GLOBAL
RISK
INTEL

Risk Report

THE INTERNET KILL SWITCH: RISKS AND AIMS OF GOVERNMENT-IMPOSED INTERNET SHUTDOWNS

OPERATIONAL

FINANCIAL

COMPLIANCE

www.globalriskintel.com

DISCLAIMER:

THE VIEWS EXPRESSED IN THIS DOCUMENT ARE THE SOLE RESPONSIBILITY OF THE AUTHOR(S) AND DO NOT NECESSARILY REFLECT THE VIEWS OF GLOBAL RISK INTELLIGENCE. THIS DOCUMENT IS ISSUED WITH THE UNDERSTANDING THAT IF ANY EXTRACT IS USED, THAT BOTH THE AUTHOR(S) AND GLOBAL RISK INTELLIGENCE SHALL BE CREDITED, PREFERABLY WITH THE DATE OF THE PUBLICATION.

THE INTERNET KILL SWITCH

RISKS AND AIMS OF GOVERNMENT-IMPOSED INTERNET SHUTDOWNS

RISK REPORT

Global Risk Intelligence

SEPTEMBER 4, 2019

Washington, D.C. · London · Dubai · Singapore

www.globalriskintel.com

Author

Yasemin Zeisl is a Risk Analyst at Global Risk Intelligence. She earned her MSc in International Relations and Affairs from the London School of Economics and Political Science (LSE). She is currently based in Austria.

List of Abbreviations:

AFRINIC	African Network Information Centre
CIPESA	Collaboration on International ICT Policy in East and Southern Africa
IMF	International Monetary Fund
ISP	Internet Service Provider
ITU	International Telecommunication Union
UNHRC	United Nations Human Rights Council

BOLTS: OPERATIONAL, FINANCIAL, COMPLIANCE.

TAGS: AFRICA, ASIA, EUROPE, MIDDLE EAST, CAMEROON, CHAD, INDIA, SPAIN, SUDAN, TURKEY, ZIMBABWE, CYBERSECURITY, GOVERNMENT CONTROL, INTERNET, INTERNET SERVICE PROVIDERS, INTERNET BLACKOUT, INTERNET SHUTDOWN, NATIONAL SECURITY, PUBLIC SAFETY, SOCIAL MEDIA, MEDIA, UNITED NATIONS.

Contents

1. Introduction: Outlining the Utilization of the Internet Kill Switch.................................. 7

2. Types of Associated Risks 10

2.1. Political Risks 10

2.2. Economic Risks 11

2.2.1. Financial Losses.. 11

2.3. Social Risks... 13

3. Digital Rights and Solutions 14

4. Select Examples 16

4.1. Sudan 16

4.2. Chad... 17

4.3. Zimbabwe 18

4.4. Cameroon.. 18

4.5. India... 19

5. Concluding Thoughts.. 20

1. Introduction: Outlining the Utilization of the Internet Kill Switch

Governments have flipped the internet kill switch and utilized network shutdowns for various purposes as early as 2005[1]. Since the Arab Spring revolution in the Middle East and North Africa in 2010 and 2011, government-imposed internet shutdowns have become a popular tool to control the behavior and communication of their citizens. In fact, temporary internet shutdowns have been activated in authoritarian as well as democratic states. Digital rights activists and opponents of the internet kill switch criticize far-reaching internet blackouts as a method to control civil dissent and govern a country's political narrative.

The concept of the 'internet kill switch' generally refers to a complete internet shutdown, but it can also imply a range of techniques which governments use to exercise control over online access within their countries. Government authorities commonly contact internet services providers (ISPs), which are often state-owned corporations licensed by the government, to cut or limit access to the internet or selected applications. ISPs oftentimes have little choice but to execute government orders, since they risk losing licenses and contracts if they refuse to cooperate.

Internet restrictions include content blocking, throttling, filtering, complete shutdowns, and cable cutting. Content blocking is a relatively moderate method that blocks access to a list of selected websites or applications. When users access these sites and apps, they receive notifications that the server could not be found or that access was denied by the network administrator. A more subtle method is throttling. Authorities decrease the bandwidth to slow down the speed at which specific websites can be accessed. A slow internet connection discourages users to connect to certain websites and does not arouse immediate suspicion. Users may assume that connection service is slow but may not conclude that this circumstance was authorized by the government. Filtering is another tool to censor targeted content and erases specific messages and terms that the

[1] Mitchell, C. (2019): Internet blackouts: The rise of government-imposed shutdowns, *Al Jazeera*. Available at: https://www.aljazeera.com/indepth/features/internet-blackouts-rise-government-imposed-shut-downs-190614091628723.html (Accessed: June 19, 2019).

government does not approve of. A list of blocked terms could include the words 'demonstrations' or "human rights".

A severe method to control online activity is a complete shutdown in which all internet services in a region or a country are fully suspended. Presumably, the most extreme version of repressing internet usage is the cutting of fiber optic cables, which transmit most of the internet data. While threats have been made to sabotage internet cables, a government would rather use such threats against foreign actors instead of the domestic population. Repairing cables and re-establishing connections domestically would prove to be inconvenient and costly, which is why governments appear more inclined to resort to the other methods.

Several potential motivations for the restriction of internet usage can be identified. For instance, the kill switch serves to censor content and constrain the spread of news. This particularly concerns news reports that cover police brutality, human rights abuses, or educational information. Governments may also utilize the kill switch to prevent government-critical protestors from communicating through message applications like WhatsApp, Facebook, or Twitter and organizing mass demonstrations. Therefore, internet restrictions can provide a way of regulating the flow of information and hindering dissent. Governments reason that internet limitations help stop the spread of fake news and strengthen national security and public safety in times of unrest.

Government-induced internet shutdowns are most common in the event of rising anti-government protests, times of political instability and upheaval, and during nationwide or regional exams. Public access to social media was blocked during and after the Easter Sunday bombings in Sri Lanka on April 21, 2019[2]. The aim of this temporary social media ban was to control the spread of speculative or false information and prevent a mass panic. The government in Senegal utilized internet bans a few months before the presidential election in February 2019 for similar reasons. Senegal's President Macky Sall argued that internet restrictions would stop the spread of false

[2] **Wakefield, J. (2019): Sri Lanka attacks: The ban on social media, *BBC*. Available at: https://www.bbc.com/news/technology-48022530 (Accessed: June 24, 2019).**

news[3], which would distort the outcome of the democratic elections. Critics maintain that this interference with internet connectivity fosters censorship. In countries like Iraq, Algeria, and Ethiopia, the government blocked the internet for several days during exam periods to stop students from cheating[4]. While this may increase fairness during exams for students, internet blackouts can be harmful if citizens who are not taking exams are affected as well.

A prevalent method that citizens use to circumvent bans is using virtual private networks (VPN). VPNs encrypt data to conceal a user's location, simulating that the user is in another country to grant access to blocked websites. Even though governments may decide to disable VPNs as well, this would inconvenience foreign diplomats and multinational corporations. Therefore, news broadcasters Al Jazeera and the BBC argue that governments are more likely to refrain from using VPN bans[5]. A strategy that civil rights and digital rights organizations employ to counter internet blackouts are digital security training sessions. By learning more about encryption and surveillance prevention, activists try to manage internet restrictions[6].

According to data by Access Now, a global independent digital rights organization, internet shutdowns are an increasing risk. In 2016, the number of shutdowns worldwide was 75. Access Now counted 108 internet blackouts in 2017 and a total of 188 internet blockages in 2018. The continents that are most affected by such government-imposed shutdowns are Asia and Africa. The organization documented 310 instances in Asia and 46 instances in Africa between 2016 and

[3] **Haque, N. (2018): Internet censorship tightens in Senegal before elections, *Al Jazeera*. Available at: https://www.aljazeera.com/news/2018/11/internet-censorship-tightens-senegal-elections-181130125836487.html (Accessed: June 24, 2019).**

[4] **Mitchell, C. (2019): Internet blackouts: The rise of government-imposed shutdowns, *Al Jazeera*. Available at: https://www.aljazeera.com/indepth/features/internet-blackouts-rise-government-imposed-shut-downs-190614091628723.html (Accessed: June 19, 2019).**

[5] **Giles, C. (2019): Africa internet: How do governments shut it down?, *BBC*. Available at: https://www.bbc.com/news/world-africa-47734843 (Accessed: June 19, 2019); Mitchell, C. (2019): Internet blackouts: The rise of government-imposed shutdowns, *Al Jazeera*. Available at: https://www.aljazeera.com/indepth/features/internet-blackouts-rise-government-imposed-shut-downs-190614091628723.html (Accessed: June 19, 2019).**

[6] **Mukeredzi, T. (2017): Uproar over internet shutdowns, *UN Africa Renewal Online*. Available at: https://www.un.org/africarenewal/magazine/august-november-2017/uproar-over-internet-shutdowns (Accessed: June 19, 2019).**

2018[7]. The steadily climbing number of internet blackouts between 2016 and 2018 demonstrates that governments resort to this method more frequently in recent years, making it an increasing risk.

2. Types of Associated Risks

Regional or country-wide internet restrictions carry severe implications for society, business, and politics. It poses a risk not only to private communication, but also to the financial sector and commercial business operations. If more governments copy other state authorities to politicize the internet as a control mechanism, risks for these sectors are expected to rise in the future.

2.1. Political Risks

Internet shutdowns frequently arise out of political concerns. Incumbent administrations and heads of state potentially fear a loss of power. Information and communication are weaponized to gain control over citizens. Governments can stop the spread of reports about atrocities that they may have warranted. Journalists and news portals are not able to reach audiences in such cases. While international news organizations may be less affected by such situations, regional or local news platforms may struggle. At the same time, internet blackouts also impede the assembly of protesters and mass rallies. Activist organizations are also severely affected by internet blackouts. Since activism is often dependent on web portals, organizations can no longer reach and educate their audiences in the event of a blackout. If internet bans are increasingly used by governments across the globe, freedom of speech and the democratic process are put at serious risk.

While the consequences of governments stifling freedom of speech among its citizens may be clearer, internet shutdowns may also produce an adverse effect on governments. Extensive internet blockages may draw attention from the international community and activists, who could publicly criticize these governments. Putting international pressure on governments, which utilize internet

[7] **Access Now (2018): *Internet shutdowns in context: Insights from the Shutdown Tracker Optimization Project (STOP)*. Available at: https://www.accessnow.org/keepiton/ (Accessed: June 24, 2019).**

blackouts, could bring about a change in the behavior of governments. The effectiveness of such international pressure, however, depends on the domestic political situation, size, economic power, and allied states of each individual country. Yet, the growing number of internet shutdowns worldwide indicate that state leaders increasingly weaponize the internet. Therefore, international pressure may only produce limited results.

2.2. Economic Risks

Internet shutdowns can negatively impact the economy in various ways. Businesses without access to the internet will have difficulties operating efficiently. Temporal internet bans paralyze the communication between firms, banks, and customers and lead to financial losses. Particularly vulnerable to the internet kill switch are e-commerce and technology companies as well as start-ups, as they are highly dependent on uninhibited internet access. Similarly, multinational corporations will be more inefficient if communication is limited in regions affected by online restrictions. Moreover, investors may be less inclined to invest in countries in which the internet connectivity is unreliable and dependent on the political climate. Moving a business into a foreign country also requires internet access. Therefore stakeholders are more likely to select a place where online services are stable. A lack of investment is particularly damaging in regions that are in dire need of economic stability and financial liquidity.

2.2.1. Financial Losses

Temporary internet restrictions result in great financial losses. Calculations by the public policy think tank Brookings Institution have shown that global internet shutdowns between 2015 and 2016 caused a loss of USD 2.4 billion in GDP worldwide[8]. Internet shutdowns and social media bans between 2015 and 2017 resulted in an estimated loss of 237 million USD in Sub-Saharan Africa

[8] **West, D. M. (2016): Internet shutdown cost countries $2.4 billion last year, *Center for Technology Innovation at Brookings*, October 2016, pp. 1-20. Available at: https://www.brookings.edu/research/internet-shutdowns-cost-countries-2-4-billion-last-year/ (Accessed: June 19, 2019).**

alone, according to Uganda-based research center Collaboration on International ICT Policy in East and Southern Africa (CIPESA)[9].

Brookings also published an in-depth study of government-imposed internet restrictions in 2016 and recorded a total of 81 internet disruptions in 19 countries worldwide between July 1, 2015 and June 30, 2016[10]. The study included various types of internet disruptions. Most frequent restrictions affected the national internet, the subnational mobile network, and national apps and services. Less frequent limitations were detected in subnational internet services, the national mobile network, and the subnational apps and services. Disruptions in national app services and subnational mobile services accounted for the greatest financial losses. Limitations on national app services cost USD 1 billion and subnational mobile restrictions cost USD 935 million globally.

Government authorities in India and Iraq resorted to internet blackouts the most, accounting for 22 blackouts respectively. Other countries that were at higher risk of experiencing government-backed internet shutdowns were Syria (8 instances) and Pakistan (6 instances). The cost of internet shutdowns between 2015 and 2016 was the highest in India with USD 968 million[11]. A report by the Indian Council for Research on International Economic Relations further revealed that internet blackouts between 2012 and 2017 cost India as much as USD 3.04 billion[12]. Other countries that suffered tremendous financial losses between 2015 and 2016 are Saudi Arabia (USD 465 million), Morocco (USD 320 million), Iraq (USD 210 million), and Brazil (USD 116 million)[13].

[9] CIPESA (2017): Calculating the economic impact of internet disruptions in Sub-Saharan Africa, *CIPESA*. Available at: https://cipesa.org/?wpfb_dl=252 (Accessed: June 24, 2019).

[10] West, D. M. (2016): Internet shutdown cost countries $2.4 billion last year, *Center for Technology Innovation at Brookings*, October 2016, pp. 1-20. Available at: https://www.brookings.edu/research/internet-shutdowns-cost-countries-2-4-billion-last-year/ (Accessed: June 19, 2019).

[11] West, D. M. (2016): Internet shutdown cost countries $2.4 billion last year, *Center for Technology Innovation at Brookings*, October 2016, pp. 1-20. Available at: https://www.brookings.edu/research/internet-shutdowns-cost-countries-2-4-billion-last-year/ (Accessed: June 19, 2019).

[12] Kathuria, R. et al. (2018): The anatomy of an internet blackout: Measuring the economic impact of internet shutdowns in India, *Indian Council for Research on International Economic Relations*. Available at: http://icrier.org/pdf/Anatomy_of_an_Internet_Blackout.pdf (Accessed: June 24, 2019).

[13] West, D. M. (2016): Internet shutdown cost countries $2.4 billion last year.

As the number of government-imposed internet restrictions is gradually rising globally, so will the financial burden. The intersection between political and financial affairs is therefore a central risk. Critics of government-authorized internet shutdowns contend that international finance institutions giving out loans to governments that utilize internet shutdowns disregard human rights, citing the case of Cameroon[14]. The Central African Republic of Cameroon received a USD 666.2 million loan from the International Monetary Fund (IMF) in June 2017[15]. The loan was granted six months after Cameroon's government started blocking access to the internet in January 2017[16]. While this does not imply that the IMF supports government-imposed internet bans, financial funding could encourage these governments' behavior since they may believe that enforcing internet restrictions will not lead to significant consequences.

2.3. Social Risks

Social issues caused by internet shutdowns assume various forms. A high-risk situation is one in which human life is on the line. If people cannot communicate with each other to deliver medication or transport others to a hospital in the case of an emergency, lives are at risk. Furthermore, online access is also vital to citizens when they view updates about traffic congestions or the location of medical centers. In particular, the medical sector and situations associated with medical issues are at high risk during internet blackouts.

[14] **Ritzen, Y. (2018): Rising internet shutdowns aimed at 'silencing dissent', *Al Jazeera*. Available at: https://www.aljazeera.com/news/2018/01/rising-internet-shutdowns-aimed-silencing-dissent-180128202743672.html (Accessed: June 19, 2019).**

[15] **International Monetary Fund (2017): *IMF Executive Board approves US$ 666.2 million arrangement under the extended credit facility for Cameroon*. Available at: https://www.imf.org/en/News/Articles/2017/06/26/pr17248-imf-executive-board-approves-arrangement-under-the-extended-credit-facility-for-cameroon (Accessed: June 24, 2019).**

[16] **Al Jazeera (2017): Cameroon shuts down internet in English-speaking areas, *Al Jazeera*. Available at: https://www.aljazeera.com/news/2017/01/cameroon-anglophone-areas-suffer-internet-blackout-170125174215077.html (Accessed: June 24, 2019).**

3. Digital Rights and Solutions

Human rights have become so interconnected with internet usage that digital rights are increasingly being considered equal to human rights. The United Nations Human Rights Council (UNHRC) affirmed in 2018 that digital rights must be protected in the same way as human rights[17]. Allocating internet access to the status of a human right is a positive development. The United Nations, however, must overcome the central challenge of implementation. Some governments may be reluctant to implement this right, and the UN has only limited power to prevent governments from utilizing the internet kill switch.

Several existing international laws can be applied to internet usage. Article 19 of the Universal Declarations of Human Rights (1948) and article 19 of the International Covenant on Civil and Political Rights (1966) safeguard the freedom of opinion and expression and the right to access to information without external interference[18]. Article 15 of the International Covenant on Economic, Social and Cultural Rights (1966) further stipulates that states should grant citizens the right "to enjoy the benefits of scientific progress and its applications"[19]. The wording of this regulation implies that the advantages of internet services are also included.[20] A more ambiguous perspective on online access and communication is adopted by the International Telecommunication Union (ITU). Article 33 of the Constitution and Convention of the International Telecommunication Union adopted by the 2018 Plenipotentiary Conference provides that international telecommunication service is a public good[21]. The ITU specifies that "Member States recognize the right of the public

[17] United Nations (2018): *The promotion, protection and enjoyment of human rights on the Internet*. Available at: http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/38/L.10/Rev.1 (Accessed: June 24, 2019).

[18] United Nations (1948): *Universal Declaration of Human Rights*. Available at: https://www.un.org/en/universal-declaration-human-rights/ (Accessed: June 24, 2019); United Nations (1966): *International Covenant on Civil and Political Rights*. Available at: https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx (Accessed: June 24, 2019).

[19] United Nations (1966): *The International Covenant on Economic, Social and Cultural Rights*. Available at: https://www.ohchr.org/en/professionalinterest/pages/cescr.aspx (Access: June 24, 2019).

[20] Chapman, A. R. (2009): Towards an understanding of the right to enjoy the benefits of scientific progress and its applications, *Journal of Human Rights*, 8, pp. 1-36.

[21] International Telecommunication Union (2019): *Constitution and Convention of the International Telecommunication adopted by the 2018 Plenipotentiary Conference*. Available at:

to correspond by means of the international service of public correspondence"[22]. Article 34 on the Stoppage of Telecommunications and article 35 on the Suspension of Services, however, declare that states possess the right to constrain transmission and communication if they threaten national security, public order, or decency norms[23]. Regardless of their true motivations, governments may therefore argue that internet services imperil state security under the pretext of conforming to international law. Furthermore, states that have not signed and ratified these international treaties are not bound by established international laws.

International advocacy organizations try to promote these international laws with global campaigns. One of these campaigns is #KeepItOn. In 2016, a group of organizations affiliated with #KeepItOn convened in San Francisco, California, to discuss human rights in the context of the internet[24]. As of June 2019, more than 150 organizations and institutions worldwide have joined the #KeepItOn initiative[25]. Another campaign endorsing uninhibited internet freedoms is #BringBackOurInternet. It was started as a counterreaction to the government in Cameroon shutting down the internet for citizens of the English-speaking region of the country[26]. The success of such initiatives, however, remains unclear since governments utilizing the kill switch may remain unconvinced even by economic arguments[27].

http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/5.22.61.en.100.pdf (Accessed: June 24, 2019).

[22] **Ibid.**

[23] **Ibid.**

[24] **Mukeredzi, T. (2017): Uproar over internet shutdowns, *UN Africa Renewal Online*. Available at: https://www.un.org/africarenewal/magazine/august-november-2017/uproar-over-internet-shutdowns (Accessed: June 19, 2019).**

[25] **Access Now (2019): *#KeepItOn campaign*. Available at: https://www.accessnow.org/keepiton/#add-your-org (Accessed: June 24, 2019).**

[26] **Internet Sans Frontieres (2018): One year of #BringBackOurInternet six months of internet shutdowns for citizens of English-speaking Cameroon*, Internet Sans Frontieres*. Available at: https://internetwithoutborders.org/one-year-of-bringbackourinternet-six-months-of-internet-shutdowns-for-citizens-of-english-speaking-cameroon/ (Accessed: June 24, 2019).**

[27] **Mukeredzi, T. (2017): Uproar over internet shutdowns, *UN Africa Renewal Online*. Available at: https://www.un.org/africarenewal/magazine/august-november-2017/uproar-over-internet-shutdowns (Accessed: June 19, 2019).**

The African Network Information Centre (AFRINIC), the regional internet registry organization for Africa, proposed sanctions as a solution for the internet blackout problem. Such sanctions would ban governments' online platforms for a year. In a final discussion, the proposal was rejected because this measure could anger governments and produce unintended consequences[28]. Sanctions against government-authorized internet blockages are as difficult to manage as sanctions against other human rights abuses. The success of sanctions depends on the individual political and economic situation of a country. Assessing these factors from an international as well as a domestic perspective produces a comprehensive assessment of the situation. Such analyses increase the chances of successfully stopping governments from utilizing internet shutdowns.

4. Select Examples

Far from being an activity dominated by authoritarian states, democratic countries also suspend internet services partially or entirely. Spain is an example of a western democratic country which banned certain websites on the Catalan independence movement in order to contain the emergent mass protests in the Catalan region of Spain[29]. Turkey also restricted social media services during the failed military coup of 2016[30]. The following select examples serve to illustrate a variety of situations in which governments have restricted internet access.

4.1. Sudan

The case of Sudan demonstrates how governments suspend internet services to stifle public protests in a time of political turmoil. The onset of the revolution in December 2018 resulted in the ousting of President Omar al-Bashir, ending his 30-year rule. Consequently, a military government

[28] Ibid.

[29] Armstrong, S. (2017): Catalonia plots digital government in exile in bid for independence, *Wired*. Available at: https://www.wired.co.uk/article/catalan-government-independence-internet-spain (Accessed: June 19, 2019).

[30] Schechner, S. (2016): Erdogan embraces social media to repel coup attempt in U-turn, *Wall Street Journal*. Available at: https://www.wsj.com/articles/erdogan-embraces-social-media-to-repel-coup-attempt-in-u-turn-1468760698 (Accessed: June 19, 2019).

was established. Citizens of Sudan continued to protest in the capital, Khartoum, where mobile internet access was blocked on June 3, 2019. After cases of killings and rape were reported, authorities also suspended the landline network[31]. In late June 2019, a Sudanese court instructed Zain Sudan, the country's largest telecommunications company, to restore services after the internet was suspended for three weeks[32]. The risk of digital blackouts such as this is that atrocities remain unreported and protesters will find it harder to communicate and mobilize. Moreover, the shutdown impairs the Sudanese economy and the ability to administer humanitarian aid.

4.2. Chad

The motivations behind government-imposed internet bans in Chad resemble those of Sudan. In both cases, the goal was to silence dissent by stopping the flow of information and communication. What distinguishes the case of Chad is that restrictive measures are connected to presidential elections. This type of motivation is not unique to Chad, but it is a relatively frequent driver of internet shutdowns. Similar events have occurred in the Democratic Republic of Congo and Uganda.

Since the presidential election in 2016, critics of Chad's President Idriss Deby have convened on social media to express discontent. Deby has been in office since 1990 and dissident citizens disapproved of the election outcome in 2016. After anti-government demonstrations took place in Ndjamena, Chad's capital, state authorities recognized the importance of social media and the internet for protesters. Access to online platforms such as WhatsApp, Facebook, and Twitter was cut in late March 2018 when the government introduced a constitutional amendment, which would allow President Deby to remain in office until 2033[33]. This case demonstrates that control

[31] **Mitchell, C. (2019): Internet blackouts: The rise of government-imposed shutdowns, *Al Jazeera*. Available at: https://www.aljazeera.com/indepth/features/internet-blackouts-rise-government-imposed-shut-downs-190614091628723.html (Accessed: June 19, 2019).**

[32] **Abdelaziz, K. (2019): Sudan court orders company to end military-ordered internet blackout: Lawyer, *Reuters*. Available at: https://www.reuters.com/article/us-sudan-politics-internet/sudan-court-orders-company-to-end-military-ordered-internet-blackout-lawyer-idUSKCN1TO0FV (Accessed: June 25, 2019).**

[33] **BBC (2019): Chad: Where social media has been cut for a year, *BBC News*. Available at: https://www.bbc.com/news/world-africa-47733383 (Accessed: June 19, 2019).**

over internet services paves a way for heads of state and other government authorities to consolidate power. Consequentially, the risk of gradually eroding democratic processes rises.

4.3. Zimbabwe

The case of Zimbabwe highlights potential consequences of legal action against internet shutdowns. After fuel prices rose in Zimbabwe in early 2019, citizens took to the streets to protest. The government subsequently shut down internet services while protests were brought under control[34]. ISPs can take legal action against government-imposed internet shutdowns, but they commonly face the risk of severing ties with the government and losing contracts if they do. Despite these risks, the case was taken to court in Zimbabwe, where judges ruled in favor of re-establishing internet connections. Zimbabwe's government reacted by tightening control of the internet through enforcing new regulative measures[35]. Hence, taking legal action can be beneficial for citizens who lost internet access due to government-imposed restrictions, but it can also lead to negative outcomes for affected citizens.

4.4. Cameroon

The case of Cameroon shows that internet restrictions can be directed at minority groups and disadvantaged communities. The majority of Cameroon's population speaks French, whereas only a small minority speaks English. When citizens in Anglophone regions of the country protested against the expansion of the French language in 2017, the government imposed a ban on social media and messaging services, targeting these regions. The first ban lasted from January to April

[34] Al Jazeera (2019): Zimbabwe imposes internet shutdown amid crackdown on protests, *Al Jazeera*. Available at: https://www.aljazeera.com/news/2019/01/zimbabwe-imposes-total-internet-shutdown-crackdown-190118171452163.html (Accessed: June 25, 2019).

[35] Mitchell, C. (2019): Internet blackouts: The rise of government-imposed shutdowns, *Al Jazeera*. Available at: https://www.aljazeera.com/indepth/features/internet-blackouts-rise-government-imposed-shut-downs-190614091628723.html (Accessed: June 19, 2019).

2017[36]. Cultural, social, or ethnic minorities can be vulnerable to internet-related discrimination by the government, depending on how easy it is to locate and restrict them. In some cases, disadvantaged communities may be geographically dispersed, which could make locating them more difficult.

4.5. India

India is a relevant case because of the frequency of internet shutdowns and the size of the country. As the world's largest democracy, internet blackouts in India affect a large number of people. Moreover, the Indian Ministry of Communication stipulated in 2017 that the government possesses the authority to temporarily stop telecommunication services if public security is under threat[37]. Shutdowns in the country are largely politically motivated since the prime target of blackouts is the disputed region of Kashmir. India, Pakistan, and China lay claim to the region in the north of the Indian subcontinent. The non-profit organization Software Freedom Law Centre in New Delhi tracked 167 internet shutdowns in Kashmir between 2012 and mid-2019. The number surpassed the frequency of shutdowns in other regions of India[38]. Political unrest and military operations are not the only drivers of government-authorized internet blackouts. Indian authorities also suspend services during exams in order to stop students from cheating[39]. The economic and political impact of such a regular suspension of internet services is severe in a country of the population size of India.

[36] **Ritzen, Y. (2018): Rising internet shutdowns aimed at 'silencing dissent', *Al Jazeera*. Available at: https://www.aljazeera.com/news/2018/01/rising-internet-shutdowns-aimed-silencing-dissent-180128202743672.html (Accessed: June 19, 2019).**

[37] **Ministry of Communications India (2017): *The Gazette of India: Extraordinary Part II, Section 3, Sub-section (i)*. Available at: http://dot.gov.in/sites/default/files/Suspension%20Rules.pdf (Accessed: June 25, 2019).**

[38] **Software Freedom Law Center India (2019): *Internet shutdowns*. Available at: https://www.internetshutdowns.in/ (Accessed: June 25, 2019).**

[39] **McCarthy, N. (2018): The countries shutting down the internet the most, *Forbes*. Available at: https://www.forbes.com/sites/niallmccarthy/2018/08/28/the-countries-shutting-down-the-internet-the-most-infographic/#4607a0e12940 (Accessed: June 19, 2019).**

5. Concluding Thoughts

Government-imposed internet shutdowns are applied in a variety of situations. They are driven by manifold political motivations and carried out in different ways, including complete shutdowns and targeted restrictions of access. The internet kill switch may be used for national security and public safety reasons to defend against external cyberattacks in an international cyber war. The risk of internet shutdowns, however, lies in their misuse by governments. Not only non-democratic states but also democratic governments can exert excessive control over internet services. While there are international laws regulating the rights of citizens to online communication and internet access, the implementation of these laws remains a challenge. Furthermore, measures against governments are difficult to plan and enforce, as they can lead to negative outcomes.

Destruction caused by internet restrictions may not be as physically apparent as military strikes, yet this does not mean that internet shutdowns are harmless. Economic burdens and human rights abuses are major consequences. In particular, developing countries and countries experiencing an economic depression are susceptible to the financial repercussions of a prolonged internet service suspension.

The population size of a country and prevalence of internet usage are important determinants in evaluating the financial and political burden of an internet shutdown. Countries that heavily invest in e-commerce and digital banking services are especially vulnerable to online service suspensions. Temporary internet bans in large countries like India or China will impact a great number of people, and financial losses will be substantial.

Internet limitations are also a convenient tool to exercise control. Governments primarily focus on political aims when they impose internet bans. At the same time, they should also consider the economic impact on the state. As multiple aspects of private and public life become increasingly reliant on the internet, risks associated with the weaponization of the internet are likely to rise in the future.

GLOBAL
RISK
INTEL

www.globalriskintel.com