Cyberstability Paper Series

New Conditions and Constellations in Cyber

Disconnecting from Cyberstability

An Assessment of how Internet Shutdowns in the Democratic Republic of Congo, Tanzania, and Uganda Undermine Cyberstability

Moses Owiny
Founder and CEO of the Centre for Multilateral Affairs (CfMA)

Sheetal Kumar
Senior Programme Lead at Global Partners Digital

September 2021

Cyberstability Paper Series
New Conditions and Constellations in Cyber

Disconnecting from Cyberstability: An Assessment of how Internet Shutdowns in the Democratic Republic of Congo, Tanzania, and Uganda Undermine Cyberstability

Moses Owiny | Founder and CEO of the Centre for Multilateral Affairs (CfMA)

Sheetal Kumar | Senior Programme Lead at Global Partners Digital

September 2021

The aim of this article is to assess how Internet shutdowns undermine cyberstability as defined by the Global Commission on the Stability of Cyberspace (GCSC). According to the GCSC framework, cyberstability means that everyone can be reasonably confident in their ability to use cyberspace safely and securely, where the availability and integrity of services and information provided in and through cyberspace are generally assured, where change is managed in relative peace, and where tensions are resolved in a non-escalatory manner.[1] The assessment of how shutdowns undermine cyberstability is based on Internet shutdowns in three neighboring countries—the Democratic Republic of Congo (DR Congo), Tanzania, and Uganda—over the past five years, and is conducted according to the GCSC's four cyberstability principles: a) Responsibility, b) Restraint, c) Requirement to act, and d) Respect for human rights. We review select cases of shutdowns in each country, describing their main characteristics (e.g., the services affected, duration of the shutdown, and the measured impact). The selection of countries was based on the

Moses Owiny is the Founder and CEO at the Centre for Multilateral Affairs (CfMA) in Uganda. In June 2021, he served as an external co-chair and Programme Committee member for the 10th edition of RightsCon under the category "Cyber Norms, Accountability, and Practice."

Sheetal Kumar is Senior Programme Lead at Global Partners Digital. Her recent work has focused on applying human-centric approaches to cyber policy, including cyber norms.

frequency of shutdowns in the East and Central Africa region and opportunities to build on existing literature, which has yet to assess the issue of shutdowns according to the concept of cyberstability. Our conclusion is that every cyberstability principle is impacted by Internet shutdowns and that States and telecommunications companies have obligations and responsibilities to end the practice of shutdowns. Civil society, the technical community, and academia also have a role to play in keeping States and telecommunications companies accountable for the negative impact caused by shutdowns.

Through this assessment, we illustrate how and where shutdowns harm cyberstability, expose the gaps required to further understand the relationship between shutdowns and cyberstability, and highlight existing relevant recommendations that would support countries' regulatory frameworks to uphold, rather than undermine, cyberstability. Of particular note is the work the UN Human Rights Council has done to highlight the impact of Internet shutdowns on human rights. In 2021, the UN Special Rapporteur on Freedom of Association and Assembly issued a highly comprehensive report focused on Internet shutdowns, complete with recommendations for States, investors, telecommunications companies, and the UN institutions. We have reviewed these recommendations and, in line with the cyberstability framework, select the most relevant to the cyberstability framework.

We employ the following definition of Internet shutdowns, which are also referred to as network disruptions or "kill switches": "an intentional disruption of Internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information." This definition has been developed by experts and widely employed, including by the NGO Access Now's "Keep It On" campaign.[2] The definition covers the range of shutdowns explored in the country case studies, for instance, those affecting social media and Short Message Services (SMS) (Tanzania), a total outage of Internet services followed by partial restoration (Uganda), and blocking of social media and SMS (DR Congo). Notably, the definition does not cover other forms of information control, such as censorship or stringent content moderation.[3] However, as is highlighted in the country case studies, shutdowns are often utilized to exert information control as part of broader authoritarian trends, which can include harassment of journalists, regulatory frameworks that stifle free expression, suppression of political opponents during an election, and other measures.

Shutdowns are often utilized to exert information control as part of broader authoritarian trends.

Beginning with the DR Congo, we first provide an overview of each country's Internet landscape, including information about the shutdowns experienced in each country. We then assess how each cyberstability principle was affected by the shutdowns.

The DR Congo has an estimated population of over 70 million people, and among the lowest technology penetration rates in the region: 17% Internet penetration and 39.7% mobile phone penetration[4] as of 2019. As in Uganda, the Internet disruption trend in DR Congo first began in 2011 when SMS were blocked for 25 days in December of that year.[5] The second shutdown occurred in January 2015 when both SMS and Internet services were blocked as citizens protested against the proposed electoral bill; the disruption lasted four days. The third shutdown occurred on December 19, 2016 when social media was blocked a day after former president Joseph Kabila was expected to step down as Head of State. The fourth shutdown occurred in December 2018 during the Presidential election and resulted in the Internet and SMS being blocked for 20 days.[6]

As of 2019, the DR Congo had four mobile operators: Vodacom RDC, Airtel Congo, Orange RDC, and Africell RDC, with Vodacom as the leader in the voice segment with 35.2% of the market, followed be Orange at 30%, Airtel at 23.9%, and Africell at 10.9%.[7] The DR Congo has experienced many Internet shutdowns over the years as noted above, and this ranges from complete country-wide shutdowns to targeted regional shutdowns of social media platforms. The laws that govern telecom companies in the DR Congo contain sections that specifically mandate that license holders may be ordered to shut off access to their networks due to concerns of national security and public order.[8] For example, all three international telecom companies in the country—Vodacom (Vodafone controlled company), Millicom, and Bharti Airtel—all publicly acknowledged receipt of an order to suspend Internet service.[9]

Internet shutdowns prevent access to information and impedes freedom of expression, assembly, association, and opinion. It impedes rights to livelihood and work, education and health.[10] For example, the Framework for Calculating the Economic Impact of Internet Disruptions in Sub-Saharan Africa report notes that the DR Congo loses at least 1,936,911 United States Dollars (USD) per day during an Internet disruption[11]. Shutdowns impact the ability of journalists to receive information that is newsworthy but also curtail their ability to share essential information with society. This violates the rights to a free press and restricts both the right to access information as well as the right to freedom of expression.[12]

Internet shutdowns prevent access to information and impedes freedom of expression, assembly, association, and opinion. It impedes rights to livelihood and work, education and health.

Tanzania has an estimated population of 61 million and an Internet penetration rate of 49%.[13] In October 2020, ahead of the general elections in Tanzania, the government ordered the blocking of widely used messaging and social media applications, including WhatsApp, Twitter, Instagram, Facebook, and Google services[14] as well as local social media including the widely popular Jamii Forum. This followed a directive by the Tanzania Communication Regulatory Authority which ordered telecom companies to suspend "bulk SMS messaging" and voice communications as well as individual text messages with certain "keywords," making it effectively impossible for millions of Tanzanians to communicate during this time.[15] While this was not a wholesale blocking, it effectively resulted in people not being able to send text messages and not being able to communicate via the most commonly used messaging platforms over the Internet. The government's justification for the shutdown was "national security and concern for the fairness of the electoral process."[16] In addition to the blocking of social media and text, it was reported that media websites, including websites reporting on election fraud or election events, were blocked and attempts by the government to slow down Internet connections were also documented[17] Virtual Private Networks (VPNs) were banned, although they continued to be accessed during this shutdown.

These attempts to control information and dissent play out in a wider context/trend of shrinking democratic space in the country, including censorship and restriction of the work of journalists, drastically affecting the ability of Tanzanians to exercise their right to freedom of expression. For example, as was covered and commented on widely at the time by both the media and human rights activists, the election shutdown was part of a wider set of information control tactics, including legislation clamping down on foreign press by outlawing international press from covering developments in the country without local media partnerships.[18] It also included other legislation requiring bloggers to register and pay license fees.[19]

In terms of the impact of the shutdown in 2020, analysts said it was "immense," leaving "millions without effective communication tools" across Tanzania and ahead of the general elections.[20] Tanzania has millions of Internet users, and many of these, especially young people, were unable to earn money without the Internet.[21] Case studies of victims collected by Access Now illustrate some of the harm caused, including an inability to work, to complete educational training, and to run businesses and make sales.[22]

Uganda is a landlocked country with an estimated population of 41.6 million people[23] and 20.1 million Internet subscribers,[24] as of April 2020. President Yoweri Museveni won re-election in the January 2021 polls with 59%, despite widespread irregularities, extending his rule to 40 years in power[25] In the lead up to the elections from January 11 to 13, 2021, social media access was blocked and the downloading of some VPNs restricted. This was followed by an Internet blackout, which was lifted by January 18, 2021.

Internet shutdowns in Uganda form part of a more long-standing trend in the country to disrupt communications and the free flow of information among citizens prior to and during elections. In the 2006 elections season, the government instructed Internet Service Providers (ISPs) to block access to the website of Radio Katwe for allegedly publishing "malicious and false information" against the ruling National Resistance Movement (NRM) party and its presidential candidate. At the time, this incident received little public outcry. Yet, it set a troubling new standard in the country. In 2011, the government again instructed ISPs to block access to Facebook and Twitter for 24 hours, during opposition protests dubbed "walk to work" over rising fuel and food prices. However, following this directive, some Internet Service Providers (ISPs) did not respond, claiming they received the directive after the dates specified in the directive. On the eve of the presidential election on February 18, 2016, authorities cut off access to Twitter, Facebook, WhatsApp, YouTube, and Mobile Money services.[26] Later that year, after a disputed election that saw the swearing in of President Museveni in May, social media platforms, including Facebook, WhatsApp, and Twitter, were blocked (with the exception of Mobile Money).[27] More recently, beginning in 2018 and upon the introduction of taxes to access social media platforms, authorities have threatened to block VPNs for those using them to bypass paying the taxes.[28]

The very nature of the shutdowns displayed the multiple actors required to exert control over access to the Internet.

Justifications for the various shutdowns in Uganda by the state have included threats to "national security" from public unrest, the elimination of "the connection and sharing of information that incites the public"[29] and protection of the "national interest".[30]

In the following section, we consider how each of the principles of the cyberstability framework is impacted by the shutdowns discussed above. We take each principle in turn, beginning with the "Responsibility" principle.

The GCSC's framework "responsibility principle" states that everyone is responsible for ensuring the stability of cyberspace. This includes individuals, groups such as civil society, the private sector, technical communities, and academia. In each of the three countries included above, the very nature of the shutdowns displayed the multiple actors required to exert control over access to the Internet. For example, the government could not drastically reduce the ability to communicate without the compliance of telecommunications companies, including Internet Service Providers. In each country, telecommunications companies complied with orders by government actors to

shut off access to the Internet, despite their responsibility to protect and promote human rights, and to provide secure and stable Internet access.[31] While the definition of the responsibility principle does not refer explicitly to international law, all actors are bound by international law, and David Kaye, former UN Special Rapporteur on Freedom of Expression, has stated that "a general network shutdown is in clear violation of international law and cannot be justified by any means".[32]

For example, in Uganda, telecom companies such as MTN, Airtel, and Africell all implemented government directives to block Internet access. In the DR Congo, telecom operators were asked by the regulator to restrict communications "In order to prevent the exchange of abusive images via social media by subscribers and to ... take technical measures to restrict to a minimum the capacity to transmit images".[33] In Tanzania, telecom companies Viettel Tanzania, Vodacom Tanzania, and Tigo also immediately complied with government directives. On the other hand, Internet Service Providers in countries such as Lesotho and Gabon have pushed back against Internet shutdowns.[34] They questioned their intentionality, pointing out provisions in law that guarantee enjoyment of rights to freedom of expression, and engaged the government with support of civil society to maintain and defend uninterrupted Internet access and use.

A general network shutdown is in clear violation of international law and cannot be justified by any means.

As such, telecom companies can and should take the responsibility to resist government measures that undermine responsible behavior, and the government should not abuse their position of power in relation to other actors in the distributed ecosystem by ordering the shutdowns. As UN Special Rapporteur on the rights to freedom of peaceful assembly and of association, Clément N. Voule, has outlined in a recent report to the Human Rights Council, there are a range of measures that digital technology companies, including telecommunications providers and digital communications platforms, can undertake to ensure compliance with their human rights responsibilities even in light of business pressure and other limitations.[35]

The "Restraint" principle provides that no state or non-state actor should take actions that impair the stability of cyberspace. Each of the shutdowns in DR Congo, Tanzania, and Uganda disrupted all users' confidence in their ability to use cyberspace safely and securely, and meant that they could not be assured of the availability and integrity of services and information.

The GCSC also describes this principle as the expectation that both state and non-state actors "prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security." As the Internet Society has pointed out, "Internet users within a country experiencing a shutdown could lose access or experience reduced speed on interconnected networks if traffic needs to be routed through less optimal paths, resulting in collateral damage or systemic risks that go beyond a country's borders.[36] According to ISOC, "wide-scale Internet shutdowns can also have a detrimental impact on the domain name system (DNS),"[37] due to asymmetric DNS traffic requests that can result from shutdowns, which results in a surge in DNS requests and increased load on resolver infrastructure that can have collateral effects. Shutdowns that impact interconnection points or other significant infrastructure components could also impact connectivity and Internet performance in other countries, which could inadvertently harm international relations."[38] For example, "the outlawing of VPNs can severely inconvenience foreign diplomats and large companies which use them because they provide extra security."[39] In addition, if the country hosts services or platforms that are used outside the country, then users outside the country risk losing access to these services, platforms, or related applications. Global organizations op-

erating both within and outside the DR Congo, Tanzania, and Uganda would have been required to have their own platform in order to communicate freely with colleagues outside the country, or rely on VPNs. Yet, further research is required to understand whether or how these countries' shutdowns affected the DNS, connectivity, network resilience, and Internet performance in neighboring countries.[40]

The DR Congo shutdown did elicit diplomatic reaction, with the United States, Canadian, and Swiss heads of mission in Kinshasa urging the government to immediately restore communications,[41] while the EU condemned the 2021 shutdown in Uganda.[42] However, further research could also explore whether, by ordering the wide-scale blocking of texts and social media applications, including VPNs, these countries engaged in ICT practices that risked harming international relations by inconveniencing neighboring countries as well as foreign entities, including companies and diplomats within the country. It could also assess whether trust and relationships between ISPs are impacted, particularly as the Border Gateway Protocol (BGP) network, which routes global Internet traffic, relies on trust between operators, ISPs, and others who are required to withdraw from the network when ordered to shutdown Internet access in the case of complete blackouts.[43]

The third principle is "a Requirement to Act" or to take affirmative action to preserve the stability of cyberspace. The "Requirement to Act" principle requires that states and non-state actors take reasonable and appropriate steps to ensure the stability of cyberspace, as defined above. The framework provides examples of such actions such as upgrading hardware and software, implementing patching, etc. As noted above, shutdowns can undermine the stability and resilience of the Internet, although further research is needed to understand the impact on the infrastructure of the Internet of the Tanzania, DR Congo, and Uganda shutdowns.

Shutdowns that impact interconnection points or other significant infrastructure components could also impact connectivity and Internet performance in other countries, which could inadvertently harm international relations.

Yet, the widespread blocking of social media experienced by those in the DR Congo, Tanzania, and Uganda, and the "Internet blackouts" experienced in Uganda can be understood to be in direct opposition of the positive and proactive steps required to ensure the stability of cyberspace, that is, to ensure the ability to use cyberspace safely, securely, and where the integrity and availability of information is assured. While some companies, such as MTN Uganda, outlined plans to refund customers whose data plans expired during the 2021 shutdown, this falls far short of the steps that telecom companies can take in the face of shutdown orders, including the adoption of mitigation strategies, transparency measures such as the disclosure of all relevant information about shutdowns (e.g., preservation of orders or threats to disrupt networks), notification to users, including at the very least the provision of "regular updates about the services affected or restored, the steps they are taking to address the issue, and explanations after the fact," and the use of legal options for challenging requests, including litigation.[44]

As the GCSC's cyberstability framework states, "compliance with the Human Rights Principle requires that states abide by their human rights obligations under international law as they engage in activities in cyberspace." The impact of Internet shutdowns on human rights, including civil, political, economic, social, and cultural rights, has been widely documented. Authorities who block Internet access and social media fail to uphold their international human rights obligations, including those relating to the right to free expression, provided for under Article 19 of the International Covenant on Civil and Political Rights (ICCPR) and Article 9 of the African Charter on Human and People's

Rights, to which the DR Congo and Tanzania and are signatories. They also violate national laws, including the national constitution of each country.[45] The circumstances under which the shutdowns occurred reveal the intent to restrict rights to freedom of expression and information, and to interfere with the right to freedom of assembly and association, particularly during events such as elections, conflicts, or mass demonstrations.[46] The UN Special Rapporteur, Clement Voule, has noted that national security cannot be invoked as a rationale for blocking Internet access, when in an actual sense the very reason for deteriorating national security is the suppression of human rights itself.[47, 48] Furthermore, Principle 37 of the Declaration of Principles on Freedom of Expression and Access to Information in Africa (revised in 2019) provides that States must facilitate the rights to freedom of expression and access to information online and the means necessary to exercise these rights, and must recognize that universal, equitable, affordable, and meaningful access to the Internet is necessary for the realization of freedom of expression, access to information, and the exercise of other human rights.[49]

The circumstances under which the shutdowns occurred reveal the intent to restrict rights to freedom of expression and information, and to interfere with the right to freedom of assembly and association, particularly during events such as elections, conflicts, or mass demonstrations.

The same Declaration states that "States shall not engage in or condone any disruption of access to the Internet and other digital technologies for segments of the public or an entire population." In addition, the general comment No. 34 (2011) on the freedoms of opinion and expression, the Human Rights Committee, notes that Internet shutdowns are a disproportionate measure (generic bans on the operation of certain sites and systems are not compatible with paragraph 3).[50] The shutdowns, therefore, violated freedom of expression, access to information, and the right to peaceful assembly.

The impact of the Internet shutdowns in each country on human rights also affected economic, social, and cultural rights. The International Covenant on Economic, Social and Cultural Rights (ICESCR) defines a number of rights, including the free pursuit of his or her economic, social, and cultural development. The shutdowns in the DR Congo, Tanzania, and Uganda directly impacted these rights by vastly reducing the ability of millions of people in each country to trade, make money, and access a wide range of services, including educational and health services. The disruption to mobile services in Uganda impacted mobile money services, which are critical to both the formal and informal economies.

One example is a February 2021 report from the Daily Monitor: one of the leading newspaper dailies in Uganda notes that Internet shutdowns affected "key sectors of the economy such as trade, transport, banking, telecom, education, entertainment, media, health, and information technology support."[51] The same Daily Monitor report continued to assert that shutting down the Internet affected payment systems, Real Time Gross Transfers, and Electronic File Transfers. It stressed that "13,000 bank agents who conduct money transfers, Internet banking, and the Automatic Teller Machine"[52] were affected. According to the Internet Society, the cost of Internet shutdowns on the five-day shutdown in Uganda during the 2021 elections amounted to 9 million USD.[53] According to Jumia Uganda—an online shopping store—"cash reconciliation was very difficult because it relies on the Internet, and the whole supply chain suffered, resulting in a lack of access to food, medicines, and groceries."[54] The shutdown in the Democratic Republic of Congo in December 2018 is estimated to have cost the country 3 million USD.[55] In Tanzania, millions of people were unable to earn a livelihood; according to estimates, between 15–27% of young people's income is made

online in the country.[56] It's important to note that the increased dependence on the Internet as a result of the COVID-19 pandemic exacerbated the impact of the shutdown on all of these rights, as people became increasingly dependent on the Internet to carry out basic daily activities, including schooling/education, access to healthcare, transportation and other services.[57]

In addition, Uganda, Tanzania, and the DR Congo have all ratified the Convention on the Elimination of Discrimination against Women (CEDAW). Recent research demonstrates that shutdowns disproportionately impact women as a result of existing inequalities and more vulnerable positions in the economy and society, drawing on cases in India, Iran, Venezuela, and Pakistan.[58] This includes impacts to personal safety and professional and economic safety. However, research on the gender impact in other parts of the world that experience Internet shutdowns has been more limited to date. Further research on the impact of the shutdowns on women and the gender-differentiated impact of Internet shutdowns in the East Africa region would support a better understanding of how the rights of women and girls are affected by Internet shutdowns in different regions of the world.

Our preliminary assessment of the shutdowns in the DR Congo, Tanzania, and Uganda show that the shutdowns undermine the cyberstability framework, as these actions violate all four cyberstability principles; they can be seen as a detrimental effect on regional or national cyberstability overall. In particular, they impacted the human rights principle, a situation which was exacerbated by the increased reliance on digital technology during the COVID-pandemic in 2020. However, further research that captures more granular information about the impact of shutdowns, as recommended elsewhere by GNI, for example,[59] including its gendered impact, would support a greater understanding of the way that shutdowns impact the human rights principle of the cyberstability framework. This could build on work already done on the gendered impact in other countries and regions. The shutdowns impacted the "Responsibility," "Restraint," and "Requirement to Act" principles, particularly as they resulted in the inability of citizens to be able to use cyberspace safely, securely, and in a way where the integrity and availability of information is assured. Further research into how shutdowns impact the restraint principle should be further explored, including the impact on the DNS and on the resilience of networks/access in neighboring countries through collateral border effects. Further research could explore how shutdowns affect the GCSC norms, including, for example, the public core norm—particularly if sufficient evidentiary information on how shutdowns affect the DNS and network stability can be collected. This exploratory article has shown that shutdowns undermine the framework in different ways, and it has identified some gaps where further research would be helpful in forming a more detailed understanding of the relationship between cyberstability and Internet shutdowns. It is a first step and could be expanded to other countries in order to better understand the range of contexts in which shutdowns occur, the similarities between them, and their differences in relation to the GCSC's cyberstability framework.

Our preliminary assessment of the shutdowns in the DR Congo, Tanzania, and Uganda show that the shutdowns undermine the cyberstability framework, as these actions violate all four cyberstability principles; they can be seen as a detrimental effect on regional or national cyberstability overall.

Below we have drawn from the UN Special Rapporteur's comprehensive report on shutdowns and his recommendations, in particular, aligning his recommendations with the cyberstability principles.[60] We have also, where relevant from our analysis, provided some additional recommendations for each stakeholder group.

Recommendations

Responsibility

In order to uphold the principle of "Responsibility," civil society and academia should support companies in challenging unlawful shutdown orders, as well as work with other stakeholders to develop and socialize resources to help Internet users prepare for, prevent, and predict Internet shutdowns.

As stated in the most recent report by the UN Special Rapporteur on Rights to Freedom of Peaceful Assembly and of Association, governments should "ensure that the Internet, including social media and other digital communication platforms, remains open, accessible, and secure. Specifically...States should (i) order Internet Service Providers operating in their country to provide everyone with universal, affordable, high-quality, secure, and unrestricted Internet access throughout election periods, protests...And thereafter (iii) guarantee the safety of technical workers building and maintaining critical infrastructure networks, while ensuring sites are protected, and (iv) promote and protect strong encryption, including by adopting laws, regulations, and policies in line with international human rights, norms, and standards."[61]

Telecom companies and ISPs should take the responsibility to address government measures that undermine responsible behavior by promoting greater transparency.

Telecom companies and ISPs should take the responsibility to address government measures that undermine responsible behavior by promoting greater transparency. In line with the recommendations from the UN Special Rapporteur, they should disclose "information about the circumstances under which they may shut down the network, the demands they receive, and actions to push back on or mitigate the effects of government orders." Ahead of a shutdown, they should "provide timely and transparent guidance to users to identify disruptions likely to impact the quality of service they receive."[62] They should also publish transparency reports, notifying affected users and showing government requests and orders for network disruptions, as well as state their level of compliance to domestic and international laws.

Restraint

Limited publicly available evidentiary information exists on the impact of shutdowns on network stability, in particular how shutdowns may impact Internet speed in neighboring countries, and whether shutdowns that impact interconnection points or other significant infrastructure components have harmed relations in neighboring countries. Therefore, in order to uphold the principle of "Restraint," civil society and academia should work with actors in the technical community (including ISOC chapters, for example) to research the impact of shutdowns on the stability of the network, infrastructure components, the DNS, and Internet speed in neighboring countries, in order to better understand the impact of shutdowns on network availability more widely and on the Internet itself.[63]

As outlined in the aforementioned report of the UN Special Rapporteur, governments should "Refrain from shutting down, throttling, or blocking the Internet, and make a state pledge to refrain from imposing any unlawful restrictions on Internet access and telecommunication in the future, particularly in upcoming elections and protests, and amid the COVID-19 pandemic."[64]

Finally, telecom companies should "Challenge censorship and service limitation requests from states, using all available tools of law and policy, in procedure and practice,"[65] and explore oppor-

tunities to collaborate with civil society in doing so. They should also (along with civil society—as recommended above) collaborate to gather and publish granular information on the collateral impact of shutdowns on their networks and systems, including on their autonomous systems (ASes).

Requirement to Act

Civil society and academia continue to raise awareness of the impact of Internet shutdowns on people, the economy and human rights, including by collecting evidence, developing and sharing tools for documenting shutdowns, and advocating against them. They should continue to track the impact of Internet shutdowns, through the use of network measurement tools and other tracking skills—particularly in countries where there is a dearth of information available on shutdowns and their impact, e.g., the DR Congo.

Governments should proactively repeal and amend any laws and policies that allow for Internet shutdowns and enact legislation prohibiting and punishing these measures, as well as expand initiatives to provide universal and affordable Internet access.[66]

Telecom companies should "engage regulators and push back against licensing conditions (and laws governing the telecommunications sectors) that allow for shutdowns," and, where they are required to comply with shutdown orders, they should "establish response plans and channels of communication with government actors and civil society."[67] They should also "prepare for a range of threats to the rights of users, particularly where bandwidth is overwhelmed and congested as a result of large demonstrations, and ensure that the company deploys extra capacity throughout the events."[68]

Human Rights

Civil society should generate and use evidence-based data to raise awareness and stimulate discussions and debates that inform public policy across all stakeholder groups about the negative impact of Internet shutdowns on human rights, including where there is more limited information, such as on the gendered impacts of Internet shutdowns in the Africa region.

States have obligations under international human rights law to ensure that everyone within their jurisdiction is able to access and use the Internet to exercise their human rights. In line with the recommendations in the UN Special Rapporteur's report, therefore, they should "recognize the right to access and use the Internet as a constitutional and legal right and as an essential condition for the exercise of the right to freedom of peaceful assembly." They should also institute oversight mechanisms, ensuring all network disruptions are subject to detailed reports that are publicly accessible, which detail the nature and causes of the disruptions and assess legal compliance.[69]

Telecom companies should develop and make publicly available policies that specifically state their position against Internet shutdowns and how they address any shutdown orders from governments, in compliance with the UN Guiding Principles on Business and Human Rights.

Acknowledgements

The authors would like to extend their sincere thanks to Ashnah Kalemera (CIPESA) for her review and feedback, and to Nazar Nicholas (ISOC Tanzania) for the fact-checking and guidance he provided.

Endnotes

1 "Advancing Cyberstability," Global Commission on the Stability of Cyberspace. Accessed August 4, 2021. https://cyberstability.org/report/

2 KeepItOn: Frequently Asked Questions. https://www.accessnow.org/keepiton-faq/ Accessed August 4 2021.

3 E. Marchant and N. Stremlau, (2019). Africa's Internet Shutdowns: A report on the Johannesburg Workshop. Programme in Comparative Media Law and Policy (PCMLP), University of Oxford, http://pcmlp.socleg.ox.ac.uk/wp-content/uploads/2019/10/Internet-Shutdown-Workshop-Report-171019.pdf

4 State of Internet Freedom. Democratic Republic of The Congo 2019. Mapping Trends in Government Intent Controls 1999–2019. https://cipesa.org/?wpfb_dl=408. Accessed July 4, 2020.

5 The Evolution of Internet Shutdown in DR Congo. CIPESA. https://cipesa.org/2017/03/the-evolution-of-internet-shutdowns-in-dr-congo/

6 DR Congo Internet restored after 20-day suspension over elections. Accessed August 4, 2021. https://www.aljazeera.com/news/2019/1/20/dr-congo-internet-restored-after-20-day-suspension-over-elections

7 State of Internet Freedom: Democratic Republic of Congo 2019. Mapping Trends in Government Internet Controls, 1999–2019. Accessed August 26, 2021 https://cipesa.org/?wpfb_dl=408

8 Navigating Litigation During Internet Shutdowns in Southern Africa (2019). Accessed August 26, 2021. https://www.southernafricalitigationcentre.org/wp-content/uploads/2019/08/SALC-Internet-Shutdown-Guide-FINAL.pdf

9 Violating International Law, DRC Orders Telcos to Cease Communications Services (2018). Accessed August 25, 2021. https://www.accessnow.org/violating-international-law-drc-orders-telcos-vodafone-millicon-airtel/

10 Navigating Litigation During Internet Shutdowns in Southern Africa (2019). Accessed August 26, 2021. https://www.southernafricalitigationcentre.org/wp-content/uploads/2019/08/SALC-Internet-Shutdown-Guide-FINAL.pdf

11 Disruptions to Digital Communications Persists in the Democratic Republic of Congo (2018). Edrin Wanyama. Accessed August 23, 2021. https://cipesa.org/2018/01/disruptions-to-digital-communications-persist-in-the-democratic-republic-of-congo/

12 Navigating Litigation During Internet Shutdowns in Southern Africa. 2019. Accessed August 26, 2021. https://www.southernafricalitigationcentre.org/wp-content/uploads/2019/08/SALC-Internet-Shutdown-Guide-FINAL.pdf

13 "Internet penetration rate in Tanzania from 2015 to 2020." Accessed August 4, 2021. https://www.statista.com/statistics/1226024/internet-penetration-rate-in-tanzania/

14 "Internet disrupted in Tanzania on eve of general elections." October 27, 2020. https://netblocks.org/reports/internet-disrupted-in-tanzania-on-eve-of-presidential-elections-oy9abny3

15 "Directive on Temporal Suspension of Bulk Messaging and Bulk Voice Calling Services," October 21, 2020. https://www.accessnow.org/cms/assets/uploads/2020/10/TCRA-Directive-to-telcos-in-TZ-to-filter-content.jpeg

16 "Tanzania's Internet restrictions during election are 'despicable,' digital rights activist says." October 28, 2020. https://www.pri.org/stories/2020-10-28/tanzanias-internet-restrictions-during-election-are-despicable-digital-rights

17 Ibid.

18 "As Long as I am Quiet, I am Safe: Threats to Independent Media and Civil Society in Tanzania." Human Rights Watch. October 28, 2019. https://www.hrw.org/report/2019/10/28/long-i-am-quiet-i-am-safe/threats-independent-media-and-civil-society-tanzania

19 "Tanzania's internet restrictions during election are 'despicable,' digital rights activist says". October 28, 2020. https://www.pri.org/stories/2020-10-28/tanzanias-internet-restrictions-during-election-are-despicable-digital-rights

20 "Tanzania: Internet slowdown comes at a high cost" Accessed August 4, 2021. https://www.dw.com/en/tanzania-internet-slowdown-comes-at-a-high-cost/a-55512732

21 Ibid.

22 "Tanzania is weaponizing Internet shutdowns. Here's what its people have to say." December 16, 2020. https://www.accessnow.org/tanzania-internet-shutdowns-victim-stories/

23 Uganda Bureau of Statistics (2020). Highlighting Population Issues Through Statistics. Uganda Bureau of Statistics. Accessed July 5, 2021. https://www.ubos.org/wp-content/uploads/publications/07_2020WORLD-POPULATION-DAY-BROCHURE-2020.pdf

24 Uganda Communications Commission (2020). Market Performance Report 3 Q20. Uganda Communications Commission. Accessed July 5, 2021. https://www.ucc.co.ug/wp-content/uploads/2021/01/MARKET-PERFOMANCE-REPORT-Q3-2020-Final-compressed.pdf

25 Aljazeera (2021). Museveni declared winner of disputed Uganda presidential election. https://www.aljazeera.com/news/2021/1/16/ugandas-museveni-declared-winner-of-presidential-election

26 Accessnow (2018). Time is up: Uganda in Court over internet shutdowns that violate human rights. Accessed July 17, 2021. https://www.accessnow.org/uganda-in-court-over-internet-shutdowns/

27 Ibid.

28 Daily Monitor (2018). Government moves to block VPN as Ugandans vow to dodge social media tax. https://www.monitor.co.ug/uganda/news/national/government-moves-to-block-vpn-as-ugandans-vow-to-dodge-social-media-tax-1765758

29 Assessing the impact of social media on political communication and civic engagement in Uganda. Konrad Adenauer Stiftung. https://www.kas.de/c/document_library/get_file?uuid=95eec5bf-c11c-c4eb-f504-90a4e5a4d54d&groupId=252038

30 Switching off the Internet has a huge cost; it must never happen again. Daily Monitor. https://www.monitor.co.ug/uganda/business/prosper/shutting-the-internet-must-never-happen-again--3277616

31 Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework. https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

32 DR Congo: Restore Internet services as "a matter of urgency," urges UN expert. United Nations. Accessed on July 6, 2021. https://news.un.org/en/story/2019/01/1029952

33 Patient Ligodi, Congo orders Internet slowdown to restrict social media: telecoms source. https://tinyurl.com/rlrvf8d

34 How Telecom Companies in Africa Can Respond better to Internet disruptions. CIPESA. Accessed online June 26, 2021. https://cipesa.org/?wpfb_dl=435

35 "Ending Internet shutdowns: a path forward: Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association." June 15, 2021. A/HRC/47/24/Add.2. https://undocs.org/A/HRC/47/24/Add.2

36 "Internet Society Position on Internet Shutdowns." December 17, 2019. https://www.internetsociety.org/resources/doc/2019/internet-society-position-on-internet-shutdowns/

37 Policy Brief: Internet Shutdowns. Internet Society. https://www.internetsociety.org/policybriefs/internet-shutdowns/#_edn17

38 Ibid.

39 "Africa Internet: Where and How Are Governments Blocking it," January 14, 2021. https://www.bbc.co.uk/news/world-africa-47734843

40 Ibid. Regarding access in neighboring countries, a local ISOC representative in Tanzania said that neighboring countries, including Kenya, did not seem to be affected. However, asymmetric disruptions to DNS are not more likely to affect a geographic neighbor than they are a "network neighbour." This is especially the case when the shutdown impacts general Top Level Domains, for instance, those registered under .com. In such a scenario, it is possible that a local Internet in Africa could have some global effects. More research is urgently needed.

41 "DR Congo: Internet, SMS shutdown threatens credibility of election" https://www.dw.com/en/dr-congo-internet-sms-shutdown-threatens-crediblity-of-election/a-46917740

42 EU Condemns Internet Shutdown, Security Excesses as Uganda Votes. January 20, 2021. https://ugandaradionetwork.net/story/eu-condemns-internet-shutdown-security-excesses-as-uganda-votes-

43 "A Human Rights Based Approach to Network Disruptions" https://globalnetworkinitiative.org/wp-content/uploads/2018/06/Disconnected-Report-Network-Disruptions.pdf

44 "Ending Internet shutdowns: a path forward: Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association." June 15, 2021. A/HRC/47/24/Add.2. https://undocs.org/A/HRC/47/24/Add.2

45 Article 29 of the Constitution of Uganda provides for protection of freedom of expression, assembly, and association. Articles 23–25 of the Congo's Constitution guarantee citizens the right to freedom of expression, assembly, and association. See: https://cepa.or.ug/wp-content/uploads/2018/06/300460141-ARTICLE-29-THREATENED-A-CRITICAL-DISSECTION-OF-VARIOUS-LAWS-PASSED-THAT-UNDERMINE-FUNDAMENTAL-FREEDOMS-OF-SPEECH-EXPRESSION-ASSEMBLY.pdf ; https://cipesa.org/?wpfb_dl=234

46 Internet shutdowns and elections handbook. A guide for election observers, embassies, activists, and journalists. Accessnow. Accessed July 2, 2021. https://www.accessnow.org/internet-shutdowns-and-elections-handbook/

47 "Ending Internet shutdowns: a path forward: Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association". June 15, 2021. A/HRC/47/24/Add.2. https://undocs.org/A/HRC/47/24/Add.2

48 Uganda: Authorities must lift social media block amid crackdown ahead of election. Amnesty. Accessed online June 24, 2021. https://www.amnesty.org/en/latest/news/2021/01/uganda-authorities-must-lift-social-media-block-amid-crackdown-ahead-of-election/

49 Statement: Internet Shutdowns in Uganda Erode Citizen's Enjoyment of Basic Human Rights. Global Network Initiative. Accessed June 20, 2020. https://globalnetworkinitiative.org/concerns-internet-shutdowns-uganda/

50 Human Rights Committee, general comment No. 34 (2011), para. 43.

51 How internet shutdown stalled businesses. Daily Monitor. https://www.monitor.co.ug/uganda/news/national/how-internet-shutdown-stalled-businesses-3287376

52 How internet shutdown stalled businesses. Daily Monitor. https://www.monitor.co.ug/uganda/news/national/how-internet-shutdown-stalled-businesses-3287376

53 The Cost of Internet Shutdowns: Uganda, January 2021. Internet Society Pulse. https://pulse.internetsociety.org/blog/5026

54 Ibid.

55 Policy Brief: Internet Shutdowns. Internet Society. https://www.internetsociety.org/policybriefs/internet-shutdowns/#_edn17

56 "Tanzania: Internet slowdown comes at a high cost." Accessed August 4, 2021. https://www.dw.com/en/tanzania-internet-slowdown-comes-at-a-high-cost/a-55512732

57 "Ending Internet shutdowns: a path forward: Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association." June 15, 2021. A/HRC/47/24/Add.2. https://undocs.org/A/HRC/47/24/Add.2

58 "Assessing the Gendered Impact of Internet Shutdowns," presented by Sarah Shoker (2020). https://konnect.serene-risc.ca/2021/03/11/assessing-the-gendered-impact-of-internet-shutdowns/

59 J. Rydzak, Disconnected: A Human-Rights Based Approach to Network Disruptions (2018). Global Network Initiative. https://globalnetworkinitiative.org/wp-content/uploads/2018/06/Disconnected-Report-Network-Disruptions.pdf. Accessed August 4, 2021.

60 "Ending Internet shutdowns: a path forward: Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association". June 15, 2021. A/HRC/47/24/Add.2. https://undocs.org/A/HRC/47/24/Add.2

61 Ibid.

62 Ibid.

63 Ibid.

64 Ibid.

65 Ibid.

66 Ibid.

67 Ibid.

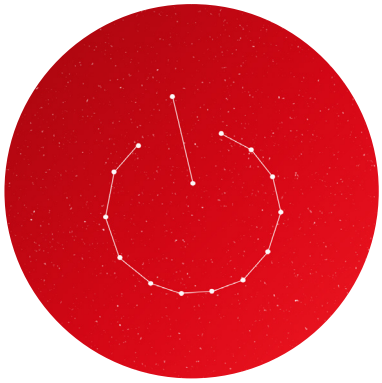
68 Ibid.

69 Ibid.

About the Authors

Moses Owiny is the Founder and Chief Executive Officer at the Centre for Multilateral Affairs (CfMA) in Uganda. The CfMA is a platform that seeks to aid policy thinking as well as contribute to research and the body of knowledge, integrating Global South perspectives in domestic, regional, and global policy discourses. His recent research work in Uganda focused on cybersecurity and state capacity. In June 2021, he served as an external co-chair and Programme Committee member for the 10th edition of RightsCon under the category "Cyber Norms, Accountability, and Practice."

Sheetal Kumar currently provides strategic oversight for a global cybersecurity capacity-building programme that supports civil society organizations from the Global South, to protect and promote human rights in cybersecurity- and cybercrime-related discussions. She also facilitates civil society engagement in key relevant forums, including the UN, through research, facilitation, and coordination support on a day-to-day basis. Her recent work has focused on applying human-centric approaches to cyber policy, including cyber norms.



About the Cyberstability Paper Series

Since the release of the final report of the Global Commission on the Stability of Cyberspace in November 2019, the concept of cyberstability has continued to evolve. A number of new 'conditions' are emerging: new agreements on norms, capacity building and other stability measures have been proposed and solidified within the United Nations and elsewhere, and stakeholders are exploring ways to increase stability and minimize the risk of conflict in cyberspace through technical fixes or governance structures. The constellations of initiatives involved in working towards cyberstability is expanding, underlining the need to connect the traditional state-led dialogues with those of the Internet communities from civil society and industry. Gaps continue to close, between the global north and south, between technology and policy, but also the stability in and the stability of cyberspace.

The first Cyberstability Paper Series explores these "New Conditions and Constellations in Cyber" by collecting twelve papers from leading experts, each providing a glance into past or future challenges and contributions to cyberstability. The papers are released on a rolling basis from July until December 2021, culminating in an edited volume. All papers will be available for open access, and a limited number of printed hardback copies are available.

Published by

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

The Hague Centre
for Strategic Studies