The digital dictator dilemma: A comparative study of authoritarianism and internet shutdowns in Africa

Sarah Logan and Jesse Sowell

Department of International Affairs at The George H. W. Bush School of Government and Public Service at Texas A&M University

Abstract:
The use of Internet communication for dissent and to organization protests is a threat to autocrats' control of knowledge and ideas. Internet shutdowns have been deployed, with increasing frequency, as a response to threats to autocrats' power. In some cases, shutdowns are also used to cover additional human rights violations. While shutdowns have received some attention in the literature, it is limited to preliminary observations, and requires additional study to understand their impact and role in the autocrat's toolkit. This article evaluates five medium thickness cases in Africa (identified in Access Now's STOP Data), characterizing autocratic regimes by type, role of technology transfer, and frequency of shutdowns. Two threshold cases, Mali and Liberia, highlight where (1) controlling knowledge and ideas may be perceived as a greater imperative by an already fragile (threshold) autocratic regime and (2) shutdowns may be even more reliant on technology transfers as an intervening factor. A model of autocratic regimes' use of shutdowns is presented, with a special focus on the feedback between goals of the regime, technological capabilities and capacities, and the digital interventions available to reinforce the regime and maintain security. Cases contextualize the relationship between regime type, socio-economic factors, exogenous technology transfers as an intervening variable, and impact of interventions to explain factors shaping Internet shutdowns and their implications. This article concludes with initial policy recommendations on combatting the deployment of Internet shutdowns and way forward for future analysis, particularly emphasizing identification of additional threshold cases, further validating the model further contributing to the literature on the factors affecting the stability of hybrid regimes.

Keywords: Internet Shutdowns; Africa; Autocratic Regime Types; Technology Transfer

Introduction

In December of 2018, Sudan's Capital Khartoum was overrun with protestors demanding an end to Omar al-Bashir's 29-year rule (Feldstein, 2019). Al-Bashir deployed statewide, intermittent internet outages and blocked social media access (Feldstein, 2019). A military junta overthrew him but faced intensifying calls for a civilian-led government (Feldstein, 2019). In response, the transitional military council ordered a nationwide internet shutdown that lasted for three weeks (Buelgasim & Magdy, 2019). A brutal crackdown took place with an estimated death toll of 128 persons (Buelgasim & Magdy, 2019). The use of internet shutdowns by both Al-Bashir and the subsequent junta were not particularly new – they are part of a larger pattern of behavior becoming more recurrent.

Interference with digital infrastructure has become a common characteristic of autocratic and hybrid regimes. Scholarship on the phenomenon is still emerging, with much of that work focusing on China (MacKinnon, 2011; Hellmeier, 2016). Dictators have a variety of evolving options to exert control, but those options remain limited by the specific capabilities and capacities of that regime. To further complicate the situation, China has become an intervening source of technology and capabilities and capacity building that has enabled some regimes to leapfrog their existing (endogenous) capabilities, deploying newly acquired capabilities (more direct control of shutdowns, use of deep packet inspection) to achieve their goals more effectively and maintain power. Evaluating individual cases reveals a potential model of behavior that highlights feedbacks between regime stability and the use of digital interventions (among other conventional factors).

The size, scope, and frequency of shutdowns are growing. In Africa, there were a 89 between 2016 and 2019 alone (Access Now, 2020a). Despite the rise in interventions, it is unclear why states choose to deploy them. They are a blunt solution imbued with economic and human costs. Estimates place the economic toll in Africa at a little more than 2 billion USD (Woodhams & Migliano, 2021: Cost By Region). The Sudan example demonstrates that they can be used to facilitate human rights violations, including state sponsored violence and infringement upon speech and assembly. The Human Rights Council (2016: 4) took notice of the practice in a resolution condemning all measures by states to shutdown internet access and urged them to cease deploying additional shutdowns.

This article focuses on Internet shutdowns trends from 2016 to 2020 in Africa as a response to threats to incumbent power. Across the continent, governments favor statewide deployments unlike other regions that utilize more sophisticated means of targeting (Taye, 2020: 6). In part, this is a product of their capabilities and capacities limiting the types of interventions available. Complex interventions require technology and professionals capable of managing them. To lay the groundwork, the mechanisms used to limit Internet communication such as deep packet inspection or filtering are presented, followed by a brief review of existing factors driving shutdowns: regime type, and Internet Service Provider (ISP) ownership. These factors are used to explain shutdowns in five states: Ethiopia, Eritrea, Liberia, Mali, and Zimbabwe. One additional common factor is significant Chinese investment and engagement in the telecommunications sectors in these countries. Actions by Chinese state affiliated technology giants Huawei and ZTE, amongst others, appear to be diffusing dangerous norms about internet governance and privacy rights to their client states.

To evaluate the dynamics associated with Internet shutdowns, this article develops a model highlighting the relationships between regime type, political objectives, and how the regime's capabilities and capacities determine the types of intervention available to them. In a number of these cases, technology transfer from China is an intervening variable that increases the regime's technical capabilities and capacities, and, in turn, contributes to its ability to achieve goals related to censorship and surveillance. Medium thickness case studies are presented to evaluate the efficacy of this model. Analysis of these cases suggests that current efforts at combatting the use of shutdowns – naming and shaming and pointing to the economic costs – cannot achieve their ends alone.

The recommendations argue that combatting the shutdowns as a tool of authoritarian regimes will require liberal regimes take a more active role in capacity building – funding and developing telecommunications infrastructure and human capital – while being cognizant of the region's history with colonialism. Developing human capital means both immediate training, and development of training capabilities (training for trainers) in the region. Competitive western alternatives are necessary to catalyze the liberalizing benefits of the internet. Of secondary importance, the West will need to encourage private ownership of ISPs. Finally, it must support local civil society organizations that can challenge shutdown orders on behalf of ISPs, who lack the choice to ignore orders in authoritarian regimes. These recommendations will have differing levels of success depending on the regime type in question. For instance, multiparty authoritarian regimes depend on the electorate for legitimacy, so they are more likely to allow space for local civil society actors to contest actions that violate the rule of law than other types of autocracies, so supporting these organizations has the potential for success. Military regimes will likely be impervious to these campaigns. Liberal regimes will need to prioritize the appropriate mix of interventions to support where those interventions are expected to be most effective for protecting human rights. Low-cost efforts, such as naming and shaming, should not be abandoned, but they can be targeted more effectively. Finally, the article concludes with considerations for future research, particularly the identification of additional threshold cases and their relevant characteristics to create a spectrum.

Background

Studies on strategies of digital repression are numerous, but they vary widely in amount and region depending on the specific layer in question. Network layer interventions scholarship highlights sophisticated filtering regimes, such as those of China and Russia (Mou, Wu & Atkin, 2016; Sanovich, Stukal & Tucker, 2018). Whereas studies on the application layer concentrate on the power of social media for organizing, such as in the Arab Spring (Stepanova, 2011; Hussain & Howard, 2012), or disinformation, vis-à-vis Russian bots (Sanovich, 2017; Sanovich, Stukal & Tucker, 2018). Existing literature favors interventions that depend on a higher level of capabilities and capacities than found in most African states. It often warns that advanced strategies of digital repression will be exported from China or other autocracies, but rarely accounts for the relationships between autocratic regime type and their differing level capabilities and capacities. Autocratic regimes are typically sustained by a combination of internal intelligence services, control of information, and a willingness to respond violently to threats. Internet communication is the modern means of disseminating ideas, constructing, and sustaining transnational polities, such as human rights norms, that often challenge autocratic regimes. Strategies of digital repression are another tool by which autocrats survive. The kind of intervention is significant, requiring varying levels of sophistication that are not universally available. Efficacy depends on the capabilities and capacities of the regime and whether these regimes are getting substantial external support.

In Africa, strategies of control have favored interventions in the development and operation of the Internet's infrastructure. This includes the degenerate case, deliberately obstructing Internet development or the introduction of technologies that may not be as easily controlled as existing communications technologies. Where infrastructure does exist, interventions rely on partial shutdowns, complete shutdowns, and/or throttling. This section provides brief acknowledgement of network and application layer interventions, but focus primarily on infrastructure layer, nuanced regime type, and ISP ownership. This article helps understand where autocratic regimes perceive interventions to be most effective and the strategies for acquiring the capabilities and capacities necessary to achieve their goals through these types of interventions. Through five case studies, indicators are identified that help contextualize the relationships in the model. Cases pay special attention to the implications of Chinese technology investment. Taken together, this analysis

highlights that a nuanced understanding of autocratic regime type and technological capabilities and capacities are distinctions necessary to understand the role of digital interventions in regime maintenance.

Mechanisms for control

There are myriad interventions that can be deployed at various layers of the network depending on a regime's capabilities and goals. Broadly speaking, states can intervene at the physical layer (manipulating physical cables and hardware), at the network layer (manipulating how data is accessed and routed in local networks), and/or the application layer (requiring monitoring software on end devices such as mobile phones or laptops, or surreptitiously installing malware for surveillance and/or censorship on those devices) (Keremoğlu & Weidmann, 2020: 1691–1692).[1] Studies of interference at the physical layer are the least common (Keremoğlu & Weidmann, 2020: 1692). Most focus on interference at the network layer, with a notable preponderance of observations linked to the Chinese government's strategy of control (Hellmeier, 2016; Rydzak, 2016; Keremoğlu & Weidmann, 2020: 1693).

China's primary mechanism of control is the Great Firewall, one of the most sophisticated approaches to internet filtering, surveillance, and censorship in the world carried out by DNS manipulation, URL filtering, keyword filtering, and IP blocking amongst other practices (MacKinnon, 2011; Shen, 2014; Griffiths, 2021). Building and maintaining the Great Firewall required substantial technical capabilities and capacities, centralized management, and access to capital. The sizeable domestic application of these tools led to their commodification. China is now promulgating its regime internationally, in part by distributing its information flow control. China is a willing supplier that engages in capacity building vis-à-vis training personnel to manage and deploy these tools.

Autocratic regimes have a natural demand for these tools and constitute a target market in China's ideological strategy, mobilized partially via the Digital Silk Road initiative. Lacking resources, and often lacking the capabilities and capacities, developing states rely on less advanced interventions that require simple operational changes at the network layer or direct intervention at the physical layer. Shutdowns are frequently grouped into a larger strategy of control that includes internet filtering or censorship at the network layer (Zittrain et al., 2017). Unlike more sophisticated forms of intervention geared toward deterring threats, shutdowns are typically invoked as a response to threats. Their impacts are obvious and immediate to the population.

Effective analysis of digital repression requires identifying the type of intervention, and possible means to either circumvent or mitigate the impact of those interventions. Differentiating between the various strategies of interference that regimes can deploy is important for understanding their capabilities and the influence of actors capable of providing additional capabilities, such as China. Other states have similar capabilities but have not invested in them to the same extent as China, nor have they demonstrated the will to deploy interventions explicitly for political control.

Regime type

Three factors affect the relationship between authoritarianism and the use of infrastructure interventions: internet penetration; longevity in power; and regime type. Rydzak (2016: 22) argues that in non-democratic states, internet penetration and mobile density are positively correlated with the deployment of shutdowns. Further, his study suggests that this correlation "tapers off" as penetration increases (Rydzak, 2016: 18). Longevity in power is associated with deploying shutdowns. (CIPESA, 2019: 7). Regimes that deploy shutdowns are authoritarian (Howard, Agarwal & Hussain, 2011: 224). Although, hybrid regimes have also deployed shutdowns (CIPESA, 2019: 6). That said, a significant

[1] The layer language from Keremoğlu and Weidmann has been adapted for clarity.

number of autocracies have not deployed shutdowns. To better understand the relationship between autocracy and shutdowns, this article uses a nuanced typology to map the relationship between type of autocracy, goals, and infrastructure intervention. Autocracies demonstrate varying characteristics, which influence their power maintenance.

Geddes' (1999: 121) seminal autocratic regime typology initially posited three categories consisting of personalist, military, or single party. This proved too restrictive. Geddes, Wright, & Frantz (2014: 318) expanded the typology to six categories: dominant party rule, military, personalist, monarchic, oligarchic, or indirect military rule. Categorization criteria sort regimes based on who selects leaders, who controls policy, and who controls security operations (Geddes, Wright & Frantz, 2014: 318). Formal governance institutions do not matter (Geddes, 1999: 124). Geddes, Wright, & Frantz (2014: 314) contend that informal rules matter significantly more in autocracy. These coding decisions mean that while a state may experience institutional upheaval or changes in leadership, that does not automatically entail a new classification. For instance, the entirety of Somoza rule in Nicaragua is classified as the same regime type (Geddes, Wright & Frantz, 2014: 314).

While Geddes focuses on ruler identity, Wahman, Teorell, & Hadenius' (2013: 20–21) typology emphasizes how regimes use institutions to maintain control. This can lead to coding regime changes when the head of state has not changed, but their method of maintaining power has (i.e. Somoza rule is broken up into different regimes) (Wahman, Teorell & Hadenius, 2013: 21). Wahman, Teorell, & Hadenius' (2013, 24) typology includes military, monarchy, multi-party authoritarian, one-party authoritarian, no-party authoritarian, and other. The typology further disaggregates electoral autocracies by one-party, multiparty, and no-party (Wahman, Teorell & Hadenius, 2013: 31). In contrast to Geddes et al (2013), it does not include a personalist category because it blurs the distinction between rule and regime.

One key challenge is that categories developed for regime type analysis may not completely characterize all cases. Hybrid regimes are particularly difficult to classify. Some states considered electoral autocracies might better be classified as highly flawed democracies. Ontologically, typologies of comparative authoritarianism face challenges similar to typologies of democracy: exempting equally robust classifications where the "edges" of the two types of regime overlap is limiting.

This article proceeds with Anckar & Frederrikson's (2019) typology, which uses elements of both Wahman et al's and Geddes' typology to classify authoritarian regimes.[2] It is worth noting that the definitions that Anckar & Frederrikson (2019, 85-86) apply to authoritarian regimes do not differ significantly from the aforementioned datasets. It is the inclusion of subindices of democracy *alongside* authoritarianism that set Anckar and Frederrikson's dataset apart. The decision to integrate both categories of regimes into a singular dataset more accurately captures the complicated characteristics of hybrid regimes and leaves the door open for future analysis to include democratic regimes deploying shutdowns.

While the dataset covers an impressive time period, it ends in 2016. The case studies in question have been evaluated to determine if the most recent classification still applies, or if it needs reclassification. Anckar and Frederrikson (2019: 86) provide relevant definitions for each classification and information on their judgement sources, namely Freedom House and Varieties of Democracy.

ISP ownership

[2] The article also considered Steffen Kailitz's "Classifying political regimes revisited: legitimation and durability," as a potential typology, but the ones we chose are more appropriate for evaluating the gross impacts of national shutdowns. That said, ongoing work is considering the substantive content blocked in particular shutdowns and its interface with strategies of legitimation.

Although sparse, literature on ISP ownership attempts to explain the conditions under which shutdowns occur. Majority state ISP ownership was positively correlated with shutdowns prior to elections, yet numerous states with similar ownership patterns and circumstances did invoke them (Freyburg & Garbe, 2018: 3911). ISP ownership varies across states with private ISPs also complying with shutdown orders. Mare (2020) asserts that intervening variable is the ownership of Internet gateways, which link local networks to the global Internet. Rather than ordering the ISPs to deny user access to the Internet, they may simply sever connectivity for the ISP as a whole, at the gateway (Mare, 2020: 4259).

Model and case selection

This article presents five medium thickness case studies to evaluate relationship between autocratic regime type and shutdowns. Nuanced regime type, for example military rule, influences goals. How the regime achieves its goals, how easily, and how effectively, are contingent on the capabilities and capacities available to that regime. For example, deep packet inspection technology can facilitate sophisticated surveillance, censorship, and attribution goals. It offers a broader variety of options than the blunt tool of simply turning the Internet on or off. Regime capabilities and capacities thus influence the type of intervention that a regime can pursue, and to some extent, how efficiently and efficaciously it can control the flow of knowledge and ideas. Technology transfers from China are presented as an intervening variable that can bolster the capabilities and capacities of regimes. Liberal interventions can provoke a similar response in the mode by injecting technologies while encouraging their use and management be consistent with respect for human rights, such as seen in the Liberian case. Technology injections, in turn, affect the efficacy and kinds of interventions and nuance in the objectives a regime can pursue. Successful interventions reinforce the regime and can create a feedback loop. This model of behavior is depicted in Figure 1.

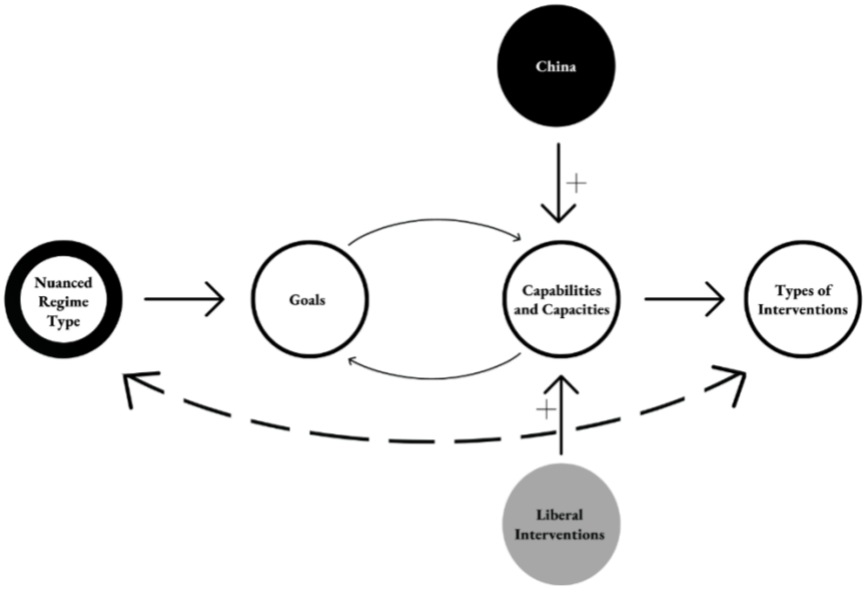

Figure 1. Model

The five cases selected are Ethiopia, Eritrea, Liberia, Mali, and Zimbabwe. Access Now's STOP Data (2020b) provides verified instances of internet shutdown from 2016 to 2020. The dataset documents shutdowns in 29 African states. Of these, 12 deployed shutdowns once. The remaining 17 deployed shutdowns 2 or more times. Only observations of national shutdowns in response to threats to incumbent power, specifically, protest, political instability, or upcoming elections, were considered.

Instances where third party, nonstate actors were responsible for deploying a shutdown were excluded. Finally, cases must be publicly sourced to provide sufficient. Among the remaining cases, selections emphasized a diversity in explanatory factors: ISP ownership, longevity of leader in power, internet penetration, and geographic area on the continent. Table I shows the selected case characteristics.

Table I. Cases

State	Shutdowns since 2016	Regime Type	Internet Penetration	State ISP Ownership	Leader Years in Power
Ethiopia	19	Multi-Party Authoritarian	25.00%	Total	1
Eritrea	1	Military Rule	1.00%	Total	26
Liberia	1	Presidentialism	22.00%	Minority	1
Mali	4	Semi-Presidentialism	26.00%	None	7
Zimbabwe	2	Multi-Party Authoritarian	25.00%	Majority	2

Cases

Each case provides a narrative of the shutdown, including duration, ISPs involved, services affected, and accounting of potential human rights violations. It then accounts for China's investment in the state's telecommunications infrastructure. One investment is present across three cases. Ethiopia, Eritrea, and Zimbabwe are all members of Comtel, a regional telecommunications network of 20 countries that partnered with ZTE in 2003 to install fiber optic cables across the region, with a ZTE investment that entitled it to shareholder status (Executive Research Associations, 2009: 57–58). According to Freedom House, government and/or media officials of these three states have also attended media trainings in China (Shahbaz, 2018: 9). Next, the level of state ownership of ISPs and context of the population's access to service is explored. Finally, the case describes regime type and how regime type characteristics influence deployment of shutdowns to achieve goals. Each case concludes with key observations that are compiled in total in the Analysis Section.

Ethiopia

In Ethiopia, the feedback loop in the model is strongest. China has engaged in significant technology injections for nearly two decades expanding Ethiopian capabilities and capacities leading to an evolution of surveillance and censorship goals. Each shutdown reinforces the regime and enhances the feedback loop. On June 6, 2019, spontaneous protests erupted following the murder of political activist, musician Haacaaluu Hundeessaa, and the government deployed a shutdown for 37 days in response (Access Now, 2020b). The statewide shutdown lasted until day 23, with various regional mobile networks and app-based disruptions intermittently applied during the final two weeks (NetBlocks, 2020a). Since 2016, Ethiopia has had 19 documented shutdowns, making it the most prolific initiator in Africa (Access Now, 2020a). Ethiopia's single, state-owned ISP, Ethiotelecom executed the shutdowns (Freyburg, Garbe & Wavre, 2019: 3; Access Now, 2020a). In the crackdown that followed, reports indicate that at least 289 people were killed, 167 were injured, and over 7000 were detained (Agence France-Presse, 2020a; Ayana, 2020). Hundeessaa ignited a generation of young political activists, and his murder provoked protest on an unprecedented scale (Ayana, 2020). Prime Minister Abiy Ahmed ordered the shutdown to limit speech that could incite further violence (Access Now, 2020a).

ZTE has been responsible for the National Fiber Backbone Project, 2G network expansion, 4G network expansions, a smart health system, a minor role in the new African Union (AU) headquarters ICT, a dense wavelength division multiplexing optical transport network for the western and southern regions, donating ICT for a Joint Innovation Center, and sole equipment provision to the state from 2006 to 2009 (ZTE Press Center, 2019; Australian Strategic Policy Institute, 2021). Huawei provisioned ICT for the AU, a Mobile Money Platform and accompanying data center for Ethiotelecom, a smart city project, parts of the National Fiber Backbone Project with ZTE, and 36

Ethiopian universities to provide the Certified Network Associates Certification to ICT professionals (Smart Cities World Forums, 2017; Australian Strategic Policy Institute, 2021). Three other Chinese technology companies have also contributed: Uniview developed the video surveillance system for the AU; China Comservices played a role in the National Fiber Backbone Project; and Hengbao is the primary SIM card supplier for Ethiotelecom (Australian Strategic Policy Institute 2021; Freedom House 2018, A. ICT Market). There is evidence that ZTE has exported monitoring and surveillance capabilities to Ethiotelecom alongside its infrastructure upgrades: the ISP can conduct deep packet inspection and utilizes ZSmart, an application that enables the state to intercept texts, access user information, record phone calls, and track phone locations in real time (Freedom House, 2018: C. Surveillance, Privacy, and Anonymity).

Internet penetration by Ethiotelecom is at 25% (The World Bank, 2020). Ethiotelecom has centralized control of all domestic internet traffic (Freedom House, 2018: Restrictions on Connectivity). Satellite, terrestrial fiber-optic connections with Sudan, and the SEACOM cable through Djibouti connect Ethiopia to the Internet (Freedom House, 2018: Restrictions on Connectivity). Despite 85% of the population residing in rural areas, access is low (Freedom House, 2018: A. Availability and Ease of Access). Mobile penetration has grown to 60%, but suffers from limited signal stations, resulting in high levels of congestion, frequent disconnections, and slow speeds (Freedom House, 2018: A. Availability and Ease of Access). Internet and mobile service prices are prohibitively steep and artificially inflated by the monopoly, excluding a majority of the population (Freedom House, 2018: A. Availability and Ease of Access). Many Ethiopians utilize cyber cafes, especially in the rural areas, but these are expensive and subject to frequent blackouts (Freedom House, 2018: A. Availability and Ease of Access).

Anckar and Fredrikkson (2019: 91–92) classify Ethiopia as a nominally multiparty authoritarian state, in which a single party dominates political offices and policymaking. Ethiopia continues to be plagued with poor institutions, widespread human rights violations, and internal conflict despite the liberalization that was expected with Ahmed's designation as Prime Minister in 2018 (Freedom House, 2020a). Ahmed was a longtime member of the Ethiopian People's Revolutionary Democratic Front (EPRDF), until founding its successor Prosperity Party; the reorganization transitioned the EPRDF from a range of ethnically based affiliates to a unitary party keeping the locus of power in the same place (Freedom House, 2020a: B1). Despite superficial changes, multiparty authoritarian remains an accurate designation. These regimes tend to be at higher risk for armed internal conflict, but their necessity for electoral support to legitimize the ruling apparatus acts as a slight restraining factor (Fjelde, 2010: 196–197). Multiparty authoritarian regimes suffer from information problems about opposition due to lack of political environment control (Fjelde, 2010: 201). They have less leverage for co-opting opposition, so in the face of challenge, violent response is likely (Fjelde, 2010: 203).

Ethiopia has the highest utilization of shutdowns. The June 2019 shutdown aimed to disrupt largely spontaneous organization while carrying out mass arrests and what has been described as crimes against humanity (Mekonnen & Jelan, 2021). The lack of restraint appears to run in contrast to what would be expected of multiparty authoritarian regimes. Shutting down the internet increases confusion and provides cover for the ruling party to retaliate against opponents while minimizing audience costs. Considering that the information problem is magnified in multiparty authoritarian regimes, and that they lack options for co-opting opposition, violent retaliation against overwhelming protest is consistent with the typology. Despite obstacles to access, Internet penetration has crossed a threshold high enough to make it a threat. State ownership of Ethiotelecom makes it easy and effective to execute shutdowns, which partially explains why Ethiopia employs shutdowns frequently. The introduction of Deep Packet Inspection through Ethiotelecom's longstanding relationship with Huawei and ZTE offers more nuanced and effective means of censorship and adds surveillance to

the state's digital repression toolkit. There is some potential evidence that Ethiopia is utilizing these expanded capabilities. In trials against journalists and bloggers, there are documented reports of the state using intercepted emails and records of mobile phone conversations, and blocked media outlet websites (O'Carroll, 2016: 15–17; Freedom House, 2018: C. Surveillance, Privacy, and Anonymity).

Eritrea

In Eritrea, the model demonstrates how the nuanced regime type, military, operates with inherent fragility, so the goal is to quash dissent entirely. Considering the low level of capabilities and capacities even with Chinese technology injections, simple infrastructure interventions vis-à-vis a shutdown reinforced the regime. On May 15, 2019, the Eritrean government deployed its first documented shutdown, lasting 10 days (Africa News, 2019). Access to social media sites was blocked in response to expected Independence Day protests (Africa News, 2019). It is unknown if any violence or arrests took place during the shutdown (Access Now, 2020a). Reporting is limited, in part due to the lack of connectivity. Eritrea's single, state-owned ISP Eritel is responsible for executing shutdowns (Freyburg, Garbe & Wavre, 2019: 3; Access Now, 2020a).

In 2011, the Chinese government provided a loan for improvements to telecommunications infrastructure by ZTE and Huawei (Australian Strategic Policy Institute, 2021). The Ministry of Information has publicized attendance at two Chinese media trainings prior to the 2019 shutdown (Eritrea Profile, 2018; Xinhua News, 2019). There little on the exact nature of these trainings, but they constitute sustained contact between the regimes and an opportunity for China to disseminate norms regarding media freedom and telecommunications.

Internet penetration in the state is the lowest in Africa at only 1% (The World Bank, 2020). Mobile Internet access is unavailable (Winter, 2014). Access is only available at the roughly 100 physically monitored internet cafes, or by a small, approved number of $200 USD per month dial up subscriptions (Winter, 2014). There are no submarine cable landing stations in Eritrea, nor fiber optic connection, with only "very small aperture terminal" connections present (Katlic, 2014; Winter, 2014). Speeds are extremely slow; it is not uncommon to wait more than a half hour for a single webpage to load (Winter, 2014). Considering how little of the population has access to the internet and the majority of those that do access it grapple with impossibly slow speeds while security services monitor their usage, the utility of a shutdown is not immediately apparent. Despite social media's prominence as an online organizing tool, text and email can achieve the same ends as effectively in limited connectivity environments.

Anckar and Fredrikkson (2019: 91) classified Eritrean autocracy as a military regime. Military regimes are defined as "a country [that] has been uninterruptedly ruled by the same person that came to power in a military coup," and that has bases of power rooted in the military (Anckar & Fredriksson, 2019: 91). Isaias Afwerki's has continued to depend on his military power base and has not instituted any serious reforms. It is one of the most repressive autocracies. Nonexistent press freedoms are a common characteristic of military regimes, and Eritrea has the lowest ranking press freedom score in the world, with all media outlets state owned and highly censored (Geddes, Frantz & Wright, 2014: 156; Kansara, 2019). Other common characteristics of military regimes include a greater propensity for violating physical integrity rights, higher levels of state fragility, and increased likelihood of using force to respond to opponents (Geddes, Frantz & Wright, 2014: 141–142, 156).

Eritrea *rarely* experiences protest. Prior to the 2019 shutdown, there was one episode of limited dissent spanning across three schools in the capital region (Zere, 2017). The regime was purportedly caught off guard and responded with a heavy military presence, in part to discourage future attempts (Zere, 2017). It is unclear if there were casualties or arrests, but participants captured the violence with cell phone videos that were shared internationally (Zere, 2017). In the post-school protest era, Afwerki may have deployed the shutdown as a complement to the traditional military response for security,

specifically to prevent any potential footage leaks and quash dissent. A heightened sense of threat in response to a rare protest resulting in an aggressive, multifaceted strategy of control fits expected regime bheavior. The 2017 protests footage leak demonstrated that cell phone video and internet access have reached a threshold to threaten the regime and proved there is latent potential for internet organized protests. Complete state ownership enabled the shutdown to be employed with speed, ease, and effectiveness when the regime perceived a threat.

Liberia

The model plays out in Liberia by including both Chinese technology injections and liberal interventions. The impact of liberal interventions is a slowing of the feedback loop and encouragement of achieving goals that are not entirely contrary to human rights norms. On June 10, 2019, the Liberian Government ordered its only documented shutdown citing public safety reasons (Access Now, 2020a). State ownership of ISPs is low in Liberia (Freyburg, Garbe, and Wavre 2019: 3). The various ISPs, Libtelco, Lonestar Cell MTN, Novafone, and Orange, executed differing interpretations of restrictions blocking access to WhatsApp, Facebook, Snapchat, Twitter, Instagram, Gmail, and the Associated Press Website (Access Now, 2020a). The widely publicized #SaveTheState protests were a response to corruption and soaring inflation; they were considered the largest anti-government protests since the civil war ended in 2003 (Dodoo, 2019; Mengonfia, 2020). Despite the volatile situation and the legacy of state-sponsored violence in response to civilian protest in Liberia, there were no reports of death, arrest, or injury (Sieh, 2019).

Liberia has the fewest investments from Chinese telecommunications firms. Court documents revealed that ZTE bribed state owned Liberia Telecommunications Corp (LTC) to steal a major upgrade contract bid from an American company in 2005 (Wu, 2018). Despite a Liberian Supreme Court order staying the project, ZTE continued its work with LTC (Balancing Act, 2006). In 2006, Huawei's developed the Comium (Novafon) Mobile GSM network (Australian Strategic Policy Institute, 2021).

While internet penetration is only at 22%, 10% of the country depends on social media for communication, and it served as a critical venue for organizing the #SaveTheState protests (Sieh, 2019; The World Bank, 2020). Liberia has benefited from recent upgrades to its telecommunications sector including the completion of a fiber optic submarine cable, and a recent partnership between the United States Agency for International Development, Google, Mutsui & Co of Japan, Convergence Partners of South Africa, and the World Bank International Finance Corporation to build a fiber ring around the capital and extend it to rural areas (International Trade Administration, 2021). Still, subscription and device costs are expensive, especially in light of rising inflation rates, speeds are slow, and rural communities lack infrastructure (Sarpong, 2020; International Trade Administration, 2021).

Anckar and Fredriksson (2019: 87) classify Liberia as a presidential system, which is a subclassification of democracy, and system of government that is directed by a president that cannot be dismissed by a no confidence vote from parliament. It suffers from election irregularities, unrealized civil liberties, and corruption, but experienced the first peaceful transfer of power since the 1940s in 2018 to George Weah and has slowly rebuilt its institutions (Freedom House, 2020b). In light of this, extending the classification is technically appropriate, but hybrid characteristics should be included due to the lack of even semi-democratic consolidation. Hybrid regimes lack respect for rule of law, struggle with corruption, score poorly on press freedom, and endure higher audience costs for mismanaging political discontent than pure autocracies (Ekman, 2009: 9, 13).

Unlike the other cases, Liberia's shutdown deployment was not utilized to provide cover for a violent crackdown. It appears the Weah regime sought to suppress online mobilization because the user threshold and dependence on social media for communication represented a threat. The higher

audience costs associated with crackdown likely restrained the regime while also explaining its desire to control the flow of information. This points to the possibility that hybrid regimes bordering on semi-consolidated democracies maintain different ends for their shutdown strategies than autocracies or hybrid regimes bordering on autocracy. Liberia is the state with the least amount of Chinese investment in its telecommunications sector. Its historic relationship with the USA has enabled competitor companies to be present in the sector, which is likely serving as a counterbalance. This demonstrates how liberal interventions can bolster capabilities and capacities of regime to pursue their goals with increased respect for human rights as described by the model.

Mali

In Mali, the model demonstrates how nuanced regime type can be influenced by significant technology injections from China without liberal interventions. Mali's capabilities and capacities have recently expanded, but this has not yet produced an observable surveillance goal shift. On July 10, 2020, the government of Mali deployed a shutdown that lasted for five days in response to widescale protests (Access Now, 2020a). The July Protests were the culmination of months of growing frustration and smaller demonstrations across the state (Agence France-Presse, 2020b). 14 were killed including 2 children, and 158 sustained injuries (Diallo, 2021). Facebook, Twitter, Instagram, WhatsApp, and Messenger were blocked (NetBlocks, 2020b). Unlike other cases, ISPs in Mali are entirely privately owned (Freyburg, Garbe & Wavre, 2019: 3). The shutdown was executed by Malitel (Sotelma), Orange (Sonatel), and Telecel (Atel) with some variety amongst execution, but the result was almost total blackout (Access Now, 2020a; NetBlocks, 2020b). Mali's level of internet penetration is at 26%, but just 22% of households have access with only 10% of those residing in rural areas (The World Bank, 2020; International Telecommunications Union, 2021). This is the fourth shutdown since 2016, with two in 2018 in response to upcoming elections, and the other in 2016 due to protests (Access Now, 2020a).

Mali has had 15 years of partnership with Huawei. In 2006, Huawei helped Soltelma secure funding to develop and equip the wireless network (Xinhua News, 2006). In 2015, the Chinese EX-IM Bank announced it would finance a Huawei fiber optic network project representing a significant upgrade to the sector (Australian Strategic Policy Institute, 2021). As part of the project, Huawei upgraded government communications systems including installing a new video conferencing system, installing traffic surveillance, providing equipment for data monitoring rooms, and building a centralized data center in Bamako (Ecofin Agency, 2015). President Ibrahim Boubacar Keïta (IBK) noted Huawei's role in smart city construction during a 2018 visit to headquarters (Huawei, 2018; Australian Strategic Policy Institute, 2021). During that visit, IBK emphasized the importance of continued partnership with the company to expand the telecommunications sector in Mali and agreed to participate in Huawei's "Seeds for Youth" project, which enables Huawei to "cultivate [Mali's] local ICT talent" (Huawei, 2018).

Mali has experienced significant political turmoil in the last year, but at the time of the 2020 shutdown, – and every shutdown in Mali – IBK was head of state. Anckar and Fredriksson (2019: 89) classified Mali as a semi-presidential system, which is a subclassification of democracy that involves power sharing between a prime minister and a president who maintains control of "important, explicit executive powers." IBK was serving out his second term as president following a 2018 election that displayed irregularities and low turnout in the north but was considered relatively free and fair (Freedom House, 2020c: A1). IBK was the first post-coup president and was widely believed to have significant support from the Malian military (Ward, 2020). While cabinet shuffles took place, and 2018 legislative elections were both delayed and tampered with, significant political change has not occurred to warrant classifying it differently (Freedom House, 2020c: A1, A2). The lack of robust institutions, strong electoral systems, and respect for political rights depict a regime that does not meet the

qualifications for even semi-consolidated democracy. Mali is an unstable hybrid that is teetering on autocracy, but the semi-presidential democracy classification is the most accurate when hybrid regime characteristics are synthesized with it.

Mali is on the opposite end of the spectrum from Liberia. Instead of bordering on transition to flawed democracy, it is close to the edge of authoritarianism. Recall that Ekman (2009: 9, 13) explains hybrid regimes suffer from lack of consolidation in rule of law, higher audience costs for violence, and poor press freedom. The audience costs were not enough to restrain a crackdown by IBK. However, the level of violence was more restrained than what is observed in purely authoritarian Ethiopia and Zimbabwe. A month after the crackdown, IBK is deposed by a widely celebrated military coup (Fornof & Cole, 2020). The lack of condemnation over IBK's forced resignation and the warm welcome extended to the coup organizers is an audience cost. It demonstrates that hybrid regimes, even those trending toward authoritarianism, still suffer from audience costs, but they are not necessarily enough to solidify restraint. IBK's decision to deploy a shutdown exemplifies the disregard for media freedom and desire to control information – this would be considered a goal in the model – common in hybrid regimes. The private ownership of Mali's ISPs led to an initially inconsistent execution of that shutdown, but it did not prevent it from occurring. Huawei's extensive investment, especially vis-à-vis a data monitoring center demonstrate potentially evolving surveillance goals.

Zimbabwe

In Zimbabwe, feedback loop highlighted in the model is strong. China has injected technologies that have bolstered Zimbabwean capabilities and capacities, in turn expanding surveillance goals. On January 15, 2019, the government of Zimbabwe deployed a nine-day shutdown of broadband and mobile internet in response to the fuel protests (Taye, 2019; Access Now, 2020a; Noyes, 2020). Major cities like Harare and Bulawayo and social media sites went offline first (NetBlocks, 2019). By the second day, statewide connections were completely severed, as was access to social media platforms Facebook, Twitter, Whatsapp, Pinterest, and Tinder (NetBlocks, 2019). The brief time lapse stems from ISP ownership. Zimbabwe has a complicated mix of state and private ownership, but the majority is state owned, with Econet Wireless, Telecel, and NetOne responsible for executing with the shutdown order (Freyburg, Garbe & Wavre, 2019: 3; Access Now, 2020a). The crackdown resulted in 17 dead, more than 1,000 arrests, and 17 reports of rape (Noyes, 2020). The fuel rotests were a crescendo following months of localized protests on various socio-economic problems plaguing Zimbabwe, and they were the largest since the country's longtime dictator Robert Mugabe was deposed (Idindili, 2019). This was the second documented shutdown since 2016, and the first since Mnangawa took power in a flawed election after the 2017 coup (Access Now, 2020a; Noyes, 2020).

Engagement between both Chinese telecommunications companies and the Mnangawa administration directly is high in Zimbabwe. China's EX-IM Bank and Development Bank have provided multiple million dollar loans for NetOne and Econet mobile service providers to purchase Huawei and ZTE equipment, respectively (Kazunga, 2014, 2015). EX-IM Bank funded the National Broadband Project, a joint venture between Zimbabwe and China to expand the primary state owned mobile broadband provider NetOne's coverage to the entire country (Freedom House, 2021: A3; Xinhua News, 2021). Huawei built a data center for state owned telecommunications operator TelOne as part of the Project (Xinhua News, 2017). Mnangawa and Cloudwalk, a tech start-up allegedly involved with human rights abuses of Uyghurs, signed an agreement for the first Artificial Intelligence project in Africa to deploy facial recognition software to the CCTV cameras and all transit security and create a national facial database (Hawkins, 2018; Reuters, 2020). In turn, Zimbabwe transmits the collected biometric data back to Cloudwalk to fine-tune the software accuracy for darker complexions (Hawkins, 2018).

Zimbabwe reports internet penetration at 25% (The World Bank, 2020). Rural penetration is significantly lower at an estimated 10% (Freedom House, 2019: A2). Expensive pricing coupled with runaway inflation have made access prohibitively expensive (Freedom House, 2019: A2). Further, Zimbabwe's broadband speeds are slow, with it being ranked at 121 out of 200 countries measured (Freedom House, 2019: A1).

Anckar and Fredriksson (2018, 91–92) classified Zimbabwe's regime as multiparty authoritarian. Mnangawa's administration welcomed a higher level of political competition in the immediate 2018 elections, but the Zimbabwe African National Union – Patriotic Front (ZANU-PF) maintained the majority (Noyes, 2020). This sparked opposition protests and a violent crackdown that marked the end of the brief period political openness (Noyes, 2020). The role of the military has been elevated by Mnangawa, but he remains a civilian leader with his primary power base in the ZANU-PF (Noyes, 2020). Despite these shifts, especially the trend toward increased military influence, the classification of multiparty authoritarian fits. Recall that Fjelde (2010: 196–197, 201, 203) notes multiparty authoritarian regimes are at higher risk for internal conflict, lack leverage for co-opting opposition, suffer from exacerbated information problems, and depend on the electorate for legitimacy. They trend toward restraint but can be provoked into violence (Fjelde, 2010: 196–197, 201, 203).

Mnangawa represented a potentially liberalizing force and hope for a country that had suffered for decades under Africa's longest ruling dictator. His ability to co-opt the opposition would be significantly constrained by these expectations. The initial period of political openness exemplifies the expected characteristic of restraint, but as protests grew in size and intensity, as did the information problem, they provoked violent response. The mixture of state and private ownership of ISPs slowed the shutdown execution, but majority state control results in a complete blackout by day two. While internet penetration is low and prohibitively expensive, it is above the threshold to constitute a threat the regime. Like in Eritrea and Mali, the fuel protests represented a *peak* in activity. Zimbabwe's tools of digital repression have expanded vis-à-vis investments from Huawei, ZTE, and Cloudwalk and Chinese media trainings. The Huawei built data center for state owned TelOne could enable Zimbabwe's digital repression strategy to expand, as Huawei has been criticized for intentionally building data centers with outdated and exploitable encryption standards (Moss, 2020). This injection of technology represents how China's interventions can expand the potential options for interventions and influence the regime's surveillance and censorship goals as seen by the model. Further, the deployment of the shutdown to successfully break a growing wave of protest shows how types of interventions can reinforce the regime.

Analysis

There are three broad categories of conclusions: regime type, ISPs and Internet access characteristics, and Chinese telecommunications investment.

Regime type

When using a nuanced typology that accounts for differences in regime types, states can be observed deploying shutdowns for myriad reasons. Hybrid regimes have to manage audience costs from the public that autocracies do not. Liberia, the hybrid regime bordering on semi-consolidated democracy, did not use its shutdown to facilitate violations of physical integrity rights, but rather to control the spread of information. The specific characteristics of the Liberian regime type bolstered its restraint, and liberal interventions weakened the feedback loop identified by the model. However, Mali, sits much closer to authoritarianism. Restraint failed, but IBK paid a significant price after his fourth shutdown. Based on the model, previous successful interventions vis-à-vis shutdowns reinforced the regime's willingness to continue deploying them. China's actions as an intervening

factor strengthened the feedback loop, even if it was ultimately broken by the coup. The authoritarian states, regardless of specific typology, utilize shutdowns to quash dissent and the multiparty authoritarians paired them with brutal, but successful crackdowns reinforcing the feedback loop.

Shutdowns are not one size fits all. Their deployment is in response to differing goals, which signals the utility of the model. Each instance in the model can be specified to understand how the feedback loop plays out. Hence, shutdowns are not used in response to every instance of protest in the same way that it can be expected for security forces to be deployed. They are intentional and appear to be used in times of desperation to ensure goals are achieved. Either periods of repeated protest, such as in Eritrea, Zimbabwe, and Mali, or protests with overwhelming turnout, whether spontaneous as in Ethiopia or publicized as in Liberia, are unnerving regimes and leading them to deploy shutdowns. The caveat is that hybrid regimes require further specialization to better understand their goals. Like democracies and autocracies, hybrid regimes have distinguished and diverging characteristics. They exist on a spectrum. Their maintenance of power and control is not uniform. Mali and Liberia exemplify that spectrum.

Finally, the correlation between regime leader duration in power and shutdown deployment does not appear relevant here. The cases represent a variety of durations in power, with the majority consisting of newer heads of state. Afwerki of Eritrea is the only exception. While it cannot be ruled out entirely without further study, this article is unconvinced about its usefulness as a variable.

ISPs and internet access characteristics

Firstly, ownership of ISPs is an uncompelling explanation alone. Shutdowns are executed more uniformly and faster in the case of states with total or majority ownership, but states with minority or no ownership of ISPs are experiencing similar shutdowns. State ownership is not a prerequisite for deploying a shutdown. However, state ownership might better explain why certain states deploy them more frequently. If executing shutdowns in cases of private ownership is onerous and time consuming, states may have little interest in repeating efforts in the future unless the situation necessitates it. While states with majority or total ownership, especially with centralized control of traffic such as Ethiopia, can achieve their goals quicker, easier, and more effectively, may perceive the strategy as more attractive.

Secondly, internet penetration in Sub-Saharan Africa is low, at 29% on average, in spite of its richer, democratic island neighbors and a few outlier countries with penetration above half (The World Bank 2020). North Africa has a somewhat higher average at 56% (The World Bank 2020). Parsing out comparisons based on penetration level across Sub-Saharan Africa has not been useful here. Accounting for disparities in access, cost, and speeds further complicates this. Eritrea demonstrates that the threshold for penetration to represent a threat is low. Numerous states with low levels of penetration are deploying shutdowns with increasing frequency and duration, which further reinforces that conclusion. States in North Africa, with higher levels of penetration, are deploying them, as well. It is unclear what role the characteristic plays. If it is based on a spectrum, as the literature review suggested, the sample size here may be too small with insignificant differences to reveal the validity of the factor.

Chinese telecommunications investment

Finally, there are the conclusions regarding Chinese telecommunications investment. China is an intervening actor in every case contributing to the feedback loop. However, it is entrenched at different levels across each regime. Norm diffusion is challenging to trace, especially when the content of important vectors, such as Chinese state ICT and media trainings, is unknown. Sustained contact results in technology injections and provides opportunities for norm diffusion regarding management and use of those technologies, nonetheless. Capabilities and capacities are bolstered, leading to an

evolution of goals and expanded types of interventions that often re-entrench the regime, as observed in the model. Each of these regime types have the latent capacity for even if they differ in intensity, rationale, and frequency, but sustained contact with China is occurring *alongside* increased intensity and frequency. Ethiopia represents the literal worst-case scenario. Digital repression has increased and evolved as contact between the states has grown. Zimbabwe is undergoing a similar evolution. Their goals and the interventions they deploy have advanced, which bodes poorly for human rights. Further, it is unclear whether these regimes will abandon primitive intervention at the infrastructure level entirely in exchange or sophisticated alternatives or deploy a mixed strategy.

Liberia's is the foil. It has the least amount of Chinese investment, and a historic relationship with the USA that entails significant American investment in the state. Competition and alternatives produce benefits, which is demonstrated in the model by liberal interventions ability to influence goals and types of interventions. While it does not curtail the usage of shutdowns entirely, it does appear to limit them and their pairing with violent crackdowns. Of course, the ideal is a state that does not violate freedom of expression and access to information, but protections for physical integrity rights have to be paramount.

Recommendations and conclusions

If these regimes only deploy protest related shutdowns in scenarios where the threat is heightened, it explains why current campaigns that emphasize the economic costs and/or name and shame are not proving effective. Regimes that feel existential threat are unlikely to care about costs, economic or reputational. Each time a successful intervention is used, it reinforces the feedback loop in the model, which further degrades the utility of those campaigns. While naming and shaming and economic cost publication should not be abandoned, additional measures should be considered. First, Western states with commitments to human rights and democracy must invest in capacity building, both funding and development of infrastructure and human capital, in Africa. Second, those same Western states should encourage ISP privatization but recognize that separation only slows shutdown execution. Third, the West must support local civil society organizations that have the capacity to pursue legal remedies to shutdowns. These recommendations must be executed with a development approach cognizant of colonial legacies.

This article is distinctly aware that the internet is a powerful vector for the transmission of ideas, but it is not the only factor. While it focuses on the internet, slowing the feedback loop present in the model will not resolve the issue of autocratic and hybrid regime types entirely. This is a discussion of relative effects but a significant contribution, nonetheless. The Internet is a powerful medium for propagating ideas that threaten these regimes, which is why they are deploying shutdowns.

Western funding and engagement

In a Post-Arab Spring world, it is clear that presence of the Internet alone is not a liberalizing force. The institutions and infrastructure that enable it to exist are critical to enabling liberal effects. The increasing level of engagement between African states and China represents a problem that grows exponentially with each day. As firms like Huawei and ZTE outfit the initial elements of the telecommunications sector, states will have little motivation to seek out alternatives. ICT professionals' working knowledge will best apply to pre-existing technology and relationships. Diversifying will require the expanding capabilities through infrastructure and capacity building. In contrast to one-off training, this will require and investment in strategies such as "training for trainers" that invests in not only immediate capabilities and capacities development, but an epistemic infrastructure necessary to sustain that development endogenously.

Multiparty authoritarian states and hybrids, due to more open political space, will be amenable to this approach. Alternatively, in regimes like Eritrea suffering from extreme insecurity, this may be

a nonstarter. The West must be critically aware of the impact that colonial and, to an extent, Cold War legacies have on many of these regime's willingness to engage. Further studies are needed, and they must also account for additional types of autocracy including oligarchy, single-party authoritarian, monarchy, and personalist rule.

ISP privatization

Privatization of ISPs does not prevent the deployment of shutdowns. However, it hinders and decreases effectiveness. Regardless of regime type, Private ISPs must comply with shutdown orders, but their executions vary. In Mali, with total private ownership of ISPs led to inconsistent blocking of social media across providers, and delayed execution. The degree of separation that privatized ISPs have from the state complicates the cost-benefit calculus for their deployment. This makes it worthwhile to encourage continued privatization efforts.

Civil society support

In Zimbabwe, the shutdown was ended by a court ruling (Mare, 2020: 4258–4259). Two local civil society organizations successfully challenged the shutdown order in Zimbabwe's High Court (Mare, 2020: 4258). States with litigious civil society organizations, or organizations that indicate an interest in litigation, could benefit from capacity building and expanded resources. This needs to be prioritized according to regime type. Due to their need for electoral legitimacy, multiparty authoritarian states allow more citizen participation and have respect for rule of law institutions than other authoritarian regime types. Litigation challenges have the potential for success in these environments. Hybrid regimes demonstrate similar characteristics that could produce success. Conversely, military regimes tend to lack independent courts or space for civil society organizations, so this strategy will face opposition there. Further research is required to determine whether the remaining autocratic regime types could benefit.

These recommendations demonstrate liberal states slow the feedback loop in the model. The West cannot sever the relationship between China and states deploying shutdowns, but it can counter them. Hybrid regimes are particularly well suited for liberal interventions. The observed spectrum ranging from more autocratic, Mali, to more democratic, Liberia, demonstrates the potential for intervening factors to bolster capabilities and capacities to encourage states to pursue their goals with either less or more respect for human rights.

The cases illustrate the utility of the model for understanding and comparing medium thickness cases. The model facilitates a better comprehension of how to limit the deleterious effects of autocratic regimes – it is explanatory. To further test and refine the model, future research will expand analysis to a mixed methods strategy using a combination of clustering analysis and case selection. It expects to differentiate where these kinds of interventions have been entrenched, to use the global data to identify additional threshold cases, to engage in developing meaningful indicators, and to identify where these interventions have been deployed by flawed and full democracies. Identification of the threshold cases will enable creation of a hybrid spectrum and refinement of their characteristics with a more explicit understanding of their goals and how third-party technology injections will impact the feedback loop.

Bibliography

Access Now (2020a) *STOP Shutdown Tracker Data*.

Access Now (2020b) Back in the dark: Ethiopia shuts down internet once again. *Freedom of Expression* (https://www.accessnow.org/back-in-the-dark-ethiopia-shuts-down-internet-once-again/).

Africa News (2019) Eritrea blocks social media, reportedly to curb planned protests. *Africanews* (https://www.africanews.com/2019/05/15/eritrea-blocks-internet-reportedly-to-curb-planned-protests/).

Agence France-Presse (2020a) 166 die during protests after shooting of Ethiopian singer. *The Guardian* 4 July (https://www.theguardian.com/world/2020/jul/04/166-dead-following-protests-at-shooting-of-ethiopian-pop-star).

Agence France-Presse (2020b) Who Is Behind Mali's Surging Protest Movement? *Voice of America* (https://www.voanews.com/a/africa_who-behind-malis-surging-protest-movement/6193002.html).

Anckar, Carsten & Cecilia Fredriksson (2019) Classifying political regimes 1800–2016: a typology and a new dataset. *European Political Science* 18(1): 84–96.

Australian Strategic Policy Institute (2021) Mapping China's Tech Giants. *Mapping China's Tech Giants | Australian Strategic Policy Institute* (https://chinatechmap.aspi.org.au/).

Ayana, Ribka (2020) How the Murder of an Ethiopian Singer Triggered an Uprising Against a Disintegrating Democracy. *Time* (https://time.com/5871217/ethiopia-protests-haacaaluu/).

Balancing Act (2006) LIBERIA TELECOMMUNICATIONS CORPORATION SPURNS SUPREME COURT RULING. *Balancing Act Liberia* (https://www.balancingact-africa.com/news/telecoms_en/5980/liberia-telecommunications-corporation-spurns-supreme-court-ruling#_).

Buelgasim, Fay & Samy Magdy (2019) Sudan activists say internet restored after crackdown. *AP NEWS* (https://apnews.com/article/e1541a09119e49d1894e8708c5683988).

CIPESA (2019) *Despots and Disruptions: Five Dimensions of Internet Shutdowns in Africa* (https://cipesa.org/?wpfb_dl=283).

Diallo, Aïssatou (2021) Mali: July protests killed 14, including 2 children - MINUSMA report. *The Africa Report* (https://www.theafricareport.com/57347/mali-minusma-report-details-unlawful-actions-at-july-protests/).

Dodoo, Lennart (2019) Liberia: June 7 'Save the State' Protest Ends in Deadlock, Poised to Continue on Monday. *FrontPageAfrica* (https://frontpageafricaonline.com/amp/news/liberia-june-7-save-the-state-protest-ends-in-deadlock-poised-to-continue-on-monday/).

Ecofin Agency (2015) Mali: Huawei awarded national broadband network contract worth FCfa 34 billion. *Ecofin Agency News* (https://www.ecofinagency.com/telecom/2210-32579-mali-huawei-awarded-national-broadband-network-contract-worth-fcfa-34-billion).

Ekman, Joakim (2009) Political Participation and Regime Stability: A Framework for Analyzing Hybrid Regimes. *International Political Science Review* 30(1): 7–31.

Eritrea Profile (2018) Training on Digitalization of Programs. *Eritrea Profile* 25 July: 2.

Executive Research Associations (2009) *China in Africa: A Strategic Overview* (https://www.ide.go.jp/library/English/Data/Africa_file/Manualreport/pdf/china_all.pdf).

Feldstein, Steven (2019) To end mass protests, Sudan has cut off Internet access nationwide. Here's why. *Washington Post* 13 June

(https://www.washingtonpost.com/politics/2019/06/13/end-mass-protests-sudan-has-cut-off-internet-access-nationwide-heres-why/).
Fjelde, Hanne (2010) Generals, Dictators, and Kings: Authoritarian Regimes and Civil Conflict, 1973—2004. *Conflict Management and Peace Science* 27(3): 195–218.
Fornof, Emily & Emily Cole (2020) Five Things to Know About Mali's Coup. *United States Institute of Peace* (https://www.usip.org/publications/2020/08/five-things-know-about-malis-coup).
Freedom House (2018) Ethiopia: Freedom on the Net 2018 Country Report. *Freedom House* (https://freedomhouse.org/country/ethiopia/freedom-net/2018).
Freedom House (2019) Zimbabwe: Freedom on the Net 2019 Country Report. *Freedom House* (https://freedomhouse.org/country/zimbabwe/freedom-net/2019).
Freedom House (2020a) Ethiopia: Freedom in the World 2020 Country Report. *Freedom House* (https://freedomhouse.org/country/ethiopia/freedom-world/2020).
Freedom House (2020b) Liberia: Freedom in the World 2020 Country Report. *Freedom House* (https://freedomhouse.org/country/liberia/freedom-world/2020).
Freedom House (2020c) Mali: Freedom in the World 2020 Country Report. *Freedom House* (https://freedomhouse.org/country/mali/freedom-world/2020).
Freedom House (2021) Zimbabwe: Freedom on the Net 2021 Country Report. *Freedom House* (https://freedomhouse.org/country/zimbabwe/freedom-net/2021).
Freyburg, Tina & Lisa Garbe (2018) Blocking the Bottleneck: Internet Shutdowns and Ownership at Election Times in Sub-Saharan Africa. *International Journal of Communication* 12: 21.
Freyburg, Tina, Lisa Garbe & Véronique Wavre (2019) Telecommunications Ownership and Control (TOSCO). A new dataset on ownership of internet infrastructure in Africa, 2000-2016. Presented at the GigaNet Annual Symposium. Berlin, Germany: Global Internet Governance Academic Network, 29.
Geddes, Barbara (1999) What Do We Know About Democratization After Twenty Years? *Annual Review of Political Science* 2(1): 115–144.
Geddes, Barbara, Erica Frantz & Joseph G Wright (2014) Military Rule. *Annual Review of Political Science* 17(1): 147–162.
Geddes, Barbara, Joseph Wright & Erica Frantz (2014) Autocratic Breakdown and Regime Transitions: A New Data Set. *Perspectives on Politics* 12(2): 313–331.
Griffiths, James (2021) *The Great Firewall of China: How to Build and Control an Alternative Version of the Internet*. Bloomsbury Publishing.
Hawkins, Amy (2018) Beijing's Big Brother Tech Needs African Faces. *Foreign Policy* (https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/).
Hellmeier, Sebastian (2016) The Dictator's Digital Toolkit: Explaining Variation in Internet Filtering in Authoritarian Regimes. *Politics & Policy* 44(6): 1158–1191.
Howard, Philip N, Sheetal D Agarwal & Muzammil M Hussain (2011) When Do States Disconnect Their Digital Networks? Regime Responses to the Political Uses of Social Media. *The Communication Review* 14(3): 216–232.
Huawei (2018) President of Mali: Mali needs the support of Huawei to develop its digital economy. *Huawei* (https://www.huawei.com/cn/news/2018/8/mali-president-visit-huawei-2018).
Human Rights Council (2016) The Promotion, Protection, and Enjoyment of Human Rights on the Internet. United Nations (https://primarysources.brillonline.com/browse/human-

rights-documents-online/promotion-and-protection-of-all-human-rights-civil-political-economic-social-and-cultural-rights-including-the-right-to-development;hrdhrd99702016149).
Hussain, Muzammil M & Philip N Howard (2012) Opening Closed Regimes: What Was the Role of Social Media during the Arab Spring. In: Eva Anduiza, Michael James Jensen & Laia Jorba (eds) *Digital Media and Political Engagement Worldwide*. Presented at the Project on Information Technology and Political Islam. Cambridge: Cambridge University Press, 200–220 (https://www.cambridge.org/core/product/identifier/CBO9781139108881A020/type/book_part).
Idindili, Mercy (2019) A Movement from Within: Zimbabwe's Fuel Protests. *The Yale Globalist* (https://globalist.yale.edu/2018-2019-issues-2/a-movement-from-within-zimbabwes-fuel-protests/).
International Telecommunications Union (2021) Digital Development Dashboard: Mali. *ITU* (https://www.itu.int:443/en/ITU-D/Statistics/Dashboards/Pages/Digital-Development.aspx).
International Trade Administration (2021) Liberia - Country Commercial Guide (https://www.trade.gov/country-commercial-guides/liberia-telecommunication).
Kansara, Reha (2019) Eritrean Press: Reporting on Africa's most secretive state. *BBC News* 27 February (https://www.bbc.com/news/blogs-trending-47319021).
Katlic, Tim (2014) Understanding Eritrea's Exceptionally Limited Internet Access. *ICT Works* (https://www.ictworks.org/understanding-eritreas-exceptionally-limited-internet-access/#.YaVjAtDMLb0).
Kazunga, Oliver (2014) Chinese bank to disburse first batch of $218,9m loan to NetOne. *The Chronicle* (https://www.chronicle.co.zw/chinese-bank-to-disburse-first-batch-of-2189m-loan-to-netone/).
Kazunga, Oliver (2015) China extends $500 mln loan to Econet. *The Chronicle* (https://www.chronicle.co.zw/china-extends-500-mln-loan-to-econet/).
Keremoğlu, Eda & Nils B Weidmann (2020) How Dictators Control the Internet: A Review Essay. *Comparative Political Studies* 53(10–11): 1690–1703.
MacKinnon, Rebecca (2011) China's 'Networked Authoritarianism'. *Journal of Democracy* 22(2): 32–46.
Mare, Admire (2020) State-Ordered Internet Shutdowns and Digital Authoritarianism in Zimbabwe. *International Journal of Communication* 14: 4244–4263.
Mekonnen, Siyanne & Bileh Jelan (2021) News Analysis: 123 people killed in June-July unrest, 76 by security forces; attacks constitute elements of crime against humanity: Ethiopia Rights Commission. *Addis Standard* (January) (https://addisstandard.com/news-analysis-123-people-killed-in-june-july-unrest-76-by-security-forces-attacks-constitute-elements-of-crime-against-humanity-ethiopia-rights-commission/).
Mengonfia, Mark Neywon (2020) The day Liberia shut down freedom of expression amid a mass protest. *Global Voices Advox* (https://advox.globalvoices.org/2020/07/31/the-day-liberia-shut-down-freedom-of-expression-amid-a-mass-protest/).
Moss, Sebastian (2020) Australia: Huawei's Papua New Guinea data center security 'openly broken,' making potential spying easy. *Data Center Dynamics* (https://www.datacenterdynamics.com/en/news/australia-huaweis-papua-new-guinea-data-center-security-openly-broken-making-potential-spying-easy/).

Mou, Yi, Kevin Wu & David Atkin (2016) Understanding the use of circumvention tools to bypass online censorship. *New Media & Society* 18(5): 837–856.
NetBlocks (2019) Zimbabwe Internet shutdowns amid fuel price protests. *NetBlocks* (https://netblocks.org/reports/zimbabwe-internet-shutdowns-amid-fuel-price-protests-OxAGDdBz).
NetBlocks (2020a) Internet cut in Ethiopia amid unrest following killing of singer. *NetBlocks* (https://netblocks.org/reports/internet-cut-in-ethiopia-amid-unrest-following-killing-of-singer-pA25Z28b).
NetBlocks (2020b) Social media restricted in Mali amid protests against president. *NetBlocks* (https://netblocks.org/reports/social-media-restricted-in-mali-amid-protests-against-president-QyKpdX8D).
Noyes, Alexander (2020) 'New Zimbabwe' Looks an Awful Lot Like the Old One (https://www.rand.org/blog/2020/03/new-zimbabwe-looks-an-awful-lot-like-the-old-one.html).
O'Carroll, Tanya (2016) *Ethiopia Offline: Evidence of Social Media Blocking and Internet Censorship in Ethiopia*. London: Amnest International, 33.
Reuters (2020) US Adds 33 Chinese Companies, Institutions to Economic Blacklist. *VOA* 22 May (https://www.voanews.com/a/usa_us-adds-33-chinese-companies-institutions-economic-blacklist/6189770.html).
Rydzak, Jan (2016) *The Digital Dilemma in War and Peace: The Determinants of Digital Network Shutdown in Non-Democracies*.
Sanovich, Sergey (2017) Computational Propaganda in Russia: The Origins of Digital Misinformation. Vol. Working Paper 2017.3. Presented at the Project on Computational Propoganda. Oxford.
Sanovich, Sergey, Denis Stukal & Joshua A Tucker (2018) Turning the Virtual Tables: Government Strategies for Addressing Online Opposition with an Application to Russia. *Comparative Politics* 50(3): 435–482.
Sarpong, Eleanor (2020) The Internet is unaffordable in Liberia: action is needed to 'SET' the agenda for positive change. *Alliance for Affordable Internet* (https://a4ai.org/the-internet-is-unaffordable-in-liberia-action-is-needed-to-set-the-agenda-for-positive-change/).
Shahbaz, Adrian (2018) *Freedom on the Net: The Rise of Digital Authoritarianism*. Freedom House (https://freedomhouse.org/sites/default/files/FOTN_2018_Final.pdf).
Shen, Fei (2014) Great Firewall of China. In: *Encyclopedia of Social Media and Politicss*. SAGE, 599–602.
Sieh, Rodney (2019) Liberia: The Ghost of April 14, 1979 Laid to Rest With Non-Violent Save-the-State Protest. *FrontPageAfrica* (https://frontpageafricaonline.com/news/liberia-the-ghost-of-april-14-1979-laid-to-rest-with-non-violent-save-the-state-protest/).
Smart Cities World Forums (2017) Ethiopian PM looks to deepen cooperation with Huawei in driving ICT growth. *Smart Cities World Forums* (https://www.smartcitiesworldforums.com/news/smart-cities-africa/finance-and-policy-af/301-ethiopian-pm-looks-to-deepen-cooperation-with-huawei-in-driving-ict-growth).
Stepanova, Ekaterina (2011) *The Role of Information Communication Technologies in the "Arab Spring"*. 6 (http://www.gwu.edu/~ieresgwu/assets/docs/ponars/pepm_159.pdf).
Taye, Berhan (2019) Zimbabwe orders a three-day, country-wide internet shutdown. *Freedom of Expression* (https://www.accessnow.org/zimbabwe-orders-a-three-day-country-wide-internet-shutdown/).

Taye, Berhan (2020) *Targeted, Cutoff, and Left in the Dark: The #KeepItOn Report on Internet Shutdowns in 2019*. New York: Access Now (https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf).
The World Bank (2020) Individuals using the Internet (% of population). *World Bank Open Data* (https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=ML-ZW-ER-ET-LR).
Wahman, Michael, Jan Teorell & Axel Hadenius (2013) Authoritarian regime types revisited: updated data in comparative perspective. *Contemporary Politics* 19(1): 19–34.
Ward, Alex (2020) How terrorism, corruption, and suspect elections led to Mali's coup. *Vox* (https://www.vox.com/2020/8/19/21375138/mali-coup-president-keita-military-election).
Winter, Caroline (2014) Eritrea: World's Least Connected Country, Tech-Wise - Bloomberg (https://www.bloomberg.com/news/articles/2014-06-26/eritrea-worlds-least-connected-country-tech-wise).
Woodhams, Samuel & Simon Migliano (2021) The Global Cost of Internet Shutdowns. *Top 10 VPN* (https://www.top10vpn.com/cost-of-internet-shutdowns/2019/).
Wu, Annie (2018) Court Records Reveal ZTE's Corruption Scheme in Liberia. *Epoch Times* (https://www.theepochtimes.com/court-records-reveal-ztes-corruption-scheme-in-liberia_2547702.html).
Xinhua News (2006) Huawei Signs Deal with Malian Telecoms Firm. *China Org* (http://www.china.org.cn/english/BAT/155282.htm).
Xinhua News (2017) Zimbabwe's state-owned telecoms firm launches Chinese-funded world class data center (http://www.xinhuanet.com//english/2017-03/25/c_136157465.htm).
Xinhua News (2019) 66 Eritrean media professionals complete Chinese media course program. *Https://Newsghana.Com.Gh/* (https://newsghana.com.gh/66-eritrean-media-professionals-complete-chinese-media-course-program/).
Xinhua News (2021) Zimbabwe partners with Huawei in major network upgrade. *XinhuaNet* (http://www.news.cn/english/2021-09/21/c_1310200916.htm).
Zere, Abraham T (2017) How a rare protest scared the Eritrean regime. *Al Jazeera* (https://www.aljazeera.com/opinions/2017/11/10/how-a-rare-protest-scared-the-eritrean-regime).
Zittrain, Jonathan L, Robert Faris, Helmi Noman, Justin Clark, Casey Tilton & Ryan Morrison-Westphal (2017) *The Shifting Landscape of Global Internet Censorship*. SSRN Scholarly Paper ID 2993485. Rochester, NY: Social Science Research Network (https://papers.ssrn.com/abstract=2993485).
ZTE Press Center (2019) ZTE and Ethio Telecom launch a joint innovation center in Ethiopia. *TelecomTV* (https://www.telecomtv.com/content/mobile/zte-and-ethio-telecom-launch-a-joint-innovation-center-in-ethiopia-34440/).