
<tr>
<td>Tel*One</td>
<td>State-Owned</td>
<td>1</td>
</tr>
<tr>
<td>Net*One</td>
<td>State-Owned (Ministry of Defence is the majority shareholder)</td>
<td>1</td>
</tr>
<tr>
<td>Africom</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>5</td>
</tr>
</tbody>
</table>

Source: POTRAZ, 2019

Before the government consolidated the telecommunications market, the Zimbabwe Defence Forces’ former director for communications, Colonel Livingstone Chineka, was quoted in the media as saying that telcos were endangering national security by owning and controlling their own international gateways (“Zimbabwe Army,” 2006). His major argument was that the liberalization of the international gateways was making it difficult for the government to monitor and track Internet and voice traffic coming into and going outside the country. He implored the government to create a single international gateway, which would make it easier for the security services to monitor and verify the revenue and international calls (“Zimbabwe Army,” 2006). This foregoing contextual information must be understood as part of the larger strategy by security services to erect a “digital authoritarian” infrastructure in Zimbabwe.

The capture of regulatory authorities by political elites in Zimbabwe across policy fields has not escaped POTRAZ. Although on paper, the regulator is supposed to operate independently, there is ample evidence to demonstrate that POTRAZ’s independence has waned over the years (Mare, 2016). Its independence has been affected by the powers of the executive through its overbearing influence on appointing key staff. For instance, members of the board are appointed by the president. Equally concerning has been the securitization of key leadership positions at POTRAZ. For instance, in 2016, the President appointed a former director at the Central Intelligence Organization (CIO), Gift Machengete, as the director general at POTRAZ. His appointment was criticized by media advocacy organizations for promoting the militarization and securitization of SoEs (Mare, 2016). It was viewed as a calculated plan by the state to entrench surveillance of online activities (Mare, 2016).

All telcos are guided by the Postal and Telecommunications Act of 2000 and the Interception of Communications Act (ICA) of 2007. The 2007 act grants power to the CIO, the Commissioner of Police, and the Zimbabwe Revenue Authority (ZIMRA) to spy on citizens’ mobile phones and e-mails. Section 9 of the act imposes intermediary liability on telcos, thereby compelling them to install the hardware and software required for the government to carry out communications surveillance. The act also requires telecommunications operators to set up a direct connection to the Interception of Communication Monitoring Center to allow real-time monitoring of voice and data traffic. A company executive who refuses to comply with government orders faces up to three years in prison. Another controversial statutory instrument (SI 95/2014) imposes mandatory subscriber identity module card registration requirements on all mobile phone users in Zimbabwe. A prior written request from an official of the law
enforcement agency is required before POTRAZ is allowed to provide information from its central database to a law enforcement agent.

In addition to the compromised regulatory and legal landscape, the government has been criticized for charging exorbitant licensing fees. This has had a net effect of discouraging both local and foreign direct investment in the sector. The last gazetted licensing fees were pegged at US$137.5 million (Karombo, 2016). License fee requirements have also been manipulated to undermine the financial viability of private players and push business toward SoEs, which are not even compelled to pay the full fees. The selective application of the law in the sector has created a comparative advantage for SoEs. In a country where lawfare has been arbitrarily used against perceived “enemies of the state,” companies such as Tel*One, Net*One, and Telecel have benefited from the use of partisan regulatory decisions by the government. Companies such as Econet Wireless Zimbabwe have complained about the unevenness of the playing field.

The Political Economic Logic of Internet Shutdowns in Zimbabwe

Zimbabwe has experienced two significant Internet shutdowns in the past four years. These shutdowns were carried out through a combination of verbal and written (through a warrant) orders. Verbal orders are often given without written justification in Zimbabwe. On the one hand, legal Internet shutdowns are conceptualized here as those that tick all the boxes of international human rights law, such as legality, legitimacy, necessity, and proportionality (Ayalew, 2019). On the other hand, “extralegal measures” denote a situation in which ministerial orders are outside the remit of the law. A classic case of extralegal measures is the government ordering telecommunications operators to block Internet access without any legal basis in July 2016.

A combination of carrot-and-stick measures has been used by Zimbabwe’s government to block Internet and social media services. In July 2016, the regulatory authority issued a strongly worded written warning to ordinary citizens. In the same written warning, POTRAZ threatened all the telecommunications operators to toe the line or risk losing their operating licenses (see Appendix 1). Following is the press statement published in the media:

The Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) together with all the telecommunications service providers in Zimbabwe have noted with concern, the gross irresponsible use of social media and telecommunications made through our infrastructure and communication platforms over the past few days. We would like all Zimbabweans to know that we are completely against this behaviour and therefore advise that anyone generating, passing on or sharing such abusive and subversive materials which are tantamount to criminal behaviour will be disconnected and the law will take its course. ("Warning Over Social," 2016)

Interestingly, the mentioned threat to disconnect individuals alleged to be abusing Internet services, such as social media, was accompanied by insinuations that the government had the capacity to undertake communications surveillance because of the database it had created as a result of mandatory
registration of SIM cards. According to statutory instrument 142 of 2013, all mobile phone users are required to produce proof of identification and complete registration forms stating their name, permanent address, gender, and nationality. Although citizens who use virtual private networks to circumvent social media blocking could be identified and ultimately punished because of this regulatory requirement, the aforementioned clause is often used to justify communications surveillance and the sharing of user information between ISPs and the government (Mare, 2016).

The ZANU-PF government has also used price increases as a mechanism to limit access to the Internet and social media services. In August 2016, mobile data prices were increased by 500% overnight in an effort to make it unaffordable for ordinary people. In this case, POTRAZ directed all mobile service providers to suspend social media data bundles. This was strongly criticized as a gross violation of the right to information, given that most Zimbabweans rely on "social media Internet"⁹ (Willems, 2016) for their information and communication needs. This is not unique to Zimbabwe. Scholars (Gerbaudo, 2013; Morozov, 2014) have shown that authoritarian regimes often use a cocktail of measures to thwart digital activism and curb online free expression. In authoritarian regimes, Internet shutdowns constitute a viable repressive and demobilizing strategy that is aimed at “disabling access to information and disabling voice” (Glasius & Michaelson, 2018, p. 3797) and controlling both information landscape and citizens’ ability to mobilize.

Another strategy that has been consistently used by the government to arm-twist private telcos relates to the issuance of direct and indirect threats to withdraw or even suspend operating licenses. In June 2010, Econet was threatened with closure for allowing the opposition party, Movement for Democratic Change-Tsvangirai (MDC-T), to campaign on its network through a toll-free interactive service. A ghostwriter, Nathaniel Manheru, widely believed to be George Charamba (who is currently the presidential spokesperson for Emmerson Mnangagwa), threatened to cancel Econet’s operating license. Manheru was quoted in an article by Chimakure (2010) as having said,

> The next polls will be fought on the waves, which is why Econet, and its card-carrying owner, Strive Masiyiwa, are so critical to the MDC-T. We wait for a new propaganda service, which MDC-T seeks to unveil on June 14, using Masiyiwa’s network, through a toll-free facility. Thank God cellular licenses are up for renewal and government has to deal with all manner of mischief. (Chimakure, 2010, p. 12)

It is clear from the preceding newspaper excerpt that the government often abuses its licensing and regulatory powers, thereby coercing private telcos into implementing its directives. Econet reacted by switching off the interactive application meant to be used by the opposition to counter public media propaganda. Licensing renewal is thus used as a weapon in the hands of the government just in case a private operator decides to push back against a government order. This chimes with the CPE approach, which articulates that there are “general and systematic constraints” (Murdock & Golding, 1973, p. 223) that negatively impact the operations of telcos in an authoritarian context.

---

⁹ This refers to partial access to the Internet through the introduction of limited data bundles and zero-rated services for popular social media platforms such as Facebook, Twitter, WhatsApp, and Instagram.
The July 2016 and Partial Internet Shutdown

The first major “partial Internet shutdown” occurred on Wednesday, July 6, 2016. Zimbabweans from all walks of life heeded the call to stay at home to put pressure on the ZANU-PF to fix the economy, respect human rights, and listen to the grievances of ordinary people (Mpofu & Mare, 2020). The protest was organized by #ThisFlag campaign and #Tajamuka movement (Mpofu & Mare, 2020). During this antigovernment protest, WhatsApp was inaccessible for at least four hours, which was evidently a deliberate move to cut off social media services used by protestors to mobilize. WhatsApp ceased to work on Tel*One, Liquid Telecom, ZOL, Telecel, Econet, and Net*One. Whereas most telcos were silent throughout the blackout period, Econet issued a statement to its stakeholders indicating that its service was temporarily down. It read as follows: “Econet would like to confirm that WhatsApp is currently down. We will notify you once it is working again.”

In line with other jurisdictions, the private telcos did not explain the specific reasons for the disruption of services. As intimated earlier, the political economy of the telcos sector, in which the government owns and controls four of five international gateways (by virtue of its ownership of Tel*One, Net*One, Telecel, and Africom), makes it easier for partial Internet shutdowns to be effected even without the buy-in of private telcos such as Econet, ZOL, Liquid Telecom, and Telco, just to name a few. The monopoly enjoyed by Econet Global Limited in the Internet provision sector does not necessarily give the company the power to resist; the government often resorts to extralegal measures (such as threatening and intimidating managers, threatening to withdraw their licenses for noncompliance, and increasing license renewal fees) to exert compliance.

Arguably, the political economy of telcos infrastructure provides the government with sufficient ammunition to order private telcos to shut down their services. Most ISPs rely on international gateway systems operated by SoEs such as Tel*One, Net*One, Africom, and Powertel. Thus, it is not only the number of ISPs in the hands of the government that necessarily and automatically increases the chance for a shutdown, but also the government and regulator’s ability to connect (and disconnect) domestic service providers with regional and international traffic through its gateways. As Weber (2011) insightfully puts it, Internet disruptions are implemented more effectively if the government is able to control the physical infrastructure.

January 2019 and Total Internet Shutdown

Unlike the first shutdown, Zimbabwe experienced a total disruption of all Internet and social media services on January 14, 2019. A total Internet shutdown occurs when all services are blocked without specific targeting of applications or websites. This followed a hefty fuel price increase of 150%, which angered the citizens, causing widespread violence and protests across the country. The government reacted by ordering all ISPs to switch off the Internet and social media services.

---

10 This happens when there is a targeted blocking of the Internet and specific websites or social media services in a given area or a country.
Like the Egyptian incident in January 2011 (Gerbaudo, 2013), the technical details of how the Zimbabwean government performed this operation are still a subject of debate among researchers. However, what is known is that the order was issued by the Minister of State Security, Owen Ncube, in terms of the Interception of Communications Act of 2007. As intimated earlier, some of the provisions of the act allow the government to lawfully intercept or monitor data and voice traffic in order to fight crime and protect national security. In this instance, the Internet shutdown was implemented to mute publicity of a security services crackdown against civilians, especially in places like Harare and Bulawayo. Taking advantage of controversial clauses in the ICA of 2007, the minister, through the CIO director general, Isaac Moyo, ordered all telcos to shut down Internet connection until further notice. The blackout left Zimbabweans without access to the Internet and social media services for at least 7 days (January 14–21, 2019). In many ways, the use of the ICA of 2007 can be conceptualized as part and parcel of the lawfare strategy in an authoritarian regime, in which controversial legal instruments are used to camouflage an unnecessary and disproportionate action with a veneer of legality while still pursuing its political objective to subdue the opponent (Magaisa, 2020).

A screenshot of a Facebook post from Econet Global Limited founder and executive chairman, Strive Masiyiwa, suggested that failure to comply with the ministerial order would have resulted in three years’ imprisonment of the top management of his company, as stipulated in the ICA of 2007. He had this to say:

This morning I was informed that the authorities in Zimbabwe have directed that all Internet services be shut down. As it was a written directive issued in terms of the law, non-compliance would result in immediate imprisonment of management on the ground. . . . I’m sure you will agree that it is extremely unfair to blame Econet executives and engineers in Zimbabwe for something over which they have no control, and which threatens them with imprisonment should they resist. . . . As an organization we are obliged to act when directed to do so in terms of the law. . . . Failure to comply would result in 3 years imprisonment for members of local management in terms of section 6:2 (b). (p. 2)

The preceding quotation suggests that instead of challenging this government order in a court of law, private telcos such as Econet Wireless Zimbabwe, ZOL, and Liquid Telecom decided to comply with the request in order to avoid imprisonment. The behavior of private telcos in Zimbabwe in the face of a government order corroborates the view that failure to follow an order from the ministry or regulatory authority may lead to loss of license or imprisonment—that is, a penalty strong enough to exact obedience in an authoritarian regime (Southern Africa Litigation Center, 2019). In many ways, this finding does not support Freyburg and Garbe’s (2018) expectation that telcos from established democracies may risk public condemnation or even legal challenges if they comply with shutdown requests from local power holders, and they are thus more likely to resist. Econet, which fused with ZOL and Liquid Telecom, is owned only about 5% by Old Mutual in the UK; the rest of shareholders have headquarters in Zimbabwe, Nigeria, and Mauritius. There is no clear-cut legislation in terms of Econet Global Limited’s corporate social responsibility, although the company supports a number of initiatives related to health, education, and youth entrepreneurship in Zimbabwe.
Internet services were partially restored during some of the days to process salaries for civil servants and debt servicing. On Thursday, January 17, 2019, the Internet was briefly restored, but again, another government order was issued, forcing telcos to switch it off. Once again, Econet confirmed the issuance of the second government order in a text message to its stakeholders:

We were served with another directive for total shutdown of the Internet until further notice. Our lawyers advised we are required to comply with the directive pending the court decision on its legality. The earlier directive(s) are already the subject of pending high court application. We sincerely apologize for all inconveniences caused by the acts of government.

Instead of supporting the public interest litigation brought to the court by media advocacy organizations, private telcos were advised by their lawyers to comply with the directive. Given the intercalary position inhabited by private telcos in an authoritarian regime where failure to comply with government orders may result in the cancellation of licenses or even imprisonment of senior managers, they have little room to maneuver. Although the government of Zimbabwe has little control over social media companies such as Facebook, Twitter, and YouTube, the prevailing political and economic framework allows it to directly and indirectly influence the operations of domestic ISPs within its jurisdiction. The relative ease with which the government was able to order all telecommunications operators to block the Internet and social media websites underscores the overbearing role of political and economic factors in a militarized authoritarian context.

The government also abused certain clauses in the licensing contracts that telcos sign with the regulator. These clauses grant POTRAZ the power to order telcos to restrict access to the Internet and social media sites under certain circumstances. Although the clause empowers POTRAZ to order shutdowns in times of national security or because of public safety concerns, it is noteworthy to highlight that these phrases are seldom defined and narrowed down in these contracts.

Although the second shutdown drew widespread condemnation from advocacy groups such as CIPESA and Access Now, the government refused to bow down to external and internal pressure. The government only restored the Internet and social media services after losing a court case in the High Court on January 21, 2019. This was after the Media Institute of Southern Africa Zimbabwe Chapter and the Zimbabwe Human Rights Forum challenged the minister’s order in court. Unlike private telcos, which took the route of compliance, civil society organizations engaged in public interest litigation to push back the digital authoritarian practices. This gives credence to the view that while in a democratic setting, telcos have a choice of whether to push back or to implement a ministerial order (Access Now, 2017); in an authoritarian regime, the situation is rather different.

In the judgment handed down in the High Court, the judge, Owen Tagu, ruled that the minister, Owen Ncube, had no authority to issue an order under the ICA of 2007 to shut down the Internet. The judge also ruled that the right to block all the Internet services lies with the president. He therefore instructed all telcos “to unconditionally resume the provision of full and unrestricted services to all subscribers forthwith.” The judgment served to clarify that according to the ICA of 2007, the president has
the authority to order all telcos to shut down Internet services when national security is under threat. Given the contentious nature of Zimbabwean politics, it is not far-fetched that in the near future, the president may resort to issuing orders to telcos as a way of demobilizing protest action. The court also served as a legal precedent for private telcos to emulate civil society organizations’ strategic litigation route rather than implementing the costly shutdowns.

**Discussion and Conclusion**

It is arguable that even though telcos are expected to balance a responsibility to respect customers’ right to privacy and freedom of expression with its obligation to respond to government orders (Adegoke, 2017), the unequal power relations rooted in political and economic considerations often tilt the pendulum in favor of state-ordered Internet shutdowns. This dovetails with McChesney’s (2003) postulation that the ownership and market structure of telcos and other forms of commercial support affect the provision of services and overall performance.

The High Court ruling has serious implications in terms of reconfiguring the unequal power relations between state and nonstate actors because, despite the assumed “capture” of the judiciary by the political elite, the ruling by judge Owen Tagu is one of few incidences in which the courts have called the government to order. On the one hand, despite the lingering structural constraints, it may empower private telcos to resist future government orders on the basis of legal precedent. On the other hand, it may force the government to implement the “law and order” route whereby the president orders telcos to shut down the Internet, citing provisions of the ICA of 2007. In short, the ruling is a double-edged sword.

In light of this, this article has critically examined why and how private telcos in Zimbabwe complied with government orders to shut down the Internet and social media services in 2016 and 2019. It makes three important arguments. First, it demonstrates that ownership and control of the international gateway systems give the government more influence in terms of restricting or throttling international traffic as part and parcel of digital authoritarianism. It has argued that whoever owns and controls international gateways has the influence to determine the speed, accessibility, and availability of the Internet and social media. This complements existing studies, such as Freyburg and Garbe (2018), that have demonstrated the salience of government ownership of ISPs as an enabler of state-ordered Internet shutdowns. Second, it highlights the role of political and regulatory power through practices such as threats to withdraw or rescind operating licenses, threats of imprisonment, and the strategic use of lawfare in arm-twisting private telcos to comply with government orders. It illustrates that private telcos in Zimbabwe have failed to push back against state-ordered Internet shutdowns. In other words, companies such as Econet, ZOL, and Liquid Telecom have worked as “enablers” rather than “resistors” partly because of the repressive legal architecture of the ZANU-PF government and threat of actual physical violence. Third, it has observed that although private telcos (Econet Global Limited) dominate the market share of mobile and fixed Internet provision, this does not necessarily empower them to resist government orders. It has also argued that regulatory capture by the political elite also plays a significant role in terms of forcing private telcos to abide by government orders.


**Appendix 1: Press Statement Issued by POTRAZ**