Internet Shutdowns During Protests: A Practice in Digital Authoritarianism.

August 2020

UoG: 2409241J

DCU: 18114687

CU: 74900848

Nishant Joshi

Presented in partial fulfilment of the requirements for the Degree of

International Master's in Security, Intelligence and Strategic Studies

Word Count: 22,035 words

Supervisor: Dr. Jivanta Schöttli

Date of Submission: August 3rd, 2020

List of Content

Acknowledgements

This dissertation id dedicated to every individual who has been through hardships during the Covid-19 Pandemic. The strength and resilience required to survive a catastrophe builds the measure of a person.

I thank the IMSISS program coordinators, Dr. Eamonn Butler, Dr. James Fitzgerald and Dr. Vitek Strickey for their invaluable support and guidance through my education. I would not have managed to finish my studies without their compassion and understanding.

To my friend, Javier Martinez, Clara Ribeiro, Marijn Pronk and Dominique Linares who were rays of hope for me in times of darkness.

To Dr. Jivanta Schottli, without whose support, I would not have been able to undertake this research. Her support, kindness and understanding gave me strength to pull through.

Lastly, I thank my family who never gave up on me.

Abstract

The tendency for democratic and authoritarian governments to enact internet shutdowns has grown to massive proportions over the past decade, owing to the capacity of social media and digital platforms to mobilize masses. The emancipatory potential possessed by information technology gets challenged by regimes seeking to preserve their legitimacy and retain power. The impacts that authoritarian measures have on digital governance in the past years have become manifold and continue to pose a threat to human rights. This research argues that internet shutdowns are inherently authoritarian practices aimed at repressing freedom of expression in protesting atmospheres. Using Practice Theory and the framework of Digital Authoritarianism, this dissertation shows the tendency for states to stifle voices of dissent and quash opposition. This dissertation will showcase how authoritarian systems tend to exploit power in order to exploit digital spaces to serve the regime and how the citizen machinery overcome the dis-connective actions imposed by repressive regimes.

Introduction

Digital rights and free expression over the internet are being vociferously contested by activist organizations over the world since the past decade. A growing number of democratic and autocratic regimes employing tactics of censorship and digital blackouts have caused concerns about the translation of individual rights over the online sphere as they are in the offline world. As a safeguard against authoritarian practices of controlling information technology, a group of 70 states signed the Declaration of Human Rights and International Covenant on Civil and Political rights on the 1st of July 2014 (Records of the General Council, 2013). The declaration, which promises to safeguard the rights of online citizens was passed as in the UN, deeming several digital governance practices such as mass surveillance, and tracking of personal data disproportionate to democratic governance. Amongst the list of practices which constituted digital repression, Internet shutdowns were contested as one of the grossest violations of freedom of expression and human rights.

Access to the internet has been growing exponentially across the developing world, where economic activity, social relations and availability of educational information is encouraging governments to look towards the emancipatory potentials of a connected infrastructure. The limits of physical space can be overcome through technological incorporation into practices of governance, communication, and economic activity, which would be beneficial to the overall development of nation states. The contestation on rights of individuals regarding access to the internet, however, gives rise to the question of maintaining authority over an informed civilian population. Repressive governments feel the need to control certain aspects of connectivity to the internet, especially when the legitimacy of rule is put to question or when tendency for mobilization to turn violent looms as a threat to law and order.

In the years since the Arab spring, the practice of shutting down the internet during protests and mass movements has been only growing, with more and more countries, regardless of their liberal democratic status are adopting measures to sever lines of communication (Rydzak, Karanja and Opiyo, 2020). The Egyptian revolution of 2011 marks one of the first recorded acts of government mandated internet shutdowns, which disconnected the population of an entire nation from the rest of the world (Rød and Weidmann, 2015). Although this should have been seen as a cautionary tale of authoritarian capabilities, more and more regimes started to adopt the Egyptian model of disconnection in the years to come. The act of throttling or disconnecting a group of people from the rest of the world in a globalized society should be seen as a worrying sign, considering that democratic governance in the offline world is taking precedence but practices of digital authoritarianism are becoming the norm (Erixon, Fredrik; Lee-Makiyama, 2011).

The following sections in this dissertation explain theoretical dimensions of blanketed disconnections or what are commonly referred to as kill-switch shutdowns (Freyburg and Garbe). Literature on how authoritarian regimes use infrastructural control over channels of communication to their advantage is reviewed in the following section of this project. With the help of social science theories and digital action theories including Practice theory (Rydzak, 2019), Liberation Technology (Diamond, 2015), Connective Action (Bennet and Segerberg, 2013) and Digital Authoritarianism (Marchant and Stremlau, 2020a), this research elaborates on how regimes systemically censor spaces for free speech to stifle dissent and retain power. In the presence of control mechanisms and centralized points of authority, the concentration of authoritative power becomes inevitable, leading to repressive regimes taking steps to limit expressions of discontentment. The tendency for technology to take the form of either a tool for emancipation or repression is explained in the following sections using theories of Liberation Technology (Diamond, 2010) and Repression Technology (Rød and Weidmann, 2015).

The internet is not owned by government, yet governments can manage content available within their own jurisdiction. The possibility of the internet to be turned into a tool for repression is not lost on authoritarian regimes and often utilized to bend to their specific. This research explains how internet access within a country can be monopolized in favour of governments looking to gain control over the media and dissemination of information. Regimes that try to control access to information usually do so by limiting competitive markets consisting of service providers and exchange points (Leon, 2020). Successful control over the internet infrastructure in any regime can be achieved when the state becomes the sole owner or a majority stakeholder in the internet infrastructure. Having operational capabilities over physical infrastructure empowers regimes to initialize authority in the digital domain in a similar manner to offline governance (Mare, 20200).

This research presents selected cases of governments known for practicing blanketed internet shutdowns on several occasions, resorting to measures of extreme control. The primary care study in this research is that of India, which has had an undisputed history of imposing internet shutdowns more than any other county in the world (Mawii et al., 2018). The following sections will explore how archaic legal structures and access of authority in a corrupt system of governance has led to the Indian state become increasingly authoritarian in the recent decade (Glasius, 2018). The decentralization of authority within several levels of governance leaves room for the federal government as well as authorities governing constituencies to enact blanketed shutdowns at their own discretion. The dynamics of frequencies with which shutdowns are imposed in India are explained in the sections relating to the legality and legitimacy of the online ecosystem in the subcontinent.

Further empirical analysis of shutdown practices as retaliatory measures against protests shows the propensity for governments to disregard impacts and consequences when considering disconnections. The analysis of cases from the past two years, including internet shutdowns enacted during three major protests involving hundreds of thousands of dissidents shows how internet shutdowns have been resorted to as means of stifling free at every presented opportunity. The case of India engaging in digitally repressive practices despite being a democratic state shows how digital repression does depend on the profile of the regime but rather on the availability of controlling mechanisms to enact authoritarianism. This research further shines light on the urgency of interventions into digital governance at the national scale, considering that every country profile covered in this dissertation has had government disagree on the necessity of human rights extending to incorporate digital freedoms within their regimental framework.

The possibility for dissidents to mobilizations has become much easier to emulate, owing to growth in social media communications and messaging platforms. The possibility of online communication channels to mobilize individuals into a group within short timeframes is the online equivalent of connective action (Bennet and Segerberg, 2013). While governments can choose to block and monitor certain content within their online jurisdictions, is becoming easier to bypass internet blockades and hide personal identities due to advancement in peer-to-peer communication strategies. Shutting down the internet, however, extinguishes any scope for communication to occur and takes away opportunitis for dissent to be expressed (Rydzak, 2019). By disconnecting populations from the internet, governments can ensure that no communication comes in or gets out, leaving plenty of room for repressive practices to take place, which could escalate to mortal atrocities (MacKinnon, 2011).

The theories explaining government ordered internet shutdowns help in understanding cases of regimes which continue the practice and of those which move towards a more inclusive online space through participatory discourse. Ethiopia, which in 2020 underwent lengthy internet shutdowns despite the Covid-19 pandemic affecting economic and social life of its citizens presents the stark reality of authoritarian practices in the modern world, where the legitimacy of regimes can outweigh basic needs of citizens (Freyburg and Garbe, 2018). Even after a regime change following public outcry and promises of emancipation, the Ethiopian leadership reverted to old ways of practicing digital control over its population within months of being instated. The Ethiopian context is shown in this research as an example of how regime changes do not solve repressive measures form being normalized and that practices need to be understood as the underlying forces enabling regimes to enact authoritative actions (Rydzak, 2019).

The case of Zimbabwe is presented as an example of how repressive governments can be challenged on their authoritarian policies through collective action. The fact that the Zimbabwean state turned towards striving for sustained online freedoms despite having lived under authoritarian rule for three decades speaks of how digital freedoms can be preserved even after repressive attempts (Warf, 2011). the structure of governance in the country is taking a turn towards ensuring digital rights of citizens owing to participation of dissidents, civil society organization and legal representations mandating the rights of the people (Sherman, 2020). A historical comparison between Zimbabwe and Ethiopia can be made n the context of how both the countries have suffered under authoritarianism and economic turmoil, yet one gets to experience positive changes in digital governance and the other faces increased control in the coming years.

The process of this research has been divided into five sections expanding on the mechanism of internet shutdowns from their ideation to implementation.

The first section explores the various theoretical dynamics of digital governance. To understand Internet shutdowns in the context of government control, this research provides a definition of internet shutdowns, which in common literature are identified as kill-switch shutdowns. The framework of infrastructure within nations and the relationships between various actors involved in the internet ecosystem is explained to elucidate chains of authority with respect to governing digital communications. Theories and practices of internet shutdowns are contextualized in this section with the help of popular literature and scholarly research conducted by industry experts, who explain aspects of convergence between technology and governance. The collection of theories presented in this research help in formulating a structure for understanding why regimes choose to disconnect their populations from the communication infrastructure to provide solutions for the future of freedom of access to the internet.

The next section elaborates on the process of shutting down channels of communications and states' perspectives on shutdowns. This section delves into justification and proportionality of internet shutdowns, elucidating concerns for security and preservation of state, which governments often cite to legitimize shutdown measures. This section explores the relationship between shutdowns, protests, and the likelihood of violent action to take place in the presence of internet shutdowns. This section sets the benchmark for the analysis of specific country profiles chosen for this research and also helps build a structure for future research in the field of connective action in authoritarian contexts.

An analysis of India in the context of protests and laws concerning digital governance in the next section sets the arena for studying the country as a unique case of digital authoritarianism. Elucidating the legal provisions provided in the constitution of India for initiating network disruptions builds an understanding on how digital freedoms are seen in the country and how normalized lack of access to basic digital infrastructures remains an issue in the country. The country's protest history shows the tendency for collective action to take root in the subcontinent and how an unfiltered digital sphere will result in higher proportions of active participation, translating into magnification of dissent through connective action.

Finally, Analysis of data obtained from international bodies, activist organizations and public databases builds evidence towards the correlation between authoritarian shutdown practices and protests to occur in tandem. Using India as a case study, this research shows that concerns for security are not necessarily the underlying factors resulting in internet shutdowns to be initiated, instead, environments of dissent, which could bring attention to government atrocities are more in line with reasons for shutdowns. The final analysis also illustrates two country cases, namely, Ethiopia and Zimbabwe, which have followed very different evolutionary trajectories in internet shutdown practices within the past decade. Since both the countries have similar governance profiles, considering the authoritarian regimes that both the countries have been governed by, comparing shutdown practices between the two cases illustrates how collective action against repressive authorities can bring about change in governance and challenge the legitimacy of regimes.

I

Review of Literature

1.1. Defining internet shutdowns

To begin discourses on government ordered internet shutdown, a conceptual framework for what internet shutdowns mean is necessary. Academicians and activists commonly use words like “Kill-switch” (Freyburg and Garbe, 2018; Rydzak, Karanja and Opiyo, 2020; Sutterlin, 2020), “just-in-time” blocking during protests (Warf, 2011) and “Network Shutdowns” (Wagner, 2018) to describe government ordered internet shutdowns. The valley of discourse on what qualifies as an internet shutdown, arguably occupies a widened territory. Yet, scholars agree on the principal outcome of internet shutdowns, which is the complete inability to connect to the internet. Generally speaking, an Internet shutdown is any attempt at stopping all internet activity for a group at a particular point in time, resulting in inaccessibility of online information by the end user (The Economist, 2013; Johnson, 2011). It could pertain to a large or small demographic and for an extended or short period of time.

Access now, an organisation working for keep the internet accessible to global geographies, interprets internet shutdowns as intentional interruption of digital or electronic telecommunications, making them completely ineffectual for a targeted populace or a location, often to exercise control over the movement of information (Taye and Access now, 2019). Since the internet is a transnational infrastructure with billions of access points across the globe and connections between service providers, governments, organisational authorities, and end users, it is hard to develop one definition of shutdowns or lay absolute accountability on one stakeholder regarding the practice of communication disruptions. This inability to find one single definition of internet shutdown limits targeted research opportunities on what could be considered authoritarian network throttling and what could be passed off as legitimate censorship. However, the lack of a standardised definitions leaves room for much necessary exploration and evolution on conceptual frameworks for kill-switch shutdowns (Glasius and Michaelsen, 2018). This research will use popular definitions in academic and humanitarian discourses to answer the research problem of the fundamental necessity of practicing internet shutdowns during mass movements such as protests.

The contrasting mechanisms of shutdown contest a broad area for discourse which needs to be studied as a spectrum rather than an absolute. Marchant and Stremlau, in their special issue on the spectrum of internet shutdowns or "Kill-switch", suggested that definitions provided by leading internet freedom advocacies should considered primarily sources when it comes to defining internet shutdowns (2020b). Previously mentioned definition by Access Now clearly defines internet shutdowns as orchestrations mandated by governments and overseeing bodies (Taye, 2021). Even though this is a narrower definition, which leaves out the scope of accidental shutdowns and network blocking dramatically, it does successfully focus the debate on legitimacy of deliberate authoritarian shutdowns around the globe. Software Freedom Law Centre defines Kill-switch shutdowns in a similar scope but also refer to the regimes in power as primary perpetrators to causing shutdowns, given their access to control over implementing shutdown measures (Software freedom law centre, 2019). Holding governments accountable for their actions of switching off the internet under any circumstances opens the door for discussion of legitimacy and citizens' rights. Not only freedom of expression, but also lives and livelihoods depend on the internet (Marchant and Stremlau, 2020a). These definitions developed by activist organisations at least provide helpful signs regarding identifying the practice of kill-switch shutdowns whenever they occur.

1.2. Internet Shutdowns and Government Control

This research develops discourse on authoritarian control over the access to the internet and the accountability of governments to implement shutdowns which influence outreach and organisational capabilities of protests. Since the discourse becomes even more expansive when the mechanisms and actors of an internet shutdown are accounted for, the scope of shutdowns mandated by governments will be accounted while omitting accidental shutdowns and possible sabotage. Loss of connectivity for a particular location could surely be a result of government ordered shutdowns (Mare, 2020) but severed underwater fibreoptic cables (Gerbaudo, 2013; Glasius and Michaelsen, 2018) would yield the same end result. Even damage to critical infrastructure on the end of service providers (Brooks and Johnston, 2017) could cause a network blackout but that would not constitute an authoritarian practice. To understand why governments shut down the internet during Instances of civil disobedience, protests and mass mobilisation, this dissertation will study deliberate acts of kill-switch shutdowns.

Internet outages in all cases would results in a loss of *en masse* channels of communication but incorporating accidental anomalies into the spectrum of intentional shutdowns will throw off the classifications established in academic studies. However, there is a gap in the definition of intentional internet shutdowns which needs to be addressed. Potentially, intentional infrastructural sabotage could be masked as an accident, leaving the door shut on inquiry against regimes. A good example of accidental damage under suspicious circumstances would be of the 2018 elections in Sierra Leone.

In April 2018, Sierra Leone suffered an internet blackout just after the general elections, resulting in the inability for the electoral commission to count runoff votes (Sutterlin, 2019). The National Telecommunications authority of Sierra Leone later issued a statement narrating severe damage to undersea cables, denying any responsibility for the occurrence, and implying that the upkeep of fibreoptic cables were under the authority of Sierra Leone Cable Company (SLAB) (Ogundeji, 2018). In such cases, intentionality cannot be clearly established due to a lack of credible evidence. Ambiguous reasons citing protection of state and national security used by governments to legitimise shutdowns, however, would be counted as intentional measures. In East Africa, the practice of shutting down the internet during times of elections and state examinations are common (Freyburg and Garbe, 2018). The argument for implementing such measures is to discourage illegitimate activity, which could threaten the democratic process. Amongst the statements cited by governments while implementing such measures, preventing the propagation of fake news, hate speech, violence and cheating are common narratives used by authorities (Ayalew, 2019; Mare, 2020; Micek and Access Now, 2017). In 2018, after a routine internet shutdown during the national elections, the Congolese Minister of Communications, Omalanga went so far as to remark that denouncing comforts of connectivity for a short period of time was a small price to pay for maintaining the security and integrity of the nation's democracy. (La République, 2019**).**

2. Theorising Internet Shutdowns as Authoritarian Practices

2.1. Practice Theory

Accidental internet blackouts differ form a practice approach to internet shutdowns. Accidental shutdowns could be a result of power cuts or severed infrastructure, which can normally be remedied through corrective measures. Although such instances pose a cost burden to economies and daily lives of individuals, they could be reflected as unintentional happenstances (West, 2016). A practiced approach to internet shutdown, on the other hand, is intentional disruption of services, which is deliberated upon and ordered by authorities in power. Practices are actions which are patterned within particular organisational contexts (Glasius and Michaelsen, 2018; Adler & Pouliot, 2011). A practice is strategic. It is an intentional act, which is set in place for the purpose of resolving contingencies using structured methods. Theodore Schatzki argues that practice approach could be used to analyse communities, governments, militaries, and corporations and implement strategies that facilitate means to an end (2001). Tactics of coercion and domination are not beyond the approach but come within the spectrum of phenomenon instituted and embodied by methods of practice. Practices can be used as benchmarks to gauge units of analyses on how things work in an organisational structure. Studying a practice can help in identifying elements of inquiry against patterns of action employed within organised settings (Bueger and Gadinger, 2015). It should be noted that studying practices is important when looking beyond regime and state machineries to incorporate wider inclusions of foreign and domestic actors which are external to the regime's organisational structure.

The modern world, connected through the internet infrastructure allows for policies to be made and implemented through transnational or private/ public cooperation and not only by government institutions for internal and external policy (Glasius and Michaelsen, 2018). Being aware of practices within organisations, whether by governments or international bodies, this research avoids making mistakes of focusing on the more spectacular, one off occurrences that catch the eye whilst ignoring routine contemporary practices (Bigo and Tsoukala, 2008). By adapting to view internet shutdowns as a practice instead of simply a measure, authorities which implement those measures can be questioned on the intentionality behind them. Practices are tradition. By questioning practices, traditions can be sustained, improved upon, or contested. By examining internet shutdowns as they are practiced during movements of protest, this research would demonstrate both phenomena as co-dependent variables observing changes in levels of violence during protests and the tendency for shutdowns to happen. This would develop a case on the legitimacy of shutdowns from the point of view of governments enacting them, citing security concerns.

2.2. Digital Authoritarianism

Government ordered internet shutdowns that are enacted as emergency measures can be argued as necessary contingency measures. One off actions as response to national security threats, which could potentially endanger the lives of citizens and critically compromise digital infrastructure (Marchant and Stremlau, 2020a) could be considered valid reason for throttling the flow of information if the security fabric is under threat. In Sri Lanka, after 250 people were left dead in late 2018, following a suicide bomb explosion, the government expediently blocked access to several social media outlets including Facebook, Instagram, WhatsApp, and YouTube (Wakefield, 2019). This was done to prevent public panic and propagation of incendiary narratives, which could be further detrimental to national security. The move, although halted free expression in the country, was heralded with positive commentary by media outlets including *The New York Times* (Swisher, 2019) and *The Guardian* (Wong and Paul, 2019). Although such moves as “measures” are arguably seen as necessary, continuous blocking of communications as a “practice” can be exploited as authoritarian tools in the hands of state regimes intending to suppress dissenting movements. This is true for several national security acts passed in regions experiencing conflict between the public and government (Sherman, 2020; Access Now, 2020a).

Deliberate censorships are known to often be invoked by regimes under the vague guise of protecting national security, handling social stability (Warf, 2011), and combating “Cyberanarchy” (Goldsmith 1998; Katyal, 2001**)**. The narrative here looks at the viral nature of the internet where certain elements in harmful information could be detrimental to the communication of truth. Governments in power would argue that allowing free flow of information in conflicting environments could feed into the propagation of false narratives and further promote harmful disinformation campaigns (De Gregorio and Stremlau, 2020). Democratic and authoritarian regimes are both faced with the dilemma of either allowing digital freedoms which enable national progress and involvement in the global information market, or limiting digital freedoms to try and quash internal dissent to preserve said regime’s power (Grinberg, 2017).

In 2020 alone, more than 450 instances of internet shutdowns were confirmed by Access Now across a database of close to 50 countries **(**Access Now, 2020b; Rydzak, Karanja and Opiyo, 2020) and instances of authoritarianism in the digital space only appear to be growing, with more and more liberal and illiberal regimes practicing such measures. Researchers and overwatching bodies use the terms digital authoritarianism (Erixon, Fredrik; Lee-Makiyama, 2011) and digital repression (Gohdes, 2020) to debate acts of network shutdowns ordered by governments worldwide. Both liberal and illiberal regimes of authoritarian and democratic regimes are capable of practicing internet shutdowns depending on the pertinent laws of the land. During the Extinction Rebellion protest in April 2019, the London Transport authority was ordered to shut down the internet in the city's subway stations to inhibit movements of protesters and their ability to mobilise (Hills, 2019). Even though this did not have much effect on the ability for citizens to connect to the internet through other networks, it stands as an example of liberal democracies practicing a mass censorship measure to stop protests. Despite the failure on the part of the effect of the measure, the action itself was authoritarian in nature.

Internet shutdowns qualify for two of the three prerequisites stipulated by Glasius and Michaelsen's conception of illiberal and authoritarian practices: violation of freedoms of expression, and secrecy and disinformation (2018). The complexity of an authoritarian practice in the realm of governance is obscure and often corresponds to illiberal practices. The definitional gaps in conceptualizing authoritarianism cannot be ignored due to the changing nature of what could be considered authoritarian in different paradigmatic times and locations (Kedzie, 1997). Sociological and technical approaches addressing control and power over information communication are more focused on what happens in applications of technological repression instead of the socio-political implications of such practices (Marquis-Boire, Marczak, Guarnieri, and Scott-Railton, 2013). Literature on authoritarianism also falls short of transcending distinctions between authoritarian and democratic regimes, owing to the empirical focus being overwhelmingly swayed towards liberal and formally democratic nations (Glasius and Michaelsen, 2018).

2.3. Liberation Technology vs Repression Technology

Digitization has been a great liberator since the industrial revolution. Every new artifact of technology has posited a connective aspect in human evolution, bringing emancipatory potential along with it. According to proponents of liberation technology theory, the internet affords populations two properties: firstly, complexifying control over broadcasting mechanisms in comparison with traditional media. Secondly, and more notably, introducing fast and more active 'peer-to-peer' communication channels, facilitating mobilization of oppositional forces (Rød and Weidmann, 2015). Larrry Diamond posits the term 'liberation technology' as 'any form of information and communication technology (ICT) wielding power to inflate social, political, and economic liberties' (2010). Contextualisation of liberation technology in the realm of citizen's movements is necessary to encapsulate the internet's capacity to mobilize against authoritarianism. It makes sense for a repressive regime to limit liberation technologies if regimental control is threatened. This research uses the liberation technology argument to show that the internet is vital when it comes to connective action. Governments are aware of this fact and the role of the internet in amplifying voices of discontent against regimes and potentially mobilizing rallies by opposition forces, making repressive governments most likely to regulate connectivity to the internet (Rød and Weidmann, 2015).

While 'liberation technology' is expected to be a harbinger of democratic empowerment; 'repression technology' proposes the tendency for innovation to serve and strengthen authoritarian rule (Rød and Weidmann, 2015). Proponents of the 'repression technology' argument posit that the internet empowers governments with even more control, given the access to surveillance and censorship methods. Scholars contend that the internet is not free form interference by governments, much like traditional media channels (Boas, 2006). Throughout the history of mass communication technologies, censorship and restriction of content have been routinely operationalised, freedom of ICT should not be mistaken as much different in that respect. Anita Ghodes, in her findings on Syrian authoritarian internet control posits that higher levels of information accessibility is linked to substantive increase in proportion and scales of targeted repression, whereas areas with little to no information access are received with more indiscriminate campaigns of violence (Gohdes, 2020). Which is to say that even though access to communication over the internet is a preventative measure against mortal atrocities, accessibility to online communication posits a threat to authoritarian regime. In the case of oppressive states which lean towards violence, the benefits of abstaining from practicing repressive measures on the internet remain largely understudied areas (MacKinnon, 2011).

If the Internet has the potential to be used as a instrument for solidifying autocratic survival by moulding public opinion as well as targeting dissidents, then the more repressive regimes would be most likely to provide online connections (Rød and Weidmann, 2015). Since investing in repression technology helps solidify control for authoritarian governments and play a major role in influencing public opinion, many autocracies opt for it. In fact, the tools for repression technology are largely inexpensive and accessible to most governments who demand them (Gohdes, 2020). Saudi Arabia, for example, defies the liberation technology argument as observed by the overwhelming presence of government surveillance and dissemination of values which coincide with the government's authority (Rød and Weidmann, 2015). Technological developments and evolution of the legal framework in this case tends to utilize Peer-to-peer mechanisms of communications and promote internet filtering to identify individuals through digital footprints when they go against the legal framework stipulated by the government (OpenNet Initiative, 2019). Tunisia was arguably the first Arab country to employ repression technology over the internet and heavily invested in infrastructure for control over its cyberspace, fashioning one of the worlds most sophisticated multi-layered censorship apparatus" (Maher and York, 2016). Theoretical arguments in line with repression technology show that affording political and social elites access to the internet in such regimes proves to be a beneficially calculated choice since it aims at greater control over the public sphere (Rød and Weidmann, 2015).

Rydzak categorizes the practice of Internet shutdowns as some of the most severe indicators of digital repression, given that the effects of such practices not only cut off individuals from *en masse* and interpersonal communications but also have a large impact radius while isolating entire societies (Rydzak, Karanja and Opiyo, 2020). The fact that governments possess the power of shutting down the voice of entire population at once is cause for concern. Which begs the question of accountability and the imbalanced power that central government authorities hold over a large demographic that they are appointed to serve. An overwhelming number of internet shutdown orders come from central authorities with the highest levels of political power (Mawii et. al, 2018)**.** The highest rankers in government authority holding access to unequivocal powers of censorship should ring alarm bells. Literature on digital authoritarianism, however, is limited in the scope of accounting for tiering such power.

By applying the practice approach to digital authoritarianism, this research would make use of broadening paradigms so that the focus does not solely remain upon the actors but emphasises the action itself. The power to instate internet shutdowns is not simply limited to central authorities, given the number of shutdowns experienced in India were the highest in the world due to executive authority held by central as well as state level actors to mandate shutdowns (Freedom House, 2020). In cases of digitally repressive state institutions, the presidency can be instrumentalised with mechanism to shield the regime against oppositional attacks (Rydzak, Karanja and Opiyo, 2020). Not only must the actor, but also the pattern of action be scrutinised to contextualise the legitimacy of a practice. An authoritarian practice undertakes attempts to enable pattens of action, which are embodied in organisational contexts and possess the power to exert political control to disable access to information while sabotaging scope for accountability (Glasius, 2018). By utilizing theories of social and political action, a roadmap of causalities can be stipulated between protests and shutdowns, using internet as a connective tissue between the two phenomena.

2.4. Dis-connective Action Theory

The ability for the internet to manage revolutionary efforts have been evidenced by the propensity for collective engagements on several occasions including the Arab spring, Hongkong protests and the global climate strikes. It shows how individuals and citizen leaders can come together to structure and organize mass movements to pressure governments in shaping policy and implementation of public demands. Connective action theory in the digital age gives collective action a necessary boost of outreach beyond confines of localized protests and helps involve larger demographics**.** Bennet and Segerberg identify connective action as the means through which individuals and movements make use of the affordances available through communication technology to gain momentum and take advantage of formerly unorganised structures in an innovatively strategic manner within highly adaptive action frames (2013). However, connective action paradigms do not fully account for the variety of authoritarian practices enabled as countermeasures and thus understate the variables of societal responses as reactions to technological repression (Rydzak, Karanja and Opiyo, 2020).

Organically flourishing systems during protests are mostly based on retaliatory measures against pushbacks and repression. Structuring a stipulative playbook for every mobilization is impossible, given the variability of responses created by the power. From the perspective of governments imposing them, the effectiveness shutdowns following the escalation of momentum of protests is questionable at best, given the fact that citizen activists tend to apply combinations of strategies to continue mobilizing despite attempts at silencing dissent (Rydzak, Karanja and Opiyo, 2020). Countries that practice kill-switch shutdowns during protests have never yet publicly issued statements acknowledging the effectiveness of shutdowns as viable means of suppressing public unrest, nor have they conducted studies to prove their means to ends (Rydzak, 2019). Despite this fact, internet shutdowns seem to remain common and growing in number each year.

Rydzak refers to the theory of disconnective action as dynamics, mobilization structures and strategies that evolve during or because of information vacuums created during shutdowns

(2019). While connective action mansifests itself in the presence of communication technology, disconnective action develops as a contrasting phenomenon, causing a shift to offline protests in the absence of communication technology. These collective actions often occur as low cost and/ or low-engagement alternatives to mass movements on the street which are not sustainable in the long run due to the high cost burden they incur on the socioeconomic paradigm upon the participating population and may slowly fade out, especially if the government does not seem to be budging from their stance or capable of meeting protesters' demand (Rydzak, 2019). Which is to say that mass protests in the physical world tend to be further encouraged when possibility of online protests are extinguished but can only be sustained if a mobilization structure is already available for its system to function. Disconnective action abbreviates or nullifies Bennet and Segerberg's (2013) theory of connective action when the network communications themselves are unavailable. A disconnective action is understood to be in occurrence when the succession of changes that occur during the coordination, organisation and outcomes of collective action can no longer take place due to the deliberate and abrupt revocation of access to digital technology. While attempt to disconnect dissenters and suppressing their voices can destabilize existing protesting movements, governments are often cautious about implementing such authoritative measures for extended periods of time. The efforts to suppress dissent can be interpreted as signs of weakness on the front of the sitting regime, making way for anger and politicization of censorship (Roberts, 2018).

3. Legitimacy and Legality

3.1. Overcoming Legal Disconnect

This research, in part argues that the practice of internet shutdowns cannot be always entirely legitimate, given the absolute authority that many sovereign states hold with respect to dissemination and coordination of information. The legal framework within which communication networks function are mostly chartered after national security and telecommunication laws pertinent to individual states, which are likely to vary within local contexts and regimes (Gohdes, 2020). This puts more urgency on monitoring internal legal frameworks of censorship for the future as governments across the world continue to invest heavily in infrastructure for digital controls (Deibert, 2003). The lack of a connected internet infrastructure in the modern world creates a digital divide between those who enjoy freedom of expression online and those who do not, and authoritarian governments often use archaic and repressive laws to extrapolate digital rights violations.

International organisations like Access Now, Internet without borders and Freedomhouse stress on the importance of maintaining checks on government mandated internet shutdowns across the world, especially owing to the expanding network of grassroots activism which holds policymakers accountable. However, pressure form organisations like the United Nations (UN) and World Trade Organisation (WTO) gauges more regulatory impact. The UN general assembly in 2013, for the first time stressed on the critical role which the internet plays in achieving progress on the Millennium Development Goals (Records of the general conference, 2013). While acknowledging the socioeconomic importance of keeping the internet on is necessary, guidelines on the implementation of control need to be addressed as well. In July 2016, United Nations Human Rights Council (UNHRC) passed a resolution condemning network disruption measures taken by states to control online access and information dissemination; stressing that rights and freedoms afforded to individuals in the offline sphere must also be unequivocally afforded to them in the online sphere (Records of the general conference, 2013).

Bodies including Internet Governance Forum (IGF) and World Summit on the Information Society (WSIS) have been created to aid the UN on internet governance, where governments, business and other stakeholders can confer on issues related to the deployment and adherence to the Universal Declaration of Digital Rights (Dragu and Lupu, 2021). The Constitution of the International Telecommunications Union (ITU) has offered legal parameters within which Internet Shutdowns are justifiable. These parameters offer states the freedom to undertake measures to block access to digital information in extreme cases which could impede state security.

3.2 International Declarations on Digital Rights

Specifying a paradigm for digital rights is important to this research as it establishes a place for recipients of authoritarian control within the framework of kill-switch shutdowns. If there is a suppressor, there will be those who are suppressed, and their rights need to be amplified through digital protection measures. In 2020, the UN Secretary General’s Roadmap on Digital Cooperation centres a document on human rights in the digital age. The document classifies blanketed internet shutdowns as violation of international human rights law (Taye and Access Now, 2021)**.** The United Nations Human rights Council Resolution 32/13 of 2016 unequivocally condemned practices intended to disrupt or prevent information dissemination online as violations against human rights laws (Amnesty International, 2020). Additionally, General Comment 37 in the same resolution unequivocally disallows internet shutdowns which hinder peaceful demonstrations and assemblies.

A sovereign states online environment must still be subject to nation laws to a large degree, and it is necessary for states to govern spaces, whether digital or physical in a manner which ensures safety and security of individuals. Which is why international bodies such as International Covenant on Civil and Political Rights, while emphasizing on freedom of expression, allow for restrictions on those freedoms under special conditions (ICCPR; United Nations, 1966, Art. 19). Exercising fundamental rights require exercising special responsibilities and duties. The right to free speech and assembly can be curbed by implementing limiting measures which would be necessary for "respecting the rights or reputation of others" or "protection of public order and National Security" (United Nations, 1966, Art. 19).

This literature review section of this research has so far encapsulated Kill-switch internet shutdowns within the framework of authoritarian practices. This section elaborated on how revocation of access to communications technology can be used to halt opposition and stop shut down protests in dissenting atmospheres. By categorizing authoritarian control over the internet kill-switch, we see how authoritarian practices in the digital sphere can shape themselves if left unregulated and without intervention. The following Methodological section would encapsulate the structure of the rest of the research project. By analysing empirical data on internet shutdowns and their correlation with protests and violence, a case for the legitimacy of such measures can be made. The existing literature highlights internet shutdowns as authoritarian practices but falls short of accounting for the necessity of it in special conditions. During instances of existential threat to sitting regimes, the literature also does not provide alternative suggestions in place of internet shutdowns to preserve the policy and governance fabric of nation states. This research uses the concepts presented thus far to make suggestions on the future of digital governance in line with national and international parameters.

The following section in this research explains the ways in which governments practice control over the internet infrastructure. If internet shutdowns are to be implemented as models of practice, a methodical framework is necessary to locate points of access. Once governments can identify the points of access, practicing control becomes simpler as gatekeeping of information can be managed through repressive measures. The next section explains disconnective action through the example of chain of command followed in the structure of digital control. By observing the dynamics between how decentralized information markets work and how state-owned infrastructures can impact the levels of freedom and surveillance afforded to the citizens, an understanding of repression technologies in modern governments is formulated.

A further analysis of legitimacy of internet shutdowns is illustrated n the following sections through state justifications for initiating network blackouts. The necessity of internet shutdowns is contested by citizens, but states present a collection reasons for enacting repressive measures as justifications. These justifications will shed a light on internet shutdowns from the perspective of governments and how they can perceptually be considered necessary measures implemented to avoid damage to the fabric of national security. The theories presented in the analysis so far would be useful in analysing the interconnected aspects of participation in digital government, which involves, regimes, service providers, civil society, and citizens.

II

Internet as a Repression Tool

1.1. Framework of Network Control

The internet infrastructure in any given country is made up of several stakeholders who are responsible for transmission of data at various stages. At times, the internet service providers are private stakeholders and at other times, they are semi-private corporations with the government as partial or majority stakeholders. The internet infrastructure is made up of several levels of operators who function at different stages of the information route. Internet Service providers (ISP) are the primary suppliers of data, who regulate collections of specific country domains and IP addresses, through which data can legally travel. They have operational jurisdiction within the allowed scope of a nation's digital borders. Data permitted through ISPs is sent as packets of information to Internet Exchange Points (IXPs). IXPs can be considered as nodes for the mass transmission of data facilitated through physical infrastructure such as internet cables and wireless exchange points to the public. For governments to be able to stop transmission of information or retain control over the internet in any geographical or demographic location, they first need to have control of authority over these elements of the internet infrastructure (Leon, 2020). A government can only block access to the internet for users under its own jurisdiction. If a user has access to foreign ISP networks which do not come under the jurisdiction of said government, then the government cannot control or block the services over that channel. Satellite telecommunications units and extraterritorial broadband units are some of the mediums which governments cannot control if the service over said infrastructure is provided from outside the country's jurisdictional borders.

Transmission of data over the internet depends on hierarchies of physical infrastructure, which work together to allow and block access to online data. Having a tangible operational capability over these infrastructures provides governments and telecommunications operators with opportunities to exercise control (Mare, 2020). Such control can manifest itself in several forms including licencing for operations, establishment of surveillance infrastructure over networks and managing international gateways for information like DNS blockings and Internet Protocol (IP) restrictions. Freyburg and Garbe have found that the tendency for state regimes to be involved in the structure of ownership in the internet infrastructure magnifies chances of internet blockades to be carried out (2018). Conversely, a decentralised internet infrastructure ecosystem with several stakeholders and multiple service providers decreases the vulnerability of networks and the probability of shutdowns to occur (Leon, 2020). However, a decentralised network of communications also increases the repertoire for encouraging surveillance infrastructures and mechanisms of infiltration; observes Morozov (2012). Governments which hold legal authority of throttling internet bandwidth instead of shutting them down have an added layer of plausible deniability, since the lines of communication are still existent, albeit slow enough so that most forms of modern data exchanges become impossible to disseminate (Gohdes, 2020**.** This is called information throttling, where kill-switch shutdowns are not carried out, but dissemination of mass communication channels are rendered ineffective.

Governments do not normally restrict internet services directly but order telecommunication operators to do so. Although service providers and other Autonomous Systems (ASs) of information communication could choose to block internet access over their networks if they wanted to, they generally would not have a reason to perform such actions unless ordered by governments (Freyburg and Garbe, 2018). For governments to practice repressive control over the ISPs, there needs to be control over the availability of a competitive market. If the internet infrastructure in a country is more decentralised with multiple service providers and exchange points, it becomes much harder for governments to order ISPs to comply with executing targeted shutdowns. In this respect, the tendency for a government to practice authoritarian control over the internet infrastructure increases its potential for mandating strict auditing for licencing to telecommunications providers.

Access Now finds in their report on internet shutdowns, that overwhelming majority of kill-switch shutdowns have been enacted either by authoritarian regimes or hybrid regimes of semi authoritative nature (2020a). They further go on to conclude that most shutdown orders come from the executive branches of authority in the government. In order to limit internet shutdowns to the central authority within a regime, the power of implementation must rest in the hands of the highest levels of execution. This observation developed on Freyburg and Garbe's study, however, does not hold to practice in the case of India. It must be noted that despite having the largest percentage of internet shutdowns in the world by a disproportionately overwhelming margin, the occurrence of multiple shutdowns in India is a result of decentralization of authority over information communications between primary and secondary levels of administrative units (Mawii et al., 2018). By granting powers of control in multiple levels of governance, India has given route to higher chances of misappropriation of authority. 22 of India’s state governments out of 29 have known to have initiated intentional shutdowns, showing how regional authority over jurisdictional internet infrastructure has made it much easier for secondary level actors to practice digital authoritarianism. is not possible to theorize an operational playbook on how shutdowns are initiated and who the practicing actors are. Instead, considering the existence of internet shutdowns within large spectrums of democratic and authoritarian states with varying levels of control should be viewed under the lens of authoritarian practices irrespective of the type of regimes under which they occur (Glasius, 2018).

2. Justifications for Shutdowns

According to data obtained from Access Now’s (2019) world internet shutdown statistics, official justifications that governments provide for ordering internet shutdowns range between stopping the dissemination of disinformation and technical problems in infrastructure The findings in the 2019 #Keepiton report by Access Now, present that in 33 percent of the cases, government justifications are rounded out to curbing misinformation, and 30 percent of the cases are attributed to precautionary measures in cases of political instability (2019). The data reveals that public safety and national security are used as justifications in 24 percent and 14 percent of the cases, respectively. Despite the limited and often ambiguous justifications provided by governments for initiating kill-switch shutdowns, critics find several other underlying factors resulting in shutdowns, amongst which stifling free speech and dissent are common (Ricknell, 2020).

2.1. Elections

In Sub-Saharan and Central Africa, elections are one of the most common reasons that governments cite for implementing internet shutdowns. Lindberg (2004) observes that 80 percent of elections in Africa in the late 1990s and early 2000s witnessed incidences of electoral violence. Countries including Burundi, Chad, Uganda, Democratic Republic of Congo, and Ethiopia have regularly interrupted access to the internet during election seasons to stop the spread of incendiary information and calls for violence online (Freyburg and Garbe, 2018). Internet was restricted during one third of the elections in Sub-Saharan Africa between 2014 and 2016; find Freyburg and Garbe. The practice of shutting down the internet has been a common tradition in many African nations, but the fact that authoritarian regimes can benefit from a lack of information disseminations through non-traditional channels of communication, which may favour oppositions cannot be ignored. Information technology possesses the capacity for offering novel communication pathways that can be fundamentally resistant to authoritarianism or state regulation, thus reducing the states' ability to nurture repression (Garrett, 2006). Unlike traditional media, the internet can hinder a states ability to control flow of political communication and propaganda.

2.2. National Security

Even though justification provided by states are mostly vague and strategically ambiguous, governments do not perceive it as necessary to reveal exact information when it comes to preservation of nation security. Which is why national security justifications are common, amounting to around a third of official justifications provided in cases of shutdowns. Self-defence as an anticipatory action has been used as a reasoning within the framework of international law since a long time, arguably assuring credibility considering the changing dynamics of contemporary warfare and militant tactics of cyber-criminality (Franck, 2003). By providing national security reasons as justification for shutdowns, states can argue their self-defensive stance against potential use of authoritarian measures (Joyner, 2001). In the context of kill-switch shutdowns, implementation can be justified as measures to avoid damage to critical infrastructure due to cyberattacks or as legitimate actions to exercise self-defence from external actors intending to interfere in internal matters of state (De Gregorio and Stremlau, 2020). Attacks on communication infrastructure and a nation's cyberspace are seen as threats to national security, owing to their devastating capabilities of not only damaging infrastructure but also other dependent services interconnected with each other (Deleure, 2020). Many countries see internet shutdowns as necessary practices in certain cases, especially with respect to critical infrastructure and cybersecurity. The 2016 Human Rights Council resolution condemning "Unequivocal measures to intentionally disrupt access to online information" (2016), was opposed by many governments known for mandating information control, among which, China, India, Russia, Saudi Arabia, and South Africa were quite vocal.

The legitimacy of justifications pertaining to internal and national security can be contested but are often pitted against hard narratives, which would be difficult to disprove, owing to the secretive nature of state security dynamics which may vary in individual cases.

Gregorio and Stremlau also point out that internet shutdowns are not always detrimental to the peace and stability of affected regions as long as prolonged outages do not increase to threatening levels which could escalate violence (De Gregorio and Stemlau, 2020). In many cases, states argue that the necessity of internet shutdowns outweigh the consequences. The Democratic republic of Congo's internet shutdowns during the 2016 general elections were urged on by the interior minister Raymond Mboulou for reasons of national security (Agence France Presse, 2016). Despite these efforts, public discontentment could not be curbed as post-election violence still broke out after Denis Sassou-Nguesso won the presidential term for the third time in a row (Al-Jazeera, 2021).

Wagner points out that incidences of governments trying to marginalise societies or groups seeking to underline violations of human rights is a common practice (Wagner, 2018). Due to public outrage against government, there have been several communication raptures, censorships, network throttles and shutdowns in Ethiopia and Equatorial Guinea, which, in the past decade have been in several lists amongst the most censored countries in the world (Freedom House, 2015) Ethiopia in 2020 and 2021 has witnessed mass protests and months long extended shutdowns following the death of a celebrity protester, for which many critics held the government responsible (*Hachalu Hundessa: 'Eighty-one killed' in protests over Ethiopian singer's death*, 2021).

2.3. Dissemination of Illegal or harmful content

In the Ethiopian context, the government has also, on many occasions shut off internet access during exam seasons. In June 2016, following a mass leak of examination question papers online, the Ethiopian government decided to shut down the internet for a week (Ayalew, 2019). The question papers circulated on the internet prior to the end-term university exams sparked a major row, in response to which the government imposed the measure (Ayalew, 2019). In the wake of very regular internet shutdowns, the government has tried to build narratives of sustained economic growth, which the country benefits from if they maintain resilience against overreliance on economic progress brought on by the internet. This narrative is built around the fact that a double-digit surge in economic activity was experienced in the country despite shutdowns being in place, extenuating a causality between the two phenomena (Ayalew, 2019).

Governments often reiterate the fact that measures effected to stifle communications are meant for maintaining public order and peace within the community. The proliferation of this justification since the past decade points towards its plausibility at face value. The fact that the internet can be used for malicious intent including propagation of misinformation and dangerous content with the potential to create false narratives is not lost on governments. The conflict in Indian Kashmir is volatile and sensitive to incendiary information, causing shutdowns to occur regularly due to dissemination of controversial viral content. Several videos which showed Indian armed forces behaving rashly with dissidents in the Kashmir valley have given rise to violent outrages (Panicker, 2020). During such incidences, shutdowns are authorised by the central government of India on a regular basis under the Indian Telegraph Act of 1885 in conjunction with Rule 419A of 1951 to curb public disharmony (Telegraph act, 1885).

The nodal distributional arrangement of social media plays an important role when it comes to disseminating objectionable content. Visual content that engages emotional responses in recipients including feelings of hate, violence, and discontentment, amplify contribution to violent escalations and promote conflicts around the world regardless of the credibility in essence of such information (Dragu and Lupu, 2021). Former US president Donald Trump remarked on the internet's capacity for being used as a tool for recruitment of terrorists while reinforcing his idea of empowering the presidential office with capabilities to switch off the internet and be used in a better ways against "Fake News" (Leon, 2020). The government in Uganda ordered blocks on social media websites including Twitter, Facebook and Whatsapp during the counting of poll results, justifying the move as a necessary security measure to prevent lies from spreading online (Duggan, 2016). Although arguments for shutdowns to curb dissemination of harmful content are legitimate, the question remains, harmful to whom? The ambiguity of what constitutes as harmful information in general is not lost on governments which seek to stop information which could threaten their regime's stronghold. It is therefore not surprising that protest leaders and opposition forces come under the scanner as peddlers of false information.

3. Shutdowns and Protests

Data from the 2020 Shutdown Tracker Optimization Program (STOP) overseen by Access Now reveals that the year witnesses at least 450 confirmed Kill-switch shutdowns between local, regional, and national levels in almost 50 countries worldwide (Access Now Keepiton Report, 2020). The propensity for governments to enact internet shutdowns, however, does not seem to have detrimental effects in the propensity for mass mobilisation activities like protests. Rydzak, Karanja and Opiyo find in their analysis that participants in active protests tend to adapt varying strategies to mobilize as conditions of information prevalence change and information spaces are disrupted (2020). Bennet and Segeberg (2013) explain this using their paradigm of connective action theory, stating that individuals and movements, including civil disobedience use the affordances provided by communication technology to gain momentum in their struggle. Participants tend to take advantage of other loose structures at their disposal to innovate new strategies and employ highly personalised frames of action.

Goodwin (2017), in their analysis of protest dynamics during information raptures analysed collective action movements in Syria and Egypt to find that although Kill-switch shutdowns lead to more decentralization in protests, they provide more opportunity for more peripheral leadership to take initiatives in pockets of resistance. The internet shutdowns in Egypt during the Arab Spring in 2011 are testaments to this finding (Rød and Weidmann, 2015). The success of a shutdown in terms of quelling protest is not always guaranteed, considering that other vectors like economic proliferation and international attention also play a part in how effective a movement becomes. When protests have been gaining momentum prior to shutdowns and are privy to reinforcements by organised movements as backups, it becomes much harder for them to be effectual (Rydzak, Karanja and Opiyo, 2020). The Mubarak regime made attempts at quelling protests by disconnecting Egyptian citizens form the global internet infrastructure during the January 2011 protests, but owing to the involvement of educated elites and technologically capable individuals, dial-up internet connections and satellite telecommunication instruments were able to surpass the restrictions in maintaining connection with the outside world (Warf, 2011).

Availability of internet connection is an important tool for connective action during mass movements, but protests have a tendency for adaptation to contingent environments. To overcome drawbacks of contingent disconnective action, states also adopt alternative strategies of engagement over time. Authoritarian governments tend to gain control over ISPs in order to hold executionary authority over the internet (Giacomello, 2005). If states own ISPs or at least are major stakeholders in a nation’s most prolific ISPs, then they can execute targeted disconnections on specific actors or selected groups (Howard, Agarwal and Hussein, 2011).

Autocratic regimes are generally more inclined towards adopting communication technology tools to their own benefit. A more connected network under the control of the autocracy translates to higher opportunity for surveillance, censorship, and tighter grip on public opinions (Ruijgrok, 2017). It also means that Opposition to the incumbent regime can be quashed much more efficiently when the content disseminated as public information is within the scope of government influence. By gaining more access to information communications, the ability for governments to initiate cyber-policy doctrines increases, making the content of online information more filtered and fitted to benefit the state authority (Bowman and Camp, 2013). Governments can further establish their stronghold by making arrests and detentions under pretexts of dissemination of unlawful information and disruption of regime stability. Arrests and detentions of cyber-dissidents is a sign of government and police presence in online arenas, which is a powerful tool when it comes to deterring such activities in the future (Rød and Weidmann, 2015).

4. Shutdowns and Violence

Gohdes (2015) finds in their study of correlation between internet shutdowns and the propensity for violence, that network outages do not necessarily increase incidences of unreported violent activities in protesting environments. They go on to say that government mandated kill-switch shutdowns are accompanied by a rise in significant levels of violent activity, particularly in locations where opposition forces are directly confrontational with the incumbent government. Conversely, they argue in another study on repression technology, that increases in levels of censorship in areas under authoritarian control, state sanctioned violence affects incumbent populations more indiscriminately (Gohdes, 2020). There have been disagreements in the academic filed whether the propensity for enacting internet shutdowns is correlational to the propensity for violence to occur. There is wide debate over whether prompt technological expansion has a deterrent effect or causes a boost to collective violent action, which may vary in context, temporality, and justification (Rydzak, Karanja and Opiyo, 2020). There have been arguments on both sides of the debate, where some link adoptions in communication technology to higher incidences of conflict and violent actions (Pierskalla and Hollenbach, 2013) while others point out that rapid increases in connective infrastructure have been found to curtail violence propagated through insurgent action owing to information technology's potential to expedite dissemination of news and real time reporting (Shapiro and Weidmann, 2015).

Rydzak (2019) finds that target kill-switch shutdowns in India are associated with upsurge in violent conflicts in subsequent days after disruptions are initiated. Public opinions of regimes which attempt to stifle free expression while public anger is at its highest do not seem to help the cause of curbing discontentment. Using Syria as a case study, Gohdes (2015) found that dramatic surges in violence followed periods of network disruptions by correlating causality data between the two phenomena. They explain how nationwide internet shutdowns coincide with higher likelihoods of state violence, indicating intentionality of the government behind employing strategies to weaken the oppositions' capabilities of coordination and mobilization.

Protests are generally aimed at voicing opinions of discontent against policies which demand change. Participating in violence could lead to a drop in the results that peaceful demonstration could yield. Usually, peaceful protests are the norm for civil disobedience and violent riots are exceptions. When met with shutdowns, peaceful protests are observably marked by a peak-and-trough variation in regularity, with a concerted hike in participation following one or two days followed by a drop-in activity to give leaders and opposition forces the opportunity to recover and gather resources whilst dealing with "protest fatigue" (Woods et al., 2012).

Government responses to protests also affects whether violence does occur during conflicting atmospheres. If use of force is deemed necessary by governments in situations where peaceful dialogue could subside the situation, there are chances of clashes and mobs erupting due to public anger. At times, disconnections can come as retroactive responses to violent clashed to protect public order. Internet shutdowns in Central Africa during violet clashes are not uncommon occurrences, where governments briefly shut down communication channels to try and dissuade propagation of violent narratives and hate speeches online (Ghodes, 2015). The potential for the internet to spread misinformation and anger should not be overlooked when proclivity for violence needs to be contained. Pierskalla and Hollenback (2013) deduced that violent incidents are more likely to prop up in locations where easier access to wireless phone networks are present, owing to the speed of communications offered.

III

India’s Shutdown Practices

1. Protests in India and Digital Communications

The role that messaging platforms and social media play in the protest dynamics in India incredibly explosive. Mobile devices have aided in the mechanisms of gaining traction within the past decade in a way which previous forms of communications could not have managed. The growth of wireless connectivity to the large demographic in India has been overwhelmingly greater than any other developing country owing to market competition, reduced costs of services and a booming smartphone market, quickly replacing the fixed-line broadband infrastructure (Rydzak, 2019). Protest movements have been bolstered on the back of digital communications due to the visibility offered through a cost-effective communication channels, doubling as devices for recruitment of like-minded individuals striving towards shared goals (Kumar and Thapa, 2015). However, rampant poverty and lack of access to communications in rural settings still leaves a wide scope for the internet to be used for grassroots efforts. By 2018, the internet penetration rates in India were lower than 35 percent, with steady increases as digital infrastructures continue to be built in remote locations (Rydzak, 2019). The tendency for commercial markets to invest in India’s connective infrastructure has given a boost to the possibility of networked protests to occur within well connected movements consisting of young and digitally capable circles (Davenport, 2010). The link between mobilization efforts and India’s growing young population including university students and youth political organizations is evident through the growing distribution of social media content via civil society social media pages (Nordas and Daveport, 2013).

In the context of the digital sphere, emerging civil society organizations which routinely engage in protests constitute of women’s liberation groups, environmentalists, poverty alleviation groups and child development organizations which have grown to 38, 300 online registered entities as of 2018 (CSRIdentity, 2018; Rydzak, 2019). Collective action has been gaining traction mostly by combining efforts with the mass disseminative capabilities afforded by connective action over the digital sphere, where words of dissent mirror public discontent through alliances with NGOs and political parties (Ren, 2017). The target of structured protests in most of these cases are governments and political elites, which should not come as a surprise, considering the growing levels of repression over online communications but cohesive tactics as a response to mobilization has a counteractive effect on the expected results. The resilience of protesting movements, which are normally non-violent in nature, observably increases as a response to organizational cohesion (Pearlman, 2012). Continuous stifling of free speech is seen amongst dissenters as a sign of government weakness, wherein communication of truth is seen as a threat to the legitimacy of rule (Sutton, Butcher and Svensson, 2013), which invariably gives opportunities to spokespersons and opposition leaders in furthering their causes.

The dynamics of protests in India are especially leader-dependent and often allow room for powerful faces to emerge as leaders lending voices to movements. This helps protests gain momentum within communities that revere leadership either in the form of institutional icons or individuals, connecting the individual to the cause. Although reactionary measures are common against protesting leaders in India, the removal of such leaders and iconic structure could backfire or precipitate into chaos, depending on the occasion and persisting ideology (Bob and Nepstad, 2007). The direction authoritative actions take is also dependent upon movements' structural formalization and existing unity. A unified opposition is seen as a threat to the incumbent regime's legitimacy, which, if left unchecked could progress into violent overthrow. In such cases, violent coercion is generally imposed as a response to rising levels of threat and continued opposition to retain regimental power (Rydzak, 2019).

The complex political climate in India allows for mobilizations to turn violent without warning due to unorganized protest structure or through acts of sabotage. Which is arguably one of the reasons why India remains one of the very few democracies in the world to routinely exercise information disruptions and kill-switch shutdowns even more assiduously than some autocracies (Rydzak, 2019). The speed at which false narratives and disinformation circulate amongst tightly knit groups is telling of the mobilizing effects of the internet. Abraham (2017) remarks that incidences of mob lynching in several instances such cow slaughter, child abduction and dacoity were attributed to disinformation made viral over WhatsApp forwards, leading to groups of angered mobs brutally attacking suspected criminals. In cases of cow slaughter, law has been often taken into the hands of extrajudicial organizations called "cow vigilantes", who would at times resort to use of physical force and extreme violence against minority groups suspected of slaughtering cattle for meat (India: Vigilante 'Cow Protection' Human Rights Watch, 2019).

The problem of separating genuine information from disinformation is not being successfully combated owing to the exceedingly large amounts of information needed to be regulated in that respect. Moreover, with growing platforms of communication on the internet, it becomes exceedingly easy to disseminate information to large masses before it ever catches the attention of concerned authorities. The growth of information communication in the digital sphere has expanded space for free expression of ideas while at the same time escalated the possibility for false information to root deeper into the public sphere in India just as anywhere else in the world (Rydzak, 2019). The fact that disinformation can quickly devolve into agitation and protests in India have likelihood of violence to be carried out, governments can justify authoritarian measures under such circumstances unequivocally. Governments in India often use pre-emptive shutdowns in cases where incendiary information has a possibility of spreading (Bhatia, 2017). Even before rumours could escalate to protests, governments often cite reasons like "maintenance" of public order or preventing "communal violence" as legitimate reasons for enacting shutdowns.

2. Legal Framework of India's Shutdowns

The pre-independent history of civil disobedience in India has been that of protests against the British empire and censorship has been a common practice to quell protests ever since. Despite the constitutional changes since and reliance on digital communication in the past decade, some archaic laws such as the Telegraph Act of 1885 have remained since the British occupation (Bhardwaj *et al.*, 2016). The Telegraph Act of 1885 empowers incumbent governments and state regimes with authority to disable channels of communication, which could be deemed incendiary or harmful to public peace and order. According to the act, the government of India's official branch the authority in dealing with the telecommunication industry to stop the spread of harmful information. The act defines dedicated rules titled under Temporary Suspension of Telecommunications Services, wherein Public Safety and Public Emergencies constitute for justifiable reasons for suspension (Nayak, 2018). The context of public emergency and public safety are vague with respect to the underlying features of what potentially constitutes as emergency and what the public needs to be secured from. The vagueness of the titles under this provision has resulted in governments gaining traction while implementing arbitrary suspensions and gaining access to instruments of censorship. The provision along with the Information Technology Act has enabled governments to make use of suspension rules and intercept communications over public networks at endemic proportions (Bhandari and Sane, 2016).

Before 2017, The operationality of Internet shutdowns were placed under the legal paradigm of criminal processes within the Code of Criminal Procedure, wherein Section 144 of the Telegraph Act authorized provisions for executing internet shutdowns for dispersing and quelling unlawful assemblies and imposing curfews (Nayak, 2018). In 2017, amendments were added to the act with respect to the authority of control over initiating internet shutdowns. Even though the new regulations established a range of checks and balances to afford state institutions the legitimacy for implementing shutdowns, including assigning authority of control exclusively in the hands of senior civil service officers, there are still numerous clauses and terms which could be left open to interpretation (Kathuria et al., 2018). The amendments have not managed to stifle the frequency with which governments at the state and national level continue to implement kill-switch shutdowns. In fact, due to the arbitrary provisions of "unlawful gatherings" under this section, internet shutdowns are given more prominence, considering shutdowns are perceived as the next logical steps towards inhibiting large gatherings during curfews and lockdowns (Narrain, 2018).

This makes the issue of protesting under military or police curfew a criminal activity, while at the same time justifying the use of kill-switch shutdowns as a safeguard to maintain public order. There have been several instances where the government has decided to implement drastic measures enabled by the Telegraph Act, including long term shutdowns which have impacted economic activity on a massive scale. In April 2017, just after the amendments to Section 144 were implemented, a largescale disconnection of services occurred in Jammu and Kashmir, wherein, 22 social media websites and applications were rendered inaccessible (Human Rights Watch, 2017). Since the amendments in 2017, observably, north and west Indian states have been the subject of volatile internet connections, owing to their tendency of experiencing unrest (Rydzak, 2019). The states of Rajasthan, Gujarat, Haryana, and Jammu and Kashmir account for over 75 percent of all shutdowns in India, while Jammu and Kashmir alone account for 47 percent.

IV

Presentation and Analysis of Data

1. Empirical Analysis: Shutdown Practices in India

India stands as one of the most complex countries to study shutdowns, considering the nation’s overwhelmingly dominant proclivity towards initiating internet blackouts. In 2020 alone, the Indian government executed over 109 kill-switch shutdowns across local and regional levels. Most of these shutdowns were temporary blockades, for which the government cites reasons of national security. However, in certain cases, shutdowns tend to last for periods over months, and are sometimes combined with bandwidth throttling measures in tandem. The idea of network throttling is to provide minimum network coverage but minimise the capability for large files such as videos and pictures to be freely disseminated online.

In the following section of this research, statistical and empirical data will be presented to show how the structure of internet shutdowns are implemented as practices by different governments. This part of the research is designed to finding evidence of whether states enact internet shutdowns during protests to quell violent action and communal riots. According to Access Now’s (2020) February Keep it On report, most justifications for internet shutdowns include stopping the spread of fake news, hate speech or disinformation, which are precursors to violent action. Other most prominent justifications are “Precautionary measures” and Public safety”, which seem to be issued in the interest of public. By analysing instances of Internet shutdowns and comparing them with violent activity and ongoing protests during kill-switch operations, this section will analyse the causality between the three phenomena.

This research will work on the assumption that internet shutdowns are authoritarian practices which are enacted only for the benefit of the incumbent regime while repressing free speech and digital rights of citizens. To test this hypothesis, India is chosen as the primary case study. The comparative analysis section of this research is divided into four parts. The first analysis tabulates data on the six highest number of internet shutdowns by country in the world within the bracket of the past two years (2019 and 2020). The second analysis is a measure of the liberal democratic index scores of the same six countries to tabulate their progression in liberal governance practices. The third analysis takes data from the year 2019 and the country India as a case study to compare instances of violence with instances where shutdowns have been implemented. The fourth analysis compares data form the year 2020 and the country India as a case study to compare instances of internet shutdowns, protests, and violent incidences.

In the first comparative analysis, six other countries with the highest internet shutdown score from 2019 have been included to display the overwhelming disproportionality with which India tends to enact internet shutdowns at various levels. Data from these countries is only used as benchmarks to understand what kind of regimes usually initiate kill-switch operations and what are the levels of freedom afforded to their populations.

Grouping of data

To study how internet shutdowns affect protesting behaviours and propensity for violence, this research has curated secondary data from two main sources and two additional sources.

1). Shutdown Tracker Optimization Project (STOP) (2019; 2020) from Access Now's database – The Access Now database has collected information on internet shutdowns around the world since 2016, where instances of kill-switch shutdowns from each country are tracked and corroborated with sources. The level of intensities for shutdowns are also listed in the database, ranging between three levels of disconnections. "Level 1 shutdowns" are passed on a local or sub-regional level and affect a minority of the population in a region. "Level 2" shutdowns are passed on a regional level, which could affect entire constituencies or several sub-regions within a constituency. "Level 3" shutdowns are passed on a national scale, which could affect the entire nation or several constituencies within a nation.

2). The Mass Mobilization Project database – The Mass Mobilization Project tracks protest movements and major occurrences of public dissent across the globe. This database includes types of protests, length of time for each protest and factors associated with movements including violence and state responses.

3). This research uses other secondary data sources to study the types of regimes which implement internet shutdowns on a regular basis. Data obtained from Freedom House and V-Dem project comes into use while comparing alongside data from Access now to understand democratic levels of governance in each of the selected cases as well as the levels of freedom allowed under several metrices.

Freedom Status of Countries with Most Kill-Switch Shutdowns

The first analysis focuses on the tendency for states which shut down the internet to sway towards authoritarianism or illiberalism. Following up on the hypothesis that internet shutdowns are authoritarian practices enacted to stifle free speech, we argue that countries with the highest number of shutdowns have a higher chance of restricting freedoms and observing illiberal practices. This is the observation that Freedom house displays in their Freedom Reports which analyse data using several metrices including internet freedom scores and freedom for protests, scoring regimes on a scale of 0 to 1, where "0" is the lowest freedom score and "1" is the highest freedom score. The data then categorises the mean average of each vector to provide one of three verdicts on freedom status of each country: "Free", "Partly Free" or "Not Free".

This analysis also uses Internet shutdown scores obtained from Access Now's database. The Shutdown ranking is derived after isolating counties with the highest number of shutdowns to the least number of shutdowns and placing them in descending order.

Comparison of data

1). The data on internet shutdowns was curated from Access Now's (2019) STOP database. For this research, a small-N size for the year 2019 was selected. 2019's data was organised according to the number of shutdowns which occurred in a timeframe of twelve months. These shutdown incidences could be ranging between "Level 1" and "Level 3" on the scale of kill-switch operations but for the purpose of this analysis, total number of shutdowns were used while avoiding the inclusion of levels of shutdowns to restrict the data by the number of incidents and not by severity. By isolating individual countries in the database, the number of entries for each country was recorded in a separate table. 2019's data was primarily used for ranking due to the fact that 2020's worldwide shutdown data would be affected by abnormal circumstances including irregular period of lockdown owing to the Covid-19 pandemic.

2). After calculating the total number of shutdowns ordered by each country, a ranking was developed, where six countries were chosen to be presented in this analysis. The number of shutdowns initiated by each country represents the shutdown score provided to them in this analysis; India- 121, Venezuela-12, Yemen-11, Iraq-8, Algeria-6, and Pakistan-5. Only six countries were chosen for this analysis as the shutdown score for all other countries following these six were too low to be included in the study and most of the remaining country scores were too similar to be ranked separately. It is also important to observe that India has the highest shutdown score, owing to the overwhelmingly large proportions of internet shutdowns initiated in the year 2019.

3). The next metric which was used to compare previous shutdown score with the latest data on internet shutdowns, is the 2020 STOP data curated from Access Now's database. Using the same methodology of isolating number of shutdowns per country, the data revealed that India still maintained the highest number of shutdowns in 2020, while Venezuela lost its position as the second highest number of shutdowns. Comparing data from both the years, we can observe significant changes in the number of shutdowns for each country which have drastically decreased over the period of one year except for India, which still shows a markedly high shutdown ranking despite fewer shutdowns compared to the previous year.

4). To analyse levels of freedom in each of the sample countries presented on the list, the freedom scores of each country in the year 2020 were positioned in the next vertex. By using Freedom House's Global Freedoms Ranking chart, we could analyse the freedom score of each of these countries on a scale of 0 to 100, where "0" denotes the lowest level of freedom and "100" denotes the highest level of freedom. This data was obtained from the Freedom House database which already ranked each country using their own metrices for analysis. The Freedom verdict provided by the database displayed the result that only India and Pakistan amongst the six biggest shutdown defaulters of 2019 could be considered "Partly Free" while Venezuela, Yemen, Iraq and Algeria were assigned the status of "Not Free".

5). Another metric used in this analysis was the Internet Freedom scores out of 100 for the six sample countries, which was also obtained from the Freedom House (2020) database. The data cannot be considered conclusive because internet scores for Yemen, Iraq and Algeria were not registered. The Internet freedom scores for India, Venezuela and Pakistan were 51, 28 and 26 respectively, which are much lower than countries in the "free category" for the year 2020.

Shutdown ranking By Country	**Shutdown score (2019)**	**Shutdown score (2020)**	**Freedom House Global Freedom Score**	**Freedom House Internet Freedom Score out of 100**	**Freedom House Global**

(2019)			**Out of 100 (2020)**	**(2020)**	**Freedom Verdict (2020)**
India	121	109	67	51	Partly Free
Venezuela	12	2	14	28	Not Free
Yemen	11	6	11	X	Not Free
Iraq	8	1	29	X	Not Free
Algeria	6	1	32	X	Not Free
Pakistan	5	2	37	26	Partly Free

Table 1. Highest number of internet shutdowns in the year 2019, compared with the shutdown scores of the same countries in 2020 along with their freedom scores 2020.

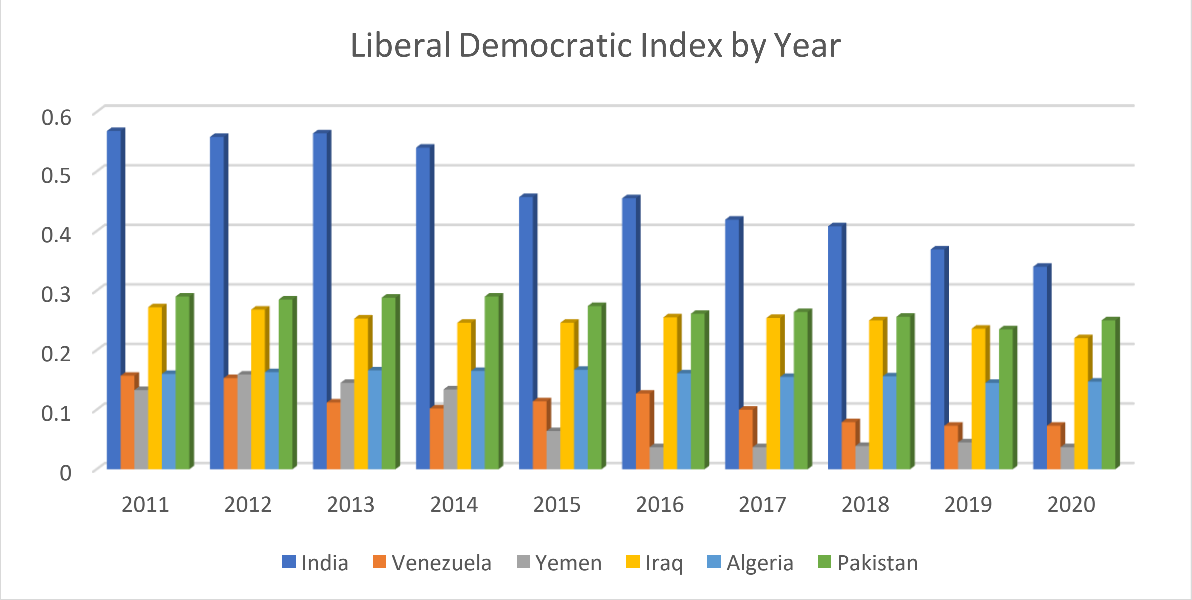
Liberal Democratic Index Score

This analysis compares the liberal democratic index of countries of each of the counties analysed in the previous section for the year 2020. For graphing their developments in liberal governance practices, secondary data collected form V-Dem institute was used. The V-Dem database tracks changes in Democratic egalitarianism, Electoral democratization, and Liberal democratization scores to assess levels of changes governance in each country by year. The scores provided in the V-Dem data are marked on a scale of 0 to 1 for each metric, with 1 being the highest score and 0 being the lowest score.

In order to track the changes in liberal indexes in each of the previously analysed countries, a small N sample size of ten years from 2011 to 2020 was selected. Each country's Liberal democratic index was isolated for the sampled years and compared in progression with the following and previous years.

Observations

The analysis of data in *Graph. 1.* shows that out of all the six countries, only India has ever had a score higher than 0.3. The data for Yemen reveals that it ranks the lowest in the index, with steadily declining scores since the year 2011 until 2020. The data also reveals that while Iraq, Algeria and Pakistan maintained a steady Liberal Democratic score (even though their scores are low) for the past decade, India, Venezuela, and Yemen have had significant fluctuations in their scores throughout the decade. The scores maintained by India for each year, although rating higher on the index as compared to the other countries, has had the most dramatic decline in the past decade. The V-Dem Autocracy report for 2020 also declared India to have fallen to the status of an “Electoral Autocracy” as compared to an “Electoral democracy” in previous years’ reports. This could be attributed to stifled freedoms of expression, crackdown on journalists and activists, and a general atmosphere of state supremacy.



Graph 1. Liberal democratic index scores awarded by the V-Dem data from V-Dem (Varieties of Democracy project)

Internet Shutdowns and Violence in India: Data from 2019

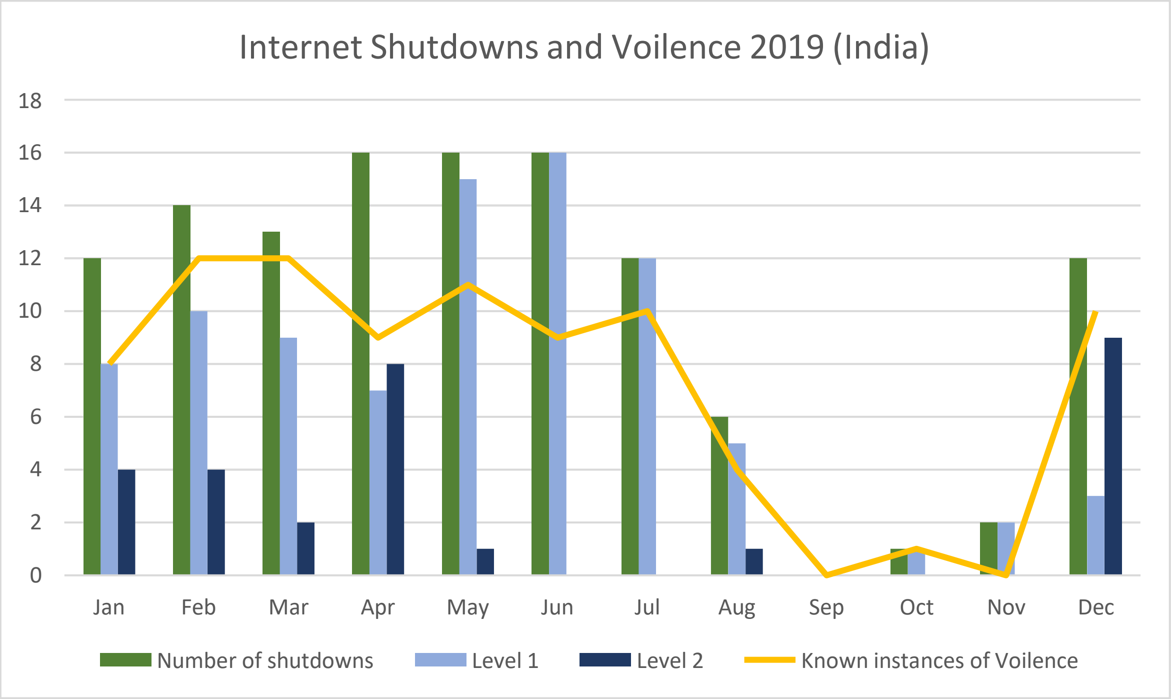
this part of the analysis studies the case of India in the year 2019, where according to the STOP data, 121 separate instances of internet shutdowns were executed throughout the year. These shutdowns vary in degree of implementation between “Level 1”, meaning kill-switch shutdown operations which are implemented on local or sub-regional level, and “Level 2”, Meaning shutdowns which are implemented on a regional or a collection of sub-regional levels. The data was assorted into 12 categories by month, where every single shutdown per each month was grouped in the corresponding vertex.

Each instance of recorded shutdown was assigned the value of “1”. If a month had more than 1 shutdown, then the sum of each shutdown was calculated towards the total number of shutdowns for that month. If a shutdown did not occur in any one month, then shutdowns score for that month was assigned a value of “0”. The levels of shutdowns were also calculated in separate vertices named “Level 1” and “Level 2”, where each instance recorded for either of the two levels of shutdown were assigned a value of "1" and the absence of a shutdown at any level was assigned a value of "0".

The data obtained from the same database for incidences of violence during each instance of shutdown was also used. The value assigned for each instance of violence during shutdowns was "1", whereas absence of violent incidences during shutdowns were assigned values of "0". The total number of incidences of shutdowns were then grouped in a separate vertex according to the month they occurred (or did not occur) in.

Observations

The results in *Graph 2.* show incidences of violence in relation to the incidents of shutdowns for the year 2019, where number of shutdowns, levels of shutdowns and number of violent incidences are calculated. The results show that in most cases where shutdowns did occur, the tendency for violence to occur was markedly lower. Especially in the months of April, May, and June 2019; when all three months saw 16 instances of shutdown for every month. The graph shows that violent incidences ranged between 9 and 11 for these months despite having the highest number of shutdowns. Violent incidences were seen to be the highest during the months of February and March, with 12 instances each recorded compared with 14 and 13 instances of shutdowns. The graph also reveals that shutdown measures in India were initiated on a sub-regional or local level for that year for most months except April and December, where number of "Level 2" shutdowns on a regional or constituent level were higher than number of "Level 1" shutdowns. The data shows that overall, Internet shutdowns in India were not always dependent on the tendency for violent action to occur for the year 2019.



Graph 2. Shows number of shutdowns initiated during the year 2019 and instances of violence during shutdowns for every month

Internet Shutdowns, Protests and Violence: Data from 2020

In this analysis, the year 2020 was taken as a target year, owing to the freshness of data and the larger scope of available metrices. The data for this study was obtained from Access Now's STOP initiative and Mass Mobilisation Project's protest database. The STOP data from access now details individual instances of internet shutdowns that have taken place for the year, while the Mass Mobilization Project data details instances of protests or political unrest and instances of violence during those movements.

To understand the correlation between internet shutdowns, protests and violence, The data was sectioned into three main vertices and two extra vertices.

1). The number of shutdowns for each year were placed in one vertex, where each shutdown was assigned a value of 1 and clubbed with the corresponding month during which they were sanctioned.

2). The Number of protests corresponding to each incident of internet shutdown by date were entered into the database and grouped together according to the month they were implement in. Each individual protest was assigned the value of "1" and the absence of protests, the value of "0". Further, the number of instances of violence during internet shutdowns was assigned a separate vertex, where each instance of violence was counted as an individual occurrence and assigned a value of "1" or "0" depending on the presence or absence of violent action.

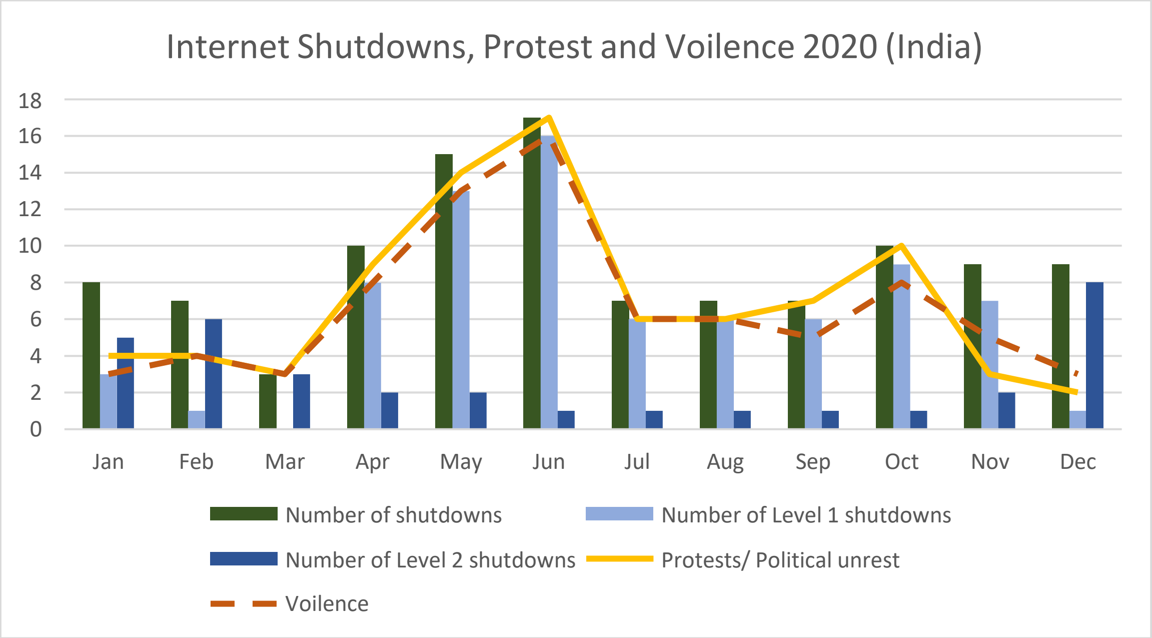
3). Separate vertices relating to the level of internet shutdowns was created, where "Level 1" was assigned to shutdowns if they occurred at a local or sub-regional level and "Level 2" was assigned for shutdowns if they happened at a regional or constituent level. Each instance of the level of shutdowns was assigned a value of "1" if shutdowns occurred and "0" if shutdowns did not occur.

Observations

The analysis of the data in *Graph. 3*. Shows the correlation between internet shutdowns, protests, and violence in India for the year 2020. The data reveals a sharp increase in the number of shutdowns between the months of April and June as well as the number of protests and incidences of violence. In the overall data, there seems to be a consistency between the number of internet shutdowns and the number of protests and violent incidences for the months of February, March, July and August. This study reveals a few notable observations for the year's internet shutdown statistics.

1). For months where larger proportion of "Level 2" shutdowns were implemented, the instances of violence dropped in comparison to months where larger proportion of "Level 1" shutdowns were implemented.

2). Number of protests and violent incidences were comparatively higher during months with the highest number of Internet shutdowns except for the months of November and December, when protests and incidences of violence dramatically declined. The months of January, February and December witnessed reduced number of registered protests despite the high number of regional or constituent level (Level 2) shutdowns, possibly due to information stifling during information blockades.



Graph 3. Shows the number of internet shutdowns by month for the year 2020 compared against the number of protest incidences and violent incidences.

The analyses of data presented above reveals the frequency with which governments enact internet shutdowns. The data at least shows that violent incidences do not always occur during shutdowns, reflecting the negative correlation between violent incidences and internet shutdowns. The data also shows that the overall frequency of internet shutdowns is more than the frequency of protests, which indicates that governments tend enact internet shutdowns as pre-emptive measures as well as reactionary measures. The number of Level 1 shutdowns in the analysis reveal the tendency for governments to exercise restricted blockades instead of conducting blanketed internet blackouts. This could be attributed to the economic drawbacks, which shutdowns pose to the markets. It could also point towards the specificity of control the government possesses over targeted shutdowns. Imposing Level 1 shutdowns disconnects smaller localities, neighborhoods and villages, which means that the authority with which the government can choose to pin-point localities to target can reveal a developed structure of authoritative framework.

The findings of this analysis prove that enacting shutdowns in India is easier for the Indian government than in any other country around the world. The accuracy with which shutdowns can be initiated presents a troubling picture regarding the continuation of disconnective action facing the country. Even though the purpose of this analysis was to show correlations between non-violent and violent mobilization, and internet shutdowns, the findings form this research can help in building a framework for the complex structure of digital authoritarianism in Indian governance. Using this analysis, the future research on shutdowns in India could explore possibilities of analysing micro and macro level structures put in place by the governments just for practicing digital control over its citizens.

2. Qualitative Analysis: Major protests and shutdowns in India: 2019-2020

Software Freedom Law Centre, India (2020) estimates that there have been over 380 different instances of internet shutdowns initiated in the country between 2014 and 2020. A quarter of all shutdowns within this time frame have lasted for not more than 24 hours but several shutdowns have been prolonged for over a hundred days. The anatomy of internet shutdowns in India is mostly limited to small scale disruptions, with local and regional internet shutdowns taking precedence over large scale blackouts. The correlation between percentages of internet penetration rates and propensity for shutdowns to be implemented cannot be ignored as scholars have found urban cities with higher scales of digital development to be less likely to suffer shutdowns beyond targeted, local levels (Kathuria et al., 2018).

Smaller localities and less digitally developed urban centres are more likely to face internet shutdowns than the more internet dependent urban centres due to the reliance on the economic and commercial implications of the networked communications. The scale of proclivity towards communications disruptions is not lost when looking at the fact that out of the 29 state governments in the country, 22 have been known to implemented internet shutdowns at some level (Panicker, 2020). This shows that governments are more prepared to take steps towards engaging in information blockades during times of perceived crisis and that practice approach is taken to the action of network disconnections.

In this analysis of internet shutdowns in India during the years 2019 and 2020, the research focuses on some of the key events which transpired immediately following the second tenure of Prime Minister Narandra Modi's regime. More specifically, three major events will be illustrated here, which caused public discontentment and dominated headlines in the Indian media for months at end. These events were selected due to the huge impact they had over public policy and civil liberties' debates, and the scale and intensity of protests, which challenged the incumbent regime on their policies. During these times, Internet shutdowns were reported at instances when either the government feared violent turnouts or the possibility of harmful information to be disseminated at a large scale as per the justifications provided by their statements.

Revocation of Article 370: 2019

For the year 2018, internet shutdowns in India accounted for 67 percent of total shutdown operations in the world, with a staggering 47 percent of them being enacted in the conflicted territories of Jammu and Kashmir **(**Panicker, 2020**).** The year 2019 had been the darkest year for the conflicted territory in terms of access to information, considering events which transpired in the month of August, including the revocation of the state's special status. On August 4, 2019, the central government of India passed a landmark bill in the upper house of the Indian parliament, authorizing the revocation of Article 370, which granted special status to the conflicted territory of Jammu and Kashmir (Pandey, 2019). The special status granted to the state allowed the government in Kashmir to implement their own constitution, make and amend laws, and delegate their own representatives to foreign affairs. The authority over communications and defence infrastructure remained in the hands of the central government, which caused discontentment amongst citizens of the state, who desired complete autonomy from the Indian central government.

The special status afforded to the state of Jammu and Kashmir was an important part of its complicated relationship with India and the relative autonomy the state enjoyed. Following the revocation of special status, the political climate in the valley witnessed instability, with arbitrary detainments, arrests and violent clashes between demonstrators and security forces (Sodhi, 2020). The government was prepared for situations to escalate and imposed mandatory lockdowns in streets and city centres within the districts of Anantnag, Shopian and Srinagar amongst others (NDTV India, *Lockdown in kashmir,* 2019), which dissidents described as gross violations of their freedoms under a police state. Despite deploying ground forces to curb dissent, the government also felt it necessary to impose multiple internet shutdowns in several districts of the state, which sometimes lasted for months on end (Software Freedom law Centre, India, 2019).

Software Freedom Law Centre India finds that Kashmir has faced over 250 days of continuous internet shutdowns between August 5 and March 2020 (2020). In 2020 alone, there have been 49 separate instances of internet shutdown in several districts of the state. 2G internet services were later restored in the valley after prolonged periods of blackout, which still throttled communications but allowed for messaging platforms to barely function (Mir, 2021). Education within the valley suffered unprecedented setbacks, while online exams for school and university students was near-impossible to be conducted (Mir, 2021). Small and large businesses which relied on the internet bore heavy losses with little to no respite from the government and Kashmir was, for all intents and purposes, shut out from the rest of the world (Freedom House, 2019). State justifications for imposing internet shutdowns in the region included dissuading "anti-national" activities and preventing "terrorist" elements from enacting non-state activities, which could harm India's sovereignty, integrity, and dignity (Panicker, 2020). The move was heavily criticized by dissidents and opposition leaders, calling it an infringement of the Article 19(1)(a) of the Indian constitution, which grants every citizen freedom of expression (Nayak, 2018).

Anti-Citizenship Amendment Act Protests: 2019

Two highly contested citizenship bills were passed by the ruling Bhartiya Janata Party in the upper house of the Indian parliament on 12 December 2019 (Economic Times, 2019a). These bills were immediately sanctioned into laws, disregarding objections posed by opposition leaders, who constituted a small majority in the house. The bills caused massive uprisings across the country amongst minority Muslims, activists, and opposition forces in the country, leading to demonstrations being held across various states with hundreds of thousands of citizens participating in protests (The Economic Times, 2019b). The two bills, dubbed the Citizenship Amendment Bill and the National Register of Citizens Bill were passed into law, which could, in theory, render millions of Muslims within the country stateless, regardless of their previously held citizenship status, as interpreted by the demonstrators (The Wire, 2019). This law was seen by the opposition as an authoritarian measure implemented by the government to exclude minorities from the voter share in the country and appease the majority community, which constitutes the centre's highest voter demographic (The Statesman, 2019). This angle to the laws was addressed in mass movements across several hotspots for protest, unleashing a grave sense of urgency amongst dissenting individuals.

As a response to the growing discontentment amongst the public, the government took steps to block communication channels including shutting down the internet at several places to curb protests. According to findings by Software freedom Law Centre India, communications raptures during Anti-CAA NRC protests accounted for a total of 16315 hours of shutdowns in total (Software Freedom Law Centre India 2020). According to the report, the northern state of Uttar Pradesh witnessed the maximum number of shutdowns, with several districts within the state facing 11 shutdowns at different times, the longest shutdown in the state lasted up to 175 hours. One of the first states to face shutdowns during the protests was Assam in the North-eastern part of India (The Statesman, 2019). The state has witnessed high influx of refugees and illegal immigrants due to its proximity to Bangladesh and Myanmar (The Statesman, 2019). The introduction of the CAA/ NRC bills threatened the residency status of persecuted minorities, especially those who belonged to the Islamic faith but had victims from other faiths suffer the consequences as well (Al-jazeera, 2019)

These protests also came at a crucial time, when the Delhi state government elections were being convened, for which, the centre-ruling BJP was the most powerful party in opposition. Following BJPs landslide losses in the election and escalations of communal grievances between the Hindu and Muslim communities, violent riots engulfed the outskirts of Delhi, causing a toll of 53 reported deaths (The Print, 2019). The shutdowns during the anti-CAA NRC protests in Delhi were earlier limited to protest-heavy areas but the riots led to larger scales of kill-switch operations to be imposed on various localities within the state (India: Freedom on the Net 2020 Country Report (2020).

Farmer Protests: 2020

In the latter half of 2020, massive protests across several states in India started to take root, opposing the controversial "Farmers' Bills". The bills were passed hastily in the upper house of the parliament on 17th of September 2020 and subsequently in the lower house, three days later (Saha, 2021). The opposition parties and activist groups were vociferously opposed to the bills and called it a "death sentence" for the Indian farmers. The three bills which were passed by the centre were dubbed "The Farmers (Empowerment and Protection) Agreement on Price Assurance and Farm Services Bill, 2020", "The Farmers' Produce and Commerce (Promotion and Facilitation) Bill, 2020" and "The Essential Commodities (Amendment) Bill, 2020 (Pundir, 2021). Although the central government stood by their statements that the bills would encourage growth in the agrarian sector and offer better prices to farmers for their produce, Landowners, farmers associations and the Agriculture Produce Market Committee (APMC) collectively opposed the government in their decisions in the form of sit-in protests and marches.

The protests soon tailgated into a highly organised movement, with economic funding, food donations and support pouring in from across the world. The organisational setup and infrastructure were unprecedented during the protests as was the turnout of farmers across the nation (Pundir, 2021). The government eventually expressed their desire to commence talks with the farmers unions while offering to adjust amendments to the laws, but the union declined the government's offers, stating that the entire charade was a deceitful and meant to quell protests (Bhalla, 2021). The protesters demanded a full withdrawal of the bills, which they claimed were passed in favour of large corporations in a bid to corporatize India's rural agrarian market (Pundis, 2021). They claimed that the new farm bills would snatch opportunities of participating in a diverse market and fair payment form agricultural producers while monopolizing the industry in favour of large conglomerates (Bhalla, 2021).

As the movement was nearing India's Independence Day on 26th of January, scores of farmers declared their intentions of marching into the capital and parading across the national monument India Gate (Pundir, 2021). The government took steps to dissuade mobilizing activity within the capital prior to the mass movement by demolishing highways, constructing concrete barricades and spiked walls to make it impossible for farmers to cross into the state border. As an added measure of security, the government decided to shut off internet and telecommunications services in districts surrounding entry points to the national capital, which garnered headlines towards the move from around the world (Pundir, 2021). There were several such shutdowns imposed when the protests started to gain momentum or violent clashes occurred but owing to the input of international attention and the public sentiment towards the plight of farmers, the farmers were able to set up their own communications and security infrastructure to combat government repression (Bhalla, 2021). Despite government efforts, the farmers protest still carries on in 2021, albeit in smaller attendance due to the Covid-19 pandemic.

The responses of the Indian government towards protesting citizens are nothing short of authoritarian. In most cases of large-scale protests, regardless of the levels of violence accompanied or the absence of it, internet shutdowns are seen as a go-to measure with the least accountability following the action. The tendency for the government to freely inhibit access to the internet, despite the dependence which the country has on the internet for social and economic stability speaks of the priorities inherent in the governance structure. Arguably, dissemination of information, whether factual or inaccurate tends to be seen by the government as a security threat, showing a lack of preparedness in dealing with situations of on-ground insecurity.

The example of India's internet shutdown practices shows that both, democratic and authoritarian regimes can practice authoritarian in digital governance. The archaic laws which support these structures show a lack of willingness to change old structures of relationship between technology and governance. Regardless of how outdated laws and practices impact populations, the government seems to stick to the convenience of carrying on traditions which help in retention of power. This stands true for government at the centre as well as in the states, considering the proclivity of internet shutdowns within both jurisdictional frameworks.

V

Case Studies: Dealing with Shutdowns as Authoritarian Practices

The following section presents case studies of two countries, which have suffered blanketed internet blackouts in recent years. Both the countries are in the continent of Africa and both the countries underwent a transfer of power under difficult circumstances. Both the countries also faced the possibility of a new era of liberal digital governance to be ushered in following regime change but only one of them seems to be on the road to succeed in liberating the internet.

The first case study is of Ethiopia under the leadership of Prime Minister Abiy Ahmed, who took over from Hailemarian Desalegn after mass protests and civil unrest forced him to give up office. Contrary to the incumbent Prime Minister's initial responses regarding freedom of expression on the internet and digital rights of citizens, the intensity of internet shutdowns during protests saw an increasing turn with repression tactics normalized in order to stifle dissent. This case draws on the length and intensity with which Ethiopia has been practicing internet shutdowns and what lead to a failed attempt at restoring liberation technology as a practice in digital governance.

The second case study is that of Zimbabwe, which was under threat of turning into a digital island under Robert Mugabe's government but managed to take the path of digital progress. Shutdowns occurred both, during and after Mugabe's rule in the country but some changes in the international digital policy landscape and internal struggle for freedom of expression changed the course that online governance was about to undergo. Breaking away from an authoritarian leader, who cracked down on individual instances of online dissent and idolized the Chinese model of internet regulation, the Zimbabwean public demanded their rights to access the internet.

Revisiting Digital Authoritarianism: Ethiopia

Ethiopia, having Africa's second largest population and one of its fastest growing economies takes a centre stage in the continent's political ecosystem. The state of repression in Ethiopia is an old phenomenon, rooted in the past quarter century of serious political and human rights violations leading up to the end of Prime Minister Desalegn's official term

(OHCHR, 2018). Arrests of Journalists, detention and killings of opposition groups and media propaganda are coupled with the tendency for the state to impose blanketed internet shutdowns over extended periods of time, leading the nation into a state of repression. Since the swearing in of Prime Minister Abiy Ahmed in April 2018, marking the end of the state of emergency in the country, a new era of renewed information freedoms and civil rights was expected. At the assumption of his office, the Abiy government released imprisoned journalists, activists, and government opposers as a mark of liberating civil society organizations and putting an end to regime censorship.

The "Utopian-Ethiopia" narrative was a short-lived dream, however, considering the massive internet shutdowns and repressive measures undertaken by the state in the following years. Following a failed coup attempt and the assassination of East African national Army's chief, the Prime minister, in no uncertain terms shut down the internet in the country, citing the spread of "deadly content" on social media (Ayalew, 2019). His discontent was further elaborated by his statement, where he threatened to "cut off the internet forever" if incitement to violent unrest continues. This was the first time since the end of Desalegn's term that the internet was shut down for reasons other than exam cheating.

In the following months since, there have been several internet shutdowns in response to opposition, criticisms, protests, and conflicts. The July 30th nationwide internet shutdown was an unprecedented act on the part of the government, which, less than two years prior had sworn to protect the internet against censorship and blocking. The ongoing unrest In the Oromo region, which had witnessed armed conflict and public demonstrations against the government's human rights violations (UN Security Council*: End Inaction on Ethiopia* (2021), took a national centre stage with the killing of celebrity musician Haacaaluu Hundessaa. The public anger was witnessed in the form of mass protests across the nation including in the capital, Addis Ababa as connective action over social media platforms propagated a mobilizing narrative of state repression. The government's instant response to the rising discontentment was to enact a full-blown internet blackout in the country for sixteen days while most of the nation remained disconnected to the world (Access now, 2020a). The unrest caused by the death of Hundessaa resulted in violent communal clashes in the Oromiya region, where much of the violent outbreaks took place before shutdowns were imposed, causing over 200 deaths as per reports (Freedom House, 2020). The internet was restored partially, with throttled speeds on July 14, 2020, but the chances of sustained shutdowns in the future loomed overhead.

The tendency for the incumbent Ethiopian regime to enact blackouts is clear form their past implementation, most of which are enacted for political reasons. Sometimes blanketed shutdowns in the country last over periods of months in certain regions. A two-month long internet shutdown crippled the opposition and put muzzles on the freedom of journalistic expression between January and March of 2020 (***UN Security Council**: End Inaction on Ethiopia* (2021). The shutdown enacted in the western Oromia region, West Wellega and Horo Gudru Wellega zones was imposed under federal military control during military incursions against the Oromo Liberation Front (Ayalew, 2019), an insurgent group fighting for the civil and land rights of Oromia. Three decades after the act of expressing dissent against the Zenawi and Desalegn governments was criminalized, the Ethiopian forces resorted to taking steps to ban OLF and its supporters. Reports have verifiably claimed that at least 59 civilians were killed on the 24th of January 2020 in the Anfilo Woreda district of the Kellem Wellega zone, while the OLF brought another 21 names to light form the Gidami district of the Kellem Wellega zone on the 30th of January (Ethiopia Inside, 2020).

The prolonged internet blackouts in the region meant that only limited amounts of information on actual ground realities could be communicated. There were no explanations provided for the internet blackout until the 3rd of February, when the federal government only described “security reasons” as justifications for the measure (OHCHR, 2020) Despite the government’s repressive tactics, the political wing of the OLF has maintained its stance on regional autonomy and registered to compete in the state elections but the government’s stance against the OLF has ensured their inability to contest in democratic process under the current Command Post rule (Ethiopia inside, 2020).

The Ethiopian government, which promised liberation and freedom of expression in 2018 unprecedentedly turned into an authoritarian state in the following year. The governments Advisory council had drafted Media Proclamations immediately after Abiy’s assumption to office, decriminalizing defamation, proclaiming autonomy to the national media, and ensuring safeguards against corruption of the Ethiopian Media Authority’s board members (OHCHR, 2020). This was regarded as a liberating move, considering the infringements on human rights and free speech which have marred the nation’s recent history. Instead, the onset of Abiy’s regime featured anti-terrorism laws restricting freedom of speech online as a measure to halt disinformation and hate speech (Freedom House, 2020). Journalists and overwatching non-governmental organizations were not barred from these laws, considering the tendency for the Ethiopian government to misappropriate legal privileges. The government’s Anti-Terrorism proclamation, which came with enhanced surveillance powers granted to the National Intelligence unit were weaponized against journalists and activists during outbreaks of violence (OHCHR, 2020). Five journalists are known to have been arrested on the 27th of January 2020, following criticisms against the government in dealing with the Oromo insurgency (Ethiopia Inside, 2020). Despite facing heavy criticism for the infringement on media freedoms, the government did not release the journalists or retract the charges.

Until April 2018, large scale protests and demonstrations were regularly followed by internet shutdowns as practices. The protests and subsequent shutdowns were resultant of the government's plans for appropriating land from the Oromo people in a bid to expand the national capital of Addis Ababa (Freedom House, 2020). Mobile internet services were regularly disrupted, and broadband services were throttled under the previous regime. The resignation of Desalegn, although seen as a welcome sign, resulted in a state of emergency coupled by internet shutdowns until Abiy was sworn in as the next Prime Minister. The tendency for shutdowns to be enacted so quickly could be attributed to the comparably low impact of shutdowns on the population. A broadband penetration rate of 15 percent and a mobile phone penetration rate of 44 percent means that majority of the population will remain unaffected by communication disruptions.

The underdeveloped internet infrastructure in Ethiopia was always a cause for concern with respect to liberation technology to take foot. Being a landlocked country, Ethiopia does not have direct access to underwater fibreoptic cable networks. The internet infrastructure that they do have is mostly satellite based receptors and two fibreoptic cable systems which pass through Sudan in the east and Djibouti in the north-eastern border (International Telecommunication Union, 2020). The lack of rigid internet infrastructure and the low penetration rates within the country result in a weak internet economy, causing shutdowns to be less impactful on the day-to-day livelihoods. Prime Minister Abiy expressed with no hesitation that his intentions to implement shutdowns in the future were unproblematic to his government, stating that his desire to develop Ethiopia does not triumph the need for public order and that the internet is “neither water nor air” (ABC News, 2020).

It is interesting to observe that the regime which was presupposed as a liberating force turned to authoritarianism at the first instance of instability. Despite the overthrow of Desalegn, authoritarianism continued in Ethiopia within the same outlines. The change in actors performing the action had shifted focus away from the practice of repression institutionalized in the regime. New regimental authorities, who promised liberalized digital governance, adopted repression technology due to the prevalence of institutionalized authoritarian practices. The continued popularity of repression technology in Ethiopia gives evidence to the tendency for practices to continue despite the change in actors if underlying authoritarian structures remain. By observing the action performed instead of the actor, practice theory shines the light on instances of kill-switch shutdowns in Ethiopia to prove that repression technology can be used as an authoritarian tool regardless of the regime in power as long as authoritarian practices are continued to be legitimized.

Hope for Liberation Technology: Zimbabwe

On 15th of January 2019, Zimbabwe's latest blanket internet shutdown was implemented (Netblocks Report, 2020). The move came after civilian protesters took to the streets in response to rising fuel prices in the country, which touched upwards of a 105 percent (Reuters, 2020). The violence which consequently broke out during the protests was attributed to an economic down-trend coupled with grievances against the President Emmerson Mnangagwa led government. The government's response was heavily criticized by opponents and dissidents, comparing the step to authoritarian practices under the regime of President Robert Mugabe. The effect of the shutdown caused a dip in Mnangagwa's approval ratings and his former links to Mugabe were augmented in public eye. Opposition forces to the government did not let go of any opportunity to criticize Mnangagwa's past as a high-ranking official under Robert Mugabe's authoritarian regime (Centre for Policy and Research Analysis, 2019). In this way, the shutdown strategy backfired for the incumbent president owing to the retaliatory effects of disconnective action. Critics accused the President of attempting to sweep security clampdowns under the rug and hide authoritarian practices from the world by disconnecting the internet (Reuters, 2020). Although connections were partially restored on the 16th of January, another full internet shutdown was imposed subsequently, which lasted until the 24th of January (Access Now, 2019). The shutdown impacted the lives and livelihoods of over 17 million citizens and was implemented as a blanketed blackout across the nation.

Zimbabwe has had a long history of repression throughout the Mugabe regime, which lasted for more than three decades and is still fresh in the minds of the Zimbabwean people. Which is why when the shutdown directives came from the Minister of State for National Security in the President's Office **(Access Now, 2020)**, civil society organizations and activists were quick to take notice. The Zimbabwe High court subsequently ruled against the Minister's decision of shutting down the internet, stating that his office does not hold the authority to implement such directives and that this move was illegal. The shutdown was consequently lifted, and full internet speeds were restored immediately following the verdict. This legal victory against the government came as a ray of hope for activists and media organizations who challenged the government's authoritarian measure. The lawsuit was filed by the Media Institute of South Africa (MISA- Zimbabwe) and human rights Lawyers arguing the case against implementation of authoritarian practices over the internet (Access Now, 2020). This ability for the legal structures to reprimand governments for misuse of authority is a sign of progress in the face of authoritarianism. In March 2020, Zimbabwe's telecom regulator, Postal and Telecommunications Authority of Zimbabwe (POTRAZ) made assurances for the proliferation of digital rights in the country, stating that uninterrupted communication services will be afforded to the public throughout the Covid-19 lockdown period and beyond.

Part of the reason why internet governance in Zimbabwe is taking a turn towards digital freedoms is due to the history of censorship in the country under Mugabe's rule. Administrators of Facebook pages, journalists and whistle-blowers were regularly reprimanded for speaking out under the regime. In July 2014, one journalist, running a whistle-blowing webpage as an anonymous administrator had incurred a bounty of over US$ 300, 000 for anyone who reveals their name, while one Facebook user was arrested earlier that same year for sharing a post claiming that the president had died (CIPESA, 2016). Dissent was punished under the rule of Mugabe as in any other authoritarian state, reprimanding dissidents for speaking out. The state's internet governance model was brought to question more frequently after the passing of the UN resolution on the Universal Declaration of Human Rights and the International Covenant on Civil and Political rights. On the 1st of July 2014, 70 states co-signed the declaration, affirming that the need to protect freedoms of expression of citizens online was just as important as protecting them offline (Mare, 2020).

5 days following the declaration, of which Zimbabwe was not a co-signee, shut-in protests took root in the capital Harare. As a response to rampant corruption at the highest levels of governance and mismanagement of public funds under the Mugabe regime, business and places of work decided to remain closed across the capital (Access Now, 2016). The protest took effect on the 6th of July, leaving streets empty and no room for crackdowns to be initiated. As a response, the government ordered ISPs in Zimbabwe to shut down the internet. This was heavily criticized as an authoritarian move against peaceful protesters in the absence of violence. Major ISPs operating in the country including Liquid Telecom Zimbabwe, Telcel,

TelOnem, ZOL and Econet were pressured into shutting down access to their services despite forecasts of facing heavy losses owing to the move (Znews 2016). Meanwhile the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) issued statements detailing warnings against "gross irresponsible use of social media and telecommunication services" (Access Now, 2016). The move was seen by the public as an attempt at stifling free speech and expressing discontentment against the regime.

The repressive online climate was not a novel phenomenon for the people of Zimbabwe as authoritarian plans were being formulated for a long time to control the internet. In a statement issued by President Mugabe in April 2016, the plans for building an internet firewall resembling that of China's was emphasized upon. The "great firewall of Zimbabwe" was imagined emulating the Chinese internet filtration system, restricting access to some websites while creating a nation-wide web for the country. Mugabe's plans on initiating the process for developing such an internet were clear form his statement "The Chinese have put in place security measures, and we will look at these so that we stop these abuses on the internet." (Kabweza, 2016). The end of Mugabe reign in 2017 inevitable came about as his popularity and political support began to waver while incendiary information and criticism could not be curbed anymore.

The tendency for the Zimbabwean government to implement shutdowns, although not extinguished, is still contested to the point of challenging the regime. As long as responsive measures are adopted by the legal authorities, government practices can be kept in check. The shutdowns initiated in 2019 under President Mnangagwa's government were marred by violence. Police crackdown on protesters caused at least three deaths in official figures, whereas human rights groups and lawyers suggest at evidence pointing towards at least a dozen deaths, several more wounded by police ammunition and hundreds of detainments (Dzirutwe, 2019). Public dissent in this case was translated into legal action against the state, holding the government accountable for repressive tactics and demanding answers for imposing disproportionate censorship measures.

Censorship over the internet and blanketed shutdowns since then then have reduced but not disappeared. Despite the Postal and Telecom Authority's assurances that internet freedoms would be upheld and access to information online would be unrestricted during the pandemic, there were at least two instances of shutdowns recorded. Netblocks (2020) recorded data on internet disruptions on the 30th and 31st of July 2020, when two-day internet disruption took place. The state-owned telecommunications service, TelOne was the only network affected during the disruptions, wherein one large and one small scale disruptions were observed. The restriction of internet services coincided with planned protests in support of detained opposition leaders, who came out to voice opinions against the president despite city-wide lockdowns being implemented (Mayo and Kingsley, 2020). The impact of disruptions, however, were significantly lower in comparison to previous blackouts. There were no total communications blackouts reported and privately owned ISPs were entirely unaffected by the move, providing full coverage across the country (Netblocks, 2020).

The power of collective action while facing authoritarian practices in the case of Zimbabwe proves that subversion of repressive practices is possible if authoritarianism is opposed through activism as well as through legislation. Even though Zimbabwe's internet infrastructure could very likely have followed the repression technology model of governance and Mugabe, in his prime, might have been intent on creating an exclusive online presence like that of China, digital authoritarianism was circumvented. The evolution of liberation technology, which is hopefully taking root in the nation will only continue to be a harbinger of citizens' rights as long as awareness of the state's capacity for practicing authoritarianism is not forgotten. Even if regime practices have changed since Mugabe's three-decade tenue in office, the structural framework remains. An authoritative government is only as strong as its ability to suppress dissent. The dynamics of collective action on the streets coupled with connective action on the internet in Zimbabwe is a testament to the fact that repression technology can be circumvented through mobilization. As long as offices of state institutions are occupied by conscientious citizens willing to represent freedoms of the people that they serve, evolution in inclusive digital governance will continue.

Conclusion

The research conducted in this project has revealed has been useful in finding correlations between internet shutdowns and protests. The fact that cases illustrated in this research revealed that shutdowns were mostly initiated as measures intended at silencing dissenting masses instead of protecting them shows the need for incumbent regimes to practice control over citizens. One off internet shutdown in most cases have shown to be within justifiable limits, considering the fact that they are implemented under special circumstances nut internet shutdowns as practices constitute repressive measures, which are signs of authoritarian control.

The case of India has revealed that democratization of state does not necessarily translate to freedoms in the digital sphere. In order to welcome cyberspace into the realm of possibilities for development, acceptance of digital rights as parts of human rights need to be addressed. The fact that entire economies and societies depend on information technology for their existence should be a clear indication for states to indulge in more inclusive governance practices in the digital sphere.

The case of Zimbabwe and the 2019 internet shutdown following protests in the capital show that despite authoritarian control, states have the ability to implement change through citizen participation. The involvement of all actors and stakeholders in the digital sphere within a country need to have a say in the implementation of laws and practices. International communities have pointed at a more inclusive digital space but the participation of all governments within the discourse is necessary. The socio-economic development of a country depends on its levels of connectivity with other economies and transnational entities. In order to allow a freer internet to grow, indicators on authoritarianism need to be monitored to understand the directions that countries could take towards enabling digital freedoms or digital repression.

Identifying Digital Authoritarianism

The interest that governments show in controlling or freeing the internet depends on what stakes they have concerning the freeing or throttling of online communications. A good measure of gauging whether shutdowns are justifiable or repressive is whether governments issue justifications in the form of laws or narratives (Ayalew, 2019). A legally sound justification will cite exact reasons and proportionality of intended shutdowns along with detailed chronology of implementations. Justifications including “National security”, “war on terror" and "stopping misinformation" are broad enough to include any scenario deemed fit for disproportionate retaliatory measures. It is important for citizens to know if their governments are imposing shutdowns for specific reasons or simply practicing control over a domain of free speech to question the practice. This research has used the practice theory benchmark (Bueger and Gadinger, 2015) to illustrate how studying repeated authoritarian actions can help underpin patterns of repression in governance.

In the context of India, archaic legislations drafted in the 17th century are used to justify impositions of restrictions on 21st century technology (Bhardwaj et al., 2019). Not only are the outdated laws repressive but also subversive of evolving communication technologies. The vagueness of IT laws and the power of authority in the hands of government increases the tendency for shutdowns to be implemented. Despite falling within the category of democratic states, regressive laws in India invariably lead to incumbent regimes abusing such power in an authoritarian manner. Freedom of expression is a constitutional right afforded to every citizen, yet expressions of discontentment yield dire consequences online and offline. An underlying cause for extreme measures such as internet shutdowns to be imposed is the fragility of regime stability in a country (Howard, Agarwal and Hussain, 2015). Due to the diverse political climate in India, several factions of dissidents mobilize to express their grievances simultaneously. India has a long history of protests and governments understand the dynamics of dissent in the country, which is why legal ambiguity regarding stifling free speech is a useful smokescreen to mask repressive intentions. A regime's stability depends upon the perception of control. The inability to quell oppositional challenge leads to detrimental effects on a regime's perception management. Even though vague narratives such as "war on terror" and "national security" leave room for speculations, they send a clear message of the incumbent regime's preparedness to take resilient steps amidst turbulent times (Ayalew, 2019).

The Ethiopian case demonstrates how authoritarianism can be implemented regardless of who the actors are. A regime, which inherits a broken state will face challenges left behind by the previous government along with the authoritarian structures. Structures which have worked in the past are likely to work in the future as well, provided that the channels of implementation remain intact. Despite making promises for liberating the internet, the government resorted to repressive measures, owing to the growing opposition challenging the regime stability. Government control over the digital space in Ethiopia can be attributed to three factors: 1). The lack of diversity in the internet infrastructure; There are very few physical lines of communication present in the country, providing fewer opportunities for diversification in the market. 2). The incumbent regime is the primary service provider; Internet exchange points need to be more distributed and numerous to allow for more diversity in service options. Higher proportions of internet connection along bordering states also increases chances for a diversified market, considering citizens living along the border could potentially choose to connect to foreign networks (Panicker, 2020). 3). Low internet penetration rates; A population with higher penetration rates would be dependent on the internet for their economic and social wellbeing whereas an economy with lower penetration rated would have developed means to base their economic and social activity separated from it. The Ethiopian government presented double digit growth figures in GDP despite internet shutdowns being in place as justifications for the proportionality of shutdown measures (Ayalew, 2019).

In the final case presented in this research, a shift towards liberalization of the internet infrastructure resulted in more democratic practices and better freedoms afforded to citizens in Zimbabwe. The liberation technology model, which is taking foot in the country is a result of several factors including active participation by all the stakeholders involved in governance of the country's digital space. The discontentment of citizens against the state's authoritarian practices coupled with active participation of civil society and legal institutions acted as correcting mechanisms, limiting the state's unprecedented control over the internet. The case of Zimbabwe is unique considering the authoritarian past which the country has overcome. Factors impacting Zimbabwe's internet freedoms towards a more liberalized direction are: 1). Diversification of service providers. The state owns only one amongst many ISPs in the country, which paves a path for fair competition in the market. A diversified internet infrastructure translates to higher stability in online governance. 2). The primacy of legality over governance. The ability for a state to reprimand its government for overstepping constitutional boundaries sets a precedent for future governance. A regime which does not hold absolute authority over the state would remain within the lines of duty to retain power. 3). Active media participation. During the 2019 shutdown in Zimbabwe, the news media and civil society organizations played an important role in highlighting the government's misappropriation of power. An active citizen machinery and institutional cross checks ensure accountability from regimes. The Zimbabwean model of connective action worked because of active participation by all stakeholders in the country's digital infrastructure.

Protests and Violence as Covert Authoritarian Tools

Participation in Public discourse should be a right granted to every citizen within a state. Criticism of the government is the backbone of any democratic nation. Under repressive states, even if the legality for participating in protests is contested, the means of organisations are always present. Dissent finds a way to seep out from the undercurrents in the face of oppression. People tend to find strategies to adapt to mechanisms of mobilization under conditions of information scarcity and infringed information arenas (Rydzak, Karanja and Opiyo, 2020). The connective action paradigm ensures the tendency for human beings to find alternatives to disruption of communication channels. In the face of censorship, new faces of leadership emerge from the fringes every time authoritarian practices are imposed (Hassanpour, 2017). Even though repression technology invariably leads to decentralization of demonstrative capabilities in a population, pockets of resistance tend to emerge at times of uncertainty. Instances of revolution taking off in the face of repression can be observed in modern history through the examples of the Arab Spring, the Orange Revolution in Ukraine, and Iran's Green Revolution (Ruijgrok, 2017).

A major drawback of decentralized protests, however, is the likelihood of movements turning violent in the absence of organizational structures. Violent movements endanger the lives and causes of citizens who demand change. The effectiveness of retaliatory violence depends upon the capabilities of a regime to manage conflicts. Against a strong military infrastructure, violent movements tend to end badly for dissenters. Governments that are aware of this knowledge could use violent action as justification for incurring authoritarian measures in response. Implementing internet shutdowns during violent demonstrations works as a double-edged sword in the hands of authoritarian regimes. Disconnecting the communication infrastructure decentralizes mobilization efforts as well as hides information of extreme measures from international scrutiny during retaliatory operations (Gohdes, 2015). The cases of mass killings in Ethiopia during protests in the past half century are testaments to unchecked authoritarian power over communication networks (Gohdes, 2020). A government that is concerned about international reputation would commence violent actions after shutdowns are imposed in order to delegitimize claims of authoritarian practice (Rød and Weidmann, 2015).

The future of research on the relationship between digital authoritarian controls and the nature of collective action can make use of observations presented in this research concerning the tendency for mass movements to turn viral over the internet. Such liberation of information turns to be detrimental to autocracies and authoritarian regimes concerned with retention of power. Bu understanding the impact that digital communications have due to the expediency of information flows coupled with the propensity for peer-to-peer communication on a global scale sheds light on why regimes fear the power of connective action. In conclusion, by studying mechanisms of authoritarianism as it is practiced over the digital space, future research can determine the levels of freedom individuals enjoy in the offline space as well. This research would help in making a start for closing the gap between human rights as they are perceived and as they should be perceived for the future of an interconnected world.

References

Amnesty International (2020) ‘A Web Of Impunity: The Killings Iran’s Internet Shutdown Hid’, *Amnesty.org*.

Access Now. (2019) '*Targeted, cut off, and left in the dark: The #KeepItOn report on Internet shutdowns in 2019*', *Access Now,* Available at: https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf

Access Now (2020) 'Back in the dark: Ethiopia shuts down internet once again', *Access Now*, Available at: https://www.accessnow.org/back-in-the-dark-ethiopia-shuts-down-internet-once-again/.

Adler, E. and Pouliot, V. (2011) 'International practices. *International theory'*, *3*(1), pp.1-36.

Al Jazeera (2019) 'Zimbabwe imposes internet shutdown amid crackdown on protests', *Al Jazeera*, Available at: https://www.aljazeera.com/news/2019/1/18/zimbabwe-imposes-internet-shutdown-amid-crackdown-on-protests.

Ayalew, Y. E. (2019) ‘The internet shutdown muzzle(S) freedom of expression in ethiopia: Competing narratives’, *Information and Communications Technology Law*, 28(2), pp. 208–224. doi: 10.1080/13600834.2019.1619906.

Bennett, W. L., & Segerberg, A. (2013) 'The logic of connective action: Digital media and the personalization of contentious politics', *Cambridge, UK: Cambridge University Press*.

Bhalla, G. (2021) *Farmers Take The Protest To Parliament: Here's Everything That Has Happened So Far*, *IndiaTimes*. Available at: https://www.indiatimes.com/news/india/farmers-protest-parliament-overall-updates-545559.html (Accessed: 3 August 2021).

Bhatia, R. (2017) *Growing unease as India curbs the net to keep the peace*, *mint*. Available at: https://www.livemint.com/Politics/t13L9GsLYgMHzoXZNj7L6J/Growing-unease-as-India-curbs-the-net-to-keep-the-peace.html (Accessed: 29 July 2021).

Bigo, D., & Tsoukala, A. (2008) 'Understanding insecurity. In D. Bigo & A. Tsoukala (Eds.)', *Terror, insecurity and liberty: Illiberal practices of liberal regimes after 9/11* (pp. 1–9). Oxford, UK: Routledge.

Boas, Taylor C. (2006) 'Weaving the authoritarian web: The control of Internet use in nondemocratic regimes, '*In: John Zysman & Abraham Newman (eds) How Revolutionary Was the Digital Revolution? National Responses, Market Transitions, and Global Technology',* Stanford, CA: Stanford University Press, 361–378.

Bob, C. and Nepstad, S. (2007) "Kill a Leader, Murder a Movement? Leadership and Assassination in Social Movements", *American Behavioral Scientist*, 50(10), pp. 1370-1394. doi: 10.1177/0002764207300162.

Bhandari, V. and Sane, R. (2016) "Towards a Privacy Framework for India in the Age of the Internet", *SSRN Electronic Journal*. doi: 10.2139/ssrn.2892368.

Brooks, L. L. Z. and Johnston, J. (2017) 'Through A Glass, Darkly: Everyday Acts of Authoritarianism in the Liberal West ARNE', *Jm*, (July), pp. 1–55.

Bueger, C., & Gadinger, F. (2015) 'The play of international practice', *International Studies Quarterly*,*59*(3), 449–460. doi:10.1111/isqu.12202

Congo holds presidential elections under media blackout (2021). Available at: https://www.aljazeera.com/news/2016/3/20/congo-in-media-blackout-for-presidential-elections (Accessed: 3 August 2021).

Davenport, C. (2010) *State repression and the domestic democratic peace*. Cambridge, UK: Cambridge University Press.

Deibert, Ronald J. (2003) 'Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace', *Millennium* 32(3): 501–30.

Deleure, F. (2020) *Cyver Operations and InternetionalL Law*. [S.l.]: Cambridge Univ Press.

Diamond, L. (2010) 'Liberation technology*', Journal of Democracy, 21(3), pp.69-83.*

Dragu, T. and Lupu, Y. (2021) 'Digital Authoritarianism and the Future of Human Rights', *International Organization*, (October). doi: 10.1017/S0020818320000624.

The Economic Times (2019b) *What is CAA, Citizenship Amendment Act? What is it and why is it seen as a problem? Everything you need to know.*, *The Economic Times*. Available at: https://m.economictimes.com/news/et-explains/citizenship-amendment-bill-what-does-it-do-and-why-is-it-seen-as-a-problem/articleshow/72436995.cms (Accessed: 3 August 2021).

Erixon, Fredrik; Lee-Makiyama, H. (2011) ‘Digital authoritarianism: Human rights, geopolitics and commerce’, *European Centre for International Political Economy (ECIPE), Brussels*, p. 24.

Franck, T. (2003) "What Happens Now? The United Nations After Iraq", *American Journal of International Law*, 97(3), pp. 607-620. doi: 10.2307/3109846.

Freedom House. (2015)"*Ethiopia: Country Profile* "Available at: https://freedomhouse.org/country/ethiopia (Accessed: 3 August 2021).

Freyburg, T. and Garbe, L. (2018) ‘Blocking the Bottleneck: Internet Shutdowns and Ownership at Election Times in Sub-Saharan Africa’, *International Journal of Communication*, 12, pp. 3896–3916.

Garrett, K. R. (2006) "Protest in an Information Society: a review of literature on social movements and new ICTs", *Information, Communication & Society*, 9(2), pp. 202-224. doi: 10.1080/13691180600630773.

Gerbaudo, P. (2013) ‘The “Kill Switch” as “Suicide Switch”: Mobilizing Side Effects of Mubarak’s Communication Blackout’, *Westminster Papers in Communication and Culture*, 9(2), p. 25. doi: 10.16997/wpcc.165.

Glasius, M. (2018) 'What authoritarianism is: A practice perspective', *International Affairs*, *94*(3), 515–533. doi:10.1093/ia/iiy060

Glasius, M. and Michaelsen, M. (2018) ‘Illiberal and Authoritarian Practices in the Digital Sphere’, *International Journal of Communication*, 12(323899), pp. 3795–3813.

Gohdes, A. R. (2020) ‘Repression Technology: Internet Accessibility and State Violence’, *American Journal of Political Science*, 64(3), pp. 488–503. doi: 10.1111/ajps.12509.

Goldsmith, J. (1998) 'Against cyberanarchy. University of Chicago Law Review', 1199(fall), 1217–1222.

Goodwin, J. (2018) "Leading from the Periphery and Network Collective Action. By Navid Hassanpour. Cambridge: Cambridge University Press, 2016.", *The Journal of Politics*, 80(3), pp. e65-e66. doi: 10.1086/697938.

De Gregorio, G. and Stremlau, N. (2020) ‘Internet Shutdowns and the Limits of Law’, *International Journal of Communication*, 14(716686), pp. 4224–4243.

Grinberg, D. (2017) ‘Chilling developments: Digital access, surveillance, and the authoritarian dilemma in Ethiopia’, *Surveillance and Society*, 15(3–4), pp. 432–438. doi: 10.24908/ss.v15i3/4.6623.

Hachalu Hundessa: 'Eighty-one killed' in protests over Ethiopian singer's death (2021). Available at: https://www.bbc.com/news/world-africa-53243325 (Accessed: 3 August 2021).

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

Howard, P., Agarwal, S. and Hussain, M. (2011) "The Dictatorss Digital Dilemma: When Do States Disconnect Their Digital Networks?", *SSRN Electronic Journal*. doi: 10.2139/ssrn.2568619.

India: Freedom on the Net 2020 Country Report (2020) *India: Freedom on the Net 2020 Country Report | Freedom House*, *Freedom House*. Available at: https://freedomhouse.org/country/india/freedom-net/2020 (Accessed: 3 August 2021).

India: Vigilante ‘Cow Protection’ Groups Attack Minorities (2019). Available at: https://www.hrw.org/news/2019/02/19/india-vigilante-cow-protection-groups-attack-minorities (Accessed: 3 August 2021).

Johnson, M. (2011) 'Knocking over entire web systems“. *The “internet kill switch” debate*', The Economist, Available at: https://www.economist.com/multimedia/2011/02/10/knocking-over-entire-web-systems.

Joyner, C. (2001) "Information Warfare as International Coercion: Elements of a Legal Framework", *European Journal of International Law*, 12(5), pp. 825-865. doi: 10.1093/ejil/12.5.825.

Katyal, N.K. (2001) 'Criminal law in cyberspace', *University of Pennsylvania Law Review*, *149*(4), pp.1003-1114.

Kedzie, C. (1997) 'Communication and democracy: Coincident revolutions and the emergent dictator’s dilemma (RAND dissertation)', *Santa Monica, CA: RAND Corporation,* Available at: http://www.rand.org/publications/RGSD/RGSD127/sec2.html.

Kumar, R. and Thapa, D. (2014) "Social media as a catalyst for civil society movements in India: A study in Dehradun city", *New Media & Society*, 17(8), pp. 1299-1316. doi: 10.1177/1461444814523725.

Lindberg, S. (2004) "The Democratic Qualities of Competitive Elections: Participation, Competition and Legitimacy in Africa", *Commonwealth & Comparative Politics*, 42(1), pp. 61-105. doi: 10.1080/14662040408565569.

MacKinnon, R. (2011) 'Liberation Technology: China's "Networked Authoritarianism"', *Journal of Democracy*, 22(2), pp. 32–46.

Maher, K. and York, J.C. (2016) 'Origins of the Tunisian Internet', In *State Power 2.0* (pp. 33-46). Routledge.

Marchant, E. and Nicole, S. (2020) 'A Spectrum of Shutdowns: Reframing Internet Shutdowns From Africa', *International Journal of Communication*, 14(716686), pp. 4327–4342.

Marchant, E. and Stremlau, N. (2020) 'The Changing Landscape of Internet Shutdowns in Africa: Introduction', *International Journal of Communication*, 14(716686), pp. 4216–4223.

Mare, A. (2020) 'State-Ordered Internet Shutdowns and Digital Authoritarianism in Zimbabwe', *International Journal of Communication*, 14, pp. 4244–4263.

Marquis-Boire, M., Marczak, B., Guarnieri, C., & Scott-Railton, J. (2013, May 1), 'For their eyes only: The commercialization of digital spying', Toronto, Canada: *Citizen Lab and Canada Centre for Global Security Studies*, Available at: https://citizenlab.ca/storage/finfisher/final/fortheireyesonly.pdf

Mawii, Z., Srivastava, R., Lal, S. and Abraham, B.P. (2018) 'Kept in the dark: Social and psychological impacts of network shutdowns in India', Digital Empowerment Foundation. Available at: *http://defindia.org/wp-content/uploads/2018/02/Kept-in-the-Dark.pdf*.

Micek, P. and Access Now. (2017) 'Shutdown tracker optimization project here', Available at: https://www.accessnow.org/cms/assets/uploads/2017/09/Shutdown-Tracker-Optimization-Project.xlsx

Mir, S. (2021) *J&K Internet Shutdown Based on 'Dubious' Legal Framework: Report*, *The Wire*. Available at: https://thewire.in/government/jammu-and-kashmir-internet-shutdown-jkccs (Accessed: 3 August 2021).

Narrain, S. (2018). Internet shutdowns: Amendment to the Telegraph Act and mobile company licenses. *Socio-Legal Review*. National Law School of India University, Mar 20.

NGOs in India (2018). Available at: http://www.indianngos.org/Default.aspx (Accessed: 30 July 2021).

Nordås, R. and Davenport, C. (2013) "Fight the Youth: Youth Bulges and State Repression", *American Journal of Political Science*, p. n/a-n/a. doi: 10.1111/ajps.12025.

Ogundeji, O. (2018) 'Internet shutdown as Sierra Leone votes. *IT Web*', Available at: https://itweb.africa/content/rW1xLv59KZjvRk6m.

OpenNet Initiative. (2019) 'Saudi Arabia', *Saudi Arabia | OpenNet Initiative*. Available at: https://opennet.net/research/profiles/saudi-arabia [Accessed March 10, 2021].

Office of the United Nations High Commissioner for Human Rights and the Ethiopian Human Rights Commission (2018) *OHCHR | Ethiopia: The Office of the United Nations High Commissioner for Human Rights and the Ethiopian Human Rights Commission to conduct a joint investigation with a view to a credible accountability process*, *Ohchr.org*. Available at: https://www.ohchr.org/EN/HRBodies/HRC/Pages/NewsDetail.aspx?NewsID=26949&LangID=E (Accessed: 3 August 2021).

Sodhi, J. (2020) *The Article 370 Amendments on Jammu and Kashmir: Explaining the Global Silence | ORF*, *ORF*. Available at: https://www.orfonline.org/research/article-370-amendments-on-jammu-and-kashmir/ (Accessed: 3 August 2021).

Pandey, G. (2019) *Article 370: India strips disputed Kashmir of special status*, *BBC News*. Available at: https://www.bbc.com/news/world-asia-india-49231619 (Accessed: 3 August 2021).

Panicker, R. (2020) "Internet Shutdown: Is It Violation of Fundamental Rights?", *SSRN Electronic Journal*. doi: 10.2139/ssrn.3667818.

Pearlman, W. (2012) "Precluding Nonviolence, Propelling Violence: The Effect of Internal Fragmentation on Movement Protest", *Studies in Comparative International Development*, 47(1), pp. 23-46. doi: 10.1007/s12116-012-9099-2.

Pierskalla, J. and Hollenbach, F. (2013) "Technology and Collective Action: The Effect of Cell Phone Coverage on Political Violence in Africa", *American Political Science Review*, 107(2), pp. 207-224. doi: 10.1017/s0003055413000075.

Pundir, P. (2021) *How Indian Protesters Are Taking News Into Their Own Hands*, *Vice.com*. Available at: https://www.vice.com/en/article/g5ba8m/india-farmer-protests-secret-bylines-anonymous-alternative-media-resistance (Accessed: 3 August 2021).

Records of the General Conference. (2013, November) '37th Session'*, UNESCO. Paris, France,* Available at: http://unesdoc.unesco.org/images/0022/002261/226162e.pdf .

Ren, X. (2016) "Land acquisition, rural protests, and the local state in China and India", *Environment and Planning C: Politics and Space*, 35(1), pp. 25-41. doi: 10.1177/0263774x16655802.

Roberts, M. E. (2018) 'Censored: Distraction and diversion inside China's Great Firewall', *Princeton, NJ: Princeton University Press.*

Rød, E. G. and Weidmann, N. B. (2015) 'Empowering activists or autocrats? The Internet in authoritarian regimes', *Journal of Peace Research*, 52(3), pp. 338–351. doi: 10.1177/0022343314555782.

Rydzak, J. (2019) 'Of Blackouts and Bandhs : The Strategy and Structure of Disconnected Protest in India', *Global Digital Policy Incubator, Stanford University*, pp. 1–54.

Rydzak, J., Karanja, M. and Opiyo, N. (2020) 'Dissent Does Not Die in Darkness: Network Shutdowns and Collective Action in African Countries', *International Journal of Communication*, 14, pp. 4264-4287.

Saha, A. (2021) "Alarming Situation in India due to Second Wave of COVID-19", *Academia Letters*. doi: 10.20935/al1391.

Schatzki, T. R. (2001) 'Introduction. In K. Knorr Cetina, T. R. Schatzki, & E. Von Savigny (Eds.)', *The practice turn in contemporary theory* (pp. 10–23). London, UK: Routledge.

Shapiro, J. and Weidmann, N. (2015) "Is the Phone Mightier Than the Sword? Cellphones and Insurgent Violence in Iraq", *International Organization*, 69(2), pp. 247-274. doi: 10.1017/s0020818314000423.

Sherman, J. (2020) 'Kashmir Internet Shutdown Continues, Despite Supreme Court Ruling', *The Diplomat*. Available at: https://thediplomat.com/2020/08/kashmir-internet-shutdown-continues-despite-supreme-court-ruling/.

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

Sutton, J., Butcher, C. and Svensson, I. (2013) "Explaining Political Jujitsu: Institutional Building and the Outcomes of Regime Violence Against Unarmed Protests", *SSRN Electronic Journal*. doi: 10.2139/ssrn.2285248.

Sutterlin, E. (2020) 'Flipping the Kill-Switch : Why Governments Shut Down the Internet (Undergraduate Honors Theses)'.

Swisher, K., 2019. Sri Lanka Shut Down Social Media. *New York Times*. Available at: https://www.nytimes.com/2019/04/22/opinion/sri-lanka-facebook-bombings.html.

The Statesman (2019) *Mobile internet services restored in Assam after 10 days of shutdown post violent CAA protests*, *The Statesman*. Available at: https://www.thestatesman.com/india/mobile-internet-services-restored-assam-10-days-shutdown-post-violent-caa-protests-1502835400.html (Accessed: 3 August 2021).

The Print (2019) *Delhi HC stays Rs 25,000 fine on police in northeast Delhi riots case*, *ThePrint*. Available at: https://theprint.in/judiciary/delhi-hc-stays-rs-25000-fine-on-police-in-northeast-delhi-riots-case/704727/ (Accessed: 3 August 2021).

Taye, B. (2019) 'The state of Internet shutdowns around the world: The 2018 #KeepItOn report', Access Now. Available at: https://www.accessnow.org/cms/assets/uploads/2019/07/KeepItOn-2018- Report.pdf.

Taye, B. (2021) 'Shattered Dreams and Lost Opportunities: A Year in the Fight to #KeepItOn', (January). Available at: https://www.accessnow.org/keepiton/.

Telegraph act (1885). India: Constitution of India.

The Economist. (2013) 'Turning off the entire internet is a nuclear option best not exercised', Available at: *http://www.economist.com/news/special -report/21574633-turning-entire-internet-nuclear-option-best-not-exercised -thou-shalt-not-kill*. The Economist 6.4.2013.

United Nations (2020, May) 'UN Secretary-General's 'FDigital Cooperation Roadmap', Retrieved Jan 22, 2021, from https://undocs.org/A/74/821; and Organization for Security and Co-operation in Europe (May 2015). *Joint Declaration on Freedom of Expression and Responses to Conflict Situations*, Available at: https://www.osce.org/fom/154846.

United Nations. (1966) 'International covenant on civil and political rights', Available at: https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx X2

UN Security Council: End Inaction on Ethiopia (2021). Available at: https://www.hrw.org/news/2021/07/02/un-security-council-end-inaction-ethiopia (Accessed: 3 August 2021).

Wagner, B. (2018) 'Understanding Internet Shutdowns: A Case Study from Pakistan', *International Journal of Communication*, 12, pp. 3917–3938.

Wakefield, J. (2019) 'Sri Lanka attacks: The ban on social media', *BBC UK*. Available at: https://www.bbc.com/news/technology-48022530.

Warf, B. (2011) 'Geographies of global Internet censorship', *GeoJournal*, 76(1), pp. 1–23. doi: 10.1007/s10708-010-9393-3.

West, D. M. (2016) 'Internet shutdowns cost countries $2.4 billion last year', *Brookings Institution*, (October), pp. 1–20. Available at: https://www.brookings.edu/research/internet-shutdowns-cost-countries-2-4-billion-last-year/.

Woods, M. et al. (2012) "'The country(side) is angry': emotion and explanation in protest mobilization", *Social & Cultural Geography*, 13(6), pp. 567-585. doi: 10.1080/14649365.2012.704643.

Wong, J.C. & Paul, K. (2019) 'Sri Lanka's social media blackout reflects sense that online dangers outweigh benefits', *The Guardian*. Available at: https://www.theguardian.com/world/2019/apr/22/sri-lankas-social-media-blackout-reflects-sense-that-online-dangers-outweigh-benefits.