SERIES ON DIGITAL RIGHTS AND INTERNET FREEDOM

Topic 1: Internet Shutdowns

Internet Shutdowns

Author: The Centre for Intellectual Property and Information Technology Law (CIPIT).

About CIPIT	About GIF
The Centre for Intellectual Property and Information Technology Law (CIPIT) is an evidence-based research and training Centre based at Strathmore University, Nairobi, Kenya. CIPIT was established in 2012 and focuses on studying, creating, and sharing knowledge on the development of intellectual property and information technology utilizing diverse methodological approaches to inform debates on ICT applications and regulation.	The Greater Internet Freedom Project (GIF) is a three-year, consortium-based, global program implemented by Internews and the GIF consortium across 39 countries. GIF places regional and local organizations at the forefront of the fight to preserve an open, reliable, secure, and interoperable Internet – and, by extension, protects the citizens, civic actors, journalists, and human rights defenders who rely on it to realize fundamental freedoms.

Table of Contents

Introduction

The CIPIT and the GIF have developed exploratory material relevant to pertinent digital rights and internet freedom topics. The 'Internet Shutdowns' topic examines efforts to promote the unhindered access and use of the Internet. It delves into three issues, including causes and motivations of shutdowns, the societal and economic impacts, legal frameworks and activism.

Internet shutdowns are becoming increasingly common across GIF countries as governments around the world attempt to maintain control of their citizens. This practice is detrimentally impacting individuals and communities. At the forefront of the opposition movement contesting internet shutdowns are three critical arguments: the human rights, social, and the economic standpoints.

These standpoints emphasize the detrimental impact of internet shutdowns on individuals and communities, as well as the adverse effects on governmental interests and public trust. These shutdowns not only curtail citizens' access to information and communication but also hinder economic growth, social cohesion, and state stability. Additionally, curtailing access to the internet is diametrically opposed to global calls to bridge the ever-growing digital divide (*see Topic 5: Digital Divides*).

The definition of an internet shutdown varies amongst organizations and GIF regions. Key considerations that influence the categorization and understanding of internet shutdowns include differing legal and policy frameworks, technological understanding and capacities, cultural norms, control mechanisms, amongst others.

Leading global champion against internet shutdowns, Access Now, under its #KeepItOn campaign, has taken steps to advance technical and non-technical definitions of internet shutdowns.

Non-technical definition: an internet shutdown is "*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.*"[1]

This definition complements the definition advanced by the Internet Society in 2019, which defines internet shutdowns as "*a deliberate interruption of the internet or electronic communications, making them inaccessible or effectively unusable for a particular location or population.*"[2]

Technical definition: an internet shutdown is an "*interference with electronic systems primarily used for person-to-person communications, intended to render them inaccessible or effectively unusable, to exert control over the flow of information.*"[3]

Generally, internet shutdowns are practically enforced by government authorities, at the local and national levels, often coopting support from private actors such as private and state-owned ISPs. As argued by the AIRA Coalition:

> "*It is important to recall that internet shutdowns 'rarely stem from intentional damage to the internet's physical infrastructure.' Instead, state actors prevent access at the service provision level, implicating governments, who give the 'kill-switch' orders, but often deny complicity, and private and state-owned ISPs, who implement shutdown orders, but often deny an intentional violation of human rights.*"[4]

> **Resource: Access Now's Internet Shutdowns Mid-Year Update, 2023**
>
> *Access Now, a digital rights international nonprofit organization, released its 'Who is shutting down the internet in 2023? A mid-year update,' documenting 80 internet shutdowns between January – May 2023. The top offenders in 2023 include the governments of Ethiopia, India, Iran, and Russia. The highest recorded internet shutdowns were*

This paper restricts itself to an exploration of the following complex challenges:

Internet Access and Internet Shutdowns: this briefly explores how individuals' and communities' ability to freely connect to and use the internet without interruption is negatively impacted by internet shutdowns.

Causes and Motivations: this explores the leading causes and motivations of internet shutdowns in 2023.

Impacts on Society and Economy: this examines the societal and economic impacts of internet shutdowns.

Legal and Policy Frameworks and Activism: this outlines legal instruments commonly relied on to push back against internet shutdowns, in the absence of a universal right to access the Internet. Examples of reliance on these frameworks by various intergovernmental organizations and private entities to propel activism and advocacy against internet shutdowns is also explored.

Internet Access and Internet Shutdowns

Generally, the ability of individuals to connect to and use the Internet using digital devices such as smartphones/digitally enabled devices, laptops, or computers, is loosely referenced as 'internet access.'[5] No express right to access the Internet has been provided in international law, but there are expanding calls for a globally recognized right to universal internet access by 2030.[6]

Despite the lack of an express right, the Internet enables and facilitates a wide range of human rights, such as the right to freedom of expression, freedom of association, access to information amongst other (*see GIF Topics 2 & 3 on 'Freedom of Expression Online' and 'Access to Information' respectively*).[7]

Universal access is an aspirational effort and goal being pursued by states across GIF regions for purposes of ensuring equitable economic development and advancing human rights.[8] This would mean that no one, irrespective of location, socio-economic status, amongst other factors, would be denied access to the Internet and its associated benefits. Illustratively, in June 2023, the United States government announced its investment of "$42 billion to make internet access universal by 2030,"[9] revealing that some states are going beyond commitments.

The International Telecommunication Union (ITU) notes that internet access is unevenly distributed globally, with 5.3 billion estimated people having access to the Internet in 2022. Figure 1 below illustrates geographical disparities amongst GIF countries (*this data may be outdated*).

Figure 1: *Number of People Using the Internet. Source: Our World in Data.*
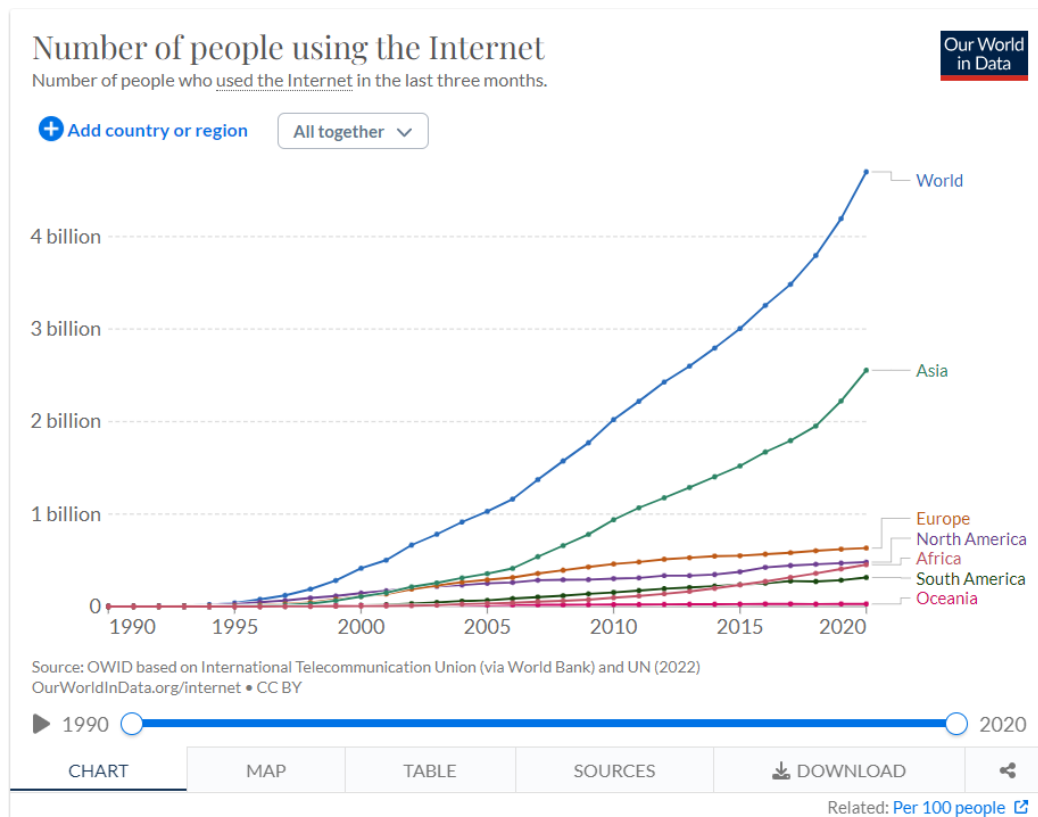
Internet shutdowns, in their varying forms, are an unjustifiable restriction on the ability of individuals and communities to access the Internet.[10] These practices impact universal access drives, socio-economic and sustainable development efforts, and the promotion of human rights globally. At the individual and community level, internet shutdowns affect many aspects of life, ranging from children's ability to access education online, workers' rights, especially for those who are part of the gig economy, amongst others.

Across GIF regions, internet shutdowns disrupt efforts to improve digital connectivity. Despite internet access lagging in the African, and Asian regions, states in these two regions are frequently flagged for disrupting internet access.

In the **Eastern Europe and Central Asian region**, the following countries disrupted the Internet in 2022, including Armenia, Azerbaijan, Kazakhstan, Russia, Tajikistan, Turkmenistan, Ukraine, and Uzbekistan.[11] These governments hampered people's ability to communicate or exercise their freedom of expression and association, evidencing disproportionate internet access limitations. As demonstrated in these instances, lack of internet access through internet censorship led to violations of other human rights such as access to information, the right to life, and freedom of expression and association.

In the **Latin America and Caribbean (LAC) region**, 'about three-quarters of the population uses the internet,' even though they frequently experience low quality Internet connections, frequent power outages, and high service fees' which restricts users' access to the internet.[12]

Definitions and Explainers

Term	Definition/Explainer
Digital/Online Activism	The use of 'digital tools (the Internet, mobile phones, social media) to bring about social and/or political change.'[13]
Internet Service Provider	A "company that provides individuals and organizations access to the internet and other related services."[14]
Internet Shutdown (Types)	
Bandwidth/Internet/Data Throttling	This refers to an intentional slowing down of internet traffic or service at the source, e.g., by ISPs. This is geared at preventing Internet users from accessing information online, through a slowed down browsing experience.[15] This is the most used internet shutdown mechanism by governments and ISPs.
Deep Packet Inspection (DPI)	DPI filtering targets 'specific domain names that contain sensitive keywords or matches banned addressed, leading to a dropped request.' DPI is costly and expensive because it requires a 'careful inspection of all data being sent and received in real time by an Internet user.'[16]
Denial of Service (DoS) attack	This refers to a "flooding of a targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users."[17]
Domain Name System (DNS) manipulation	This includes a 'redirection of traffic

	intended for specified domains from the designated servers towards servers controlled by a perpetrator.' This results in a shutdown of targeted services, where traffic is redirected to an inexistent server.[18]
Filtering	The use of filtering devices to prevent users from accessing blocked websites. Legitimate filtering devices are illegally repurposed for internet shutdown purposes enabling government authorities to block access to social media platforms and specified websites.[19]
Fundamental infrastructure shutdown	This includes shutdowns conducted "using a method external to the communications system or brought on by actual harm to the communications infrastructure." e.g., power grid shutdowns.[20]
Routing	A routing internet shutdown entails an internet or telecommunications software shutdown. This shutdown is conducted by altering routing information at key areas of the network infrastructure, such as an international gateway, to prevent the passage of traffic to other infrastructure, interrupting the connection. An example of this shutdown occurred in Benin during the 2019 parliamentary elections, where IODA data shows an internet outage that lasted about 20 hours.[21]
Virtual Private Network	This refers to a "protected information system link utilizing tunneling, security controls, and endpoint address translation giving the impression of a dedicated line."[22]
Internet Freedom	The exercise of internationally recognized

human rights online… including the freedom to seek or impart information and ideas of all kinds regardless of frontiers through any medium.[23]

Causes and Motivations of Internet Shutdowns

Government authorities impose Internet shutdowns driven by various goals and purposes. Too often, governments invoke 'national security', 'public health', 'public interest', 'public order', 'terrorism prevention', amongst others, to justify shutdowns, which justifications have legal basis in national laws, regulatory frameworks, and policies. However, it is now commonly acknowledged that these broad justifications are rarely the real reason behind an internet shutdown. The most recently invoked reasons are explored below.

To understand the now-entrenched practice of government-orchestrated internet shutdowns, it is critical to ***examine that county's stance towards democracy and ongoing political and economic conditions***.

To Disrupt Protests and Political Unrest

Government authorities use internet shutdowns to disrupt protests and quell political unrest. In the **African region,** the Senegalese government, one of the few countries on the continent that had been hailed for shying away from shutdowns, impose an internet shutdown in June 2023. According to the Senegalese Communication Ministry, this was implemented to prevent *"the dissemination of subversive and hateful messages in a context of public disorder."[24]*

In the **Central Asia region**, the Kazakhstani government in 2022 shutdown the Internet, amidst mass protests high gas prices, resulting in hundreds of people dying due to violent crackdowns.[25]

In the **LAC region,** the Ecuador government implemented various temporary shutdowns of websites, social networks, internet connections, and mobile communications in response to a national political crisis and protests.[26] According to NetBlocks, following the death of a demonstrator in 2019, state-run telecom

provider *Corporación Nacional de Telecomunicaciones* banned servers for social media apps like WhatsApp and Facebook.[27]

To Limit the Transfer of Foreign Propaganda

Internet shutdowns are used to limit the spread of foreign propaganda, often disseminated through social media and other online platforms. The **Eastern European region** has recorded high internet shutdowns since the commencement of Russia's aggression against Ukraine, and violent protests. Russia was the 'biggest executor of these shutdowns, issuing about 22 shutdowns inside Ukraine and 2 on Russian soil.'[28]

To Weaken Opposition, Dissent and Minority Groups

Authoritarian governments commonly use internet shutdowns to restrict the flow of information and communication to stifle dissent and weaken minority groups, with Ethiopia standing out as a repeat offender.

In **Ethiopia, Africa region**, the government has implemented a 2.5-year long internet shutdown in Tigray, preventing the spread of information on human rights abuses and war crimes during the Tigray War.[29] These shutdowns are used to weaken Tigray opposition forces, with this tactic, i.e., shutting away conflict areas from the world gaze, being replicated in the Oromia region in 2020. During this period, the government shut down internet access for over two months while the government conducted military operations against the Oromo Liberation Front, an armed militia in the region.[30]

Impacts on Society and the Economy

Internet shutdowns have a profound impact on societies and economies. Generally, internet shutdowns impact the free and unfettered exercise of civil and political rights,

thwart universal internet access efforts, hinders socio-economic development, and serves as direct evidence that states have failed to uphold their obligation to protect, promote, and fulfil their human rights obligations.[31]

Widening Societal and Economic Inequalities: Internet shutdowns exacerbate ongoing societal and economic inequalities amongst a nation's citizenry. Illustratively, shutdowns magnify the disparity between those who have access to technologies required to bypass shutdowns, such as purchasing VPNs, and those who are unable to access this technology, leaving the latter group at risk of an information blackout. The ability to purchase bypass technologies is reflective of purchasing power differences between populations, magnifying how internet shutdowns underscore the income gaps existing between low-income and higher-income households within a nation.

Additionally, individuals and communities living in rural areas are often disproportionately affected by internet shutdowns due to a lack of access to reliable broadband connectivity. Further, in an environment where shutdowns are used by governments, people unable to bypass shutdowns cannot continue to competitively access and use online resources and platforms, including sourcing job opportunities, magnifying the divide between rural-urban populations.

Reduced Economic Growth and Investment: Internet shutdowns impact ongoing digital transformation and digital economy efforts, hindering the growth of the ICT sector, which contributes extensively to a country's Gross Domestic Product. While the economic cost of internet shutdowns was relatively unknown around mid-2010s, more reports have uncovered the real economic cost of internet shutdowns on economic activities. In 2023, TopVPN found that "government internet disruptions have cost the global economy $42.71 billion since 2019, and resulted in 445 significant internet shutdowns in 54 countries."[32]

The economic impact of internet shutdowns is wide ranging:

"they halt e-commerce, generate losses in time-sensitive transactions, increase unemployment, interrupt business-customer communications, and create financial and reputational risks for companies."[33]

<div style="border:2px solid; background-color:#c3e03f; padding:10px;">

Resource: Internet Society NetLoss Calculator

"The NetLoss calculator is a new tool that estimates the economic cost of Internet shutdowns by way of a rigorous methodology. The NetLoss calculator uses a reproducible, econometric framework to consider a wide range of publicly available economic inputs including:
   a. Shutdown data;
   b. Protests and civil unrest;
   c. Elections;
   d. Socioeconomic indicators
   e. Additional factors impacting country-specific economic outcomes: rate of inflation (percentage), age dependency ratio (percentage of working people ages 18-65 to total population), the fraction of the population residing in urban areas, and the percentage of the labor force with basic education."

Sources: Internet Society.

</div>

Violations of Human Rights: Internet shutdowns are a gross violation of fundamental human rights and freedoms, including but not limited to the right to freedom of expression, the right to access information, the right to freedom of association and privacy rights. Further, research indicates that internet shutdowns are often accompanied by a long-term state repression of minority voices, dissenters and political opposition.[34]

Legal and Policy Frameworks and Activism

A key factor in the fight against internet shutdowns is international, regional and national instruments. One of the most important aspects of legal and policy frameworks in the context of internet shutdowns is their ability to provide a platform for activism. Activism helps create awareness about internet shutdowns, provides support for those affected by them, and encourages individuals to take action against them. Activism further provides

individuals and communities with an opportunity to make their voice heard, making it an essential tool in addressing inequalities in society.

In the absence of a universal, codified, right to access the Internet under international human rights law (IHRL), various global treaties, such as the ICCPR, can be relied on, leveraging the applicability of human rights, such as freedom of expression online. Aside from binding legal instruments, digital activists can also leverage soft law instruments, such as the UN Human Rights Council resolutions condemning internet shutdowns and calling upon States to cease and refrain from such measures.[35] Further, a key concept that digital rights and Internet freedom advocates can continue to leverage is that of *net neutrality*, which requires all internet data be treated equally without undue interference.[36]

Table 1: Selected Resources - Freedom of Expression, International and Regional Instruments

Global Instruments
Universal Declaration of Human Rights (UDHR), 1948
International Covenant on Civil and Political Rights (ICCPR), 1966
Africa: Regional Instruments
African Charter on Human and Peoples' Rights (ACHPR), 1986
Declaration of Principles on Freedom of Expression in Africa, revised in 2019
Guidelines on Freedom of Association and Assembly in Africa, 2017
Asia: Regional Instruments
Association of Southeast Asian Nations (ASEAN) Human Rights Declaration, 2009
Balkans (Europe): Regional Instruments
Charter of Fundamental Rights of the European Union, 2009
Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, or ECHR), 1953

Latin America and the Caribbean: Regional Instruments
[American Declaration of the Rights and Duties of Man](#) (1948)
[American Convention on Human Rights](#) (1969)
[Inter-American Democratic Charter](#) (2001)

In addition to legal instruments, activists can leverage inter-governmental initiatives, such as the Freedom Online Coalition (FOC) which lends strong support to human rights in the digital sphere.[37] Further, at regional levels, a number of regional mechanisms provide avenues for stakeholders to raise awareness about the prevalence of internet shutdowns, such as African Commission on Human and Peoples' Rights (ACHPR) is well known for monitoring and promoting freedom of expression online.

Resource: Media Defence Litigating Internet Shutdowns

Media Defence, details how it has leveraged international instruments and activism before courts to contest internet shutdowns in Togo, Indonesia, and Nigeria (Twitter ban).

"Pursuing strategic litigation at regional and international courts is one of the most effective tools in our fight to protect freedom of expression. By helping to develop significant legal precedents, we can contribute to bringing about long-term changes to legislation and practices, often across multiple jurisdictions simultaneously. Even in instances where a judgment is not as far-reaching as we would like or, as in the Togo case, where the judgment has yet to be fully implemented by the government, the exercise is still necessary. Bringing cases before a court can act as a way of documenting human rights abuses and raising awareness of the key challenges to freedom of expression in the respective region or country, paving the way for future legal challenges or campaigning."

Source: [Media Defence](#).

Supplementary Resources

Legal Instruments (International, Regional, National)

African Charter on Human and Peoples' Rights (ACHPR), 1986.

American Convention on Human Rights (1969).

American Declaration of the Rights and Duties of Man (1948).

Association of Southeast Asian Nations (ASEAN) Human Rights Declaration, 2009.

Charter of Fundamental Rights of the European Union, 2009.

Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, or ECHR), 1953.

Declaration of Principles on Freedom of Expression in Africa, revised in 2019.

Guidelines on Freedom of Association and Assembly in Africa, 2017.

Inter-American Democratic Charter (2001).

International Covenant on Civil and Political Rights (ICCPR), 1996.

Universal Declaration of Human Rights (UDHR), 1948.

Reports

Access Now (2022). A Taxonomy of Internet Shutdowns: the Technologies behind Network Interference.

Access Now (2022). KeepItOn: Fighting Internet Shutdowns around the World.

Berhan Taye (2018). The State of Internet Shutdowns around the World.

Brookings (2016). Internet Shutdowns Cost Countries $2.4 Billion Last Year.

NetBlocks. (2019). Regional internet disruptions in Nicaragua amid protests.

Sigi Mwanzia, Victor Kapiyo & Odanga Madung (2021). Study on Internet Shutdowns in Africa.

The Association for Progressive Communications (2022). Internet Shutdowns and Human Rights.

Websites and Blogs

Access Now (2023). Global Coalition to Indian Government: Reform Legal Framework on Internet Shutdowns.

Body of European Regulators for Electronic Communications (2022). BEREC Guidelines on the Implementation of the Open Internet Regulation.

OONI Explorer.

Sarthak Gupta (2023). Internet Shutdowns in Asia: Locating the Right to the Internet a Human Right under International Human Rights Law.

Statista (2022). Economic Cost of Internet Shutdowns Worldwide 2021.

References

[1] Access Now (2016). No more internet shutdowns! Let's #KeepItOn.

[2] Internet Society (2019). Policy Brief: Internet Shutdowns.

[3] Access Now (2022). A Taxonomy of Internet Shutdowns: The Technologies behind Network Interference

[4] The African Internet Rights Alliance (2021). Study on Internet Shutdowns in Africa, 2021.

[5] Technopedia (2016). Internet Access.

[6] OHCHR (2023). It May be Time to Reinforce Universal Access to the Internet as a Human Right, Not Just a Privilege, High Commissioner tells Human Rights Council; Media Defence. Module 3: Access to the Internet.

[7] Paul Garnett (2021). Accelerating Universal Digital Connectivity UNDP Regional Bureau for Asia and the Pacific Strategy, Policy and Partnerships Policy Brief.

[8] *Ibid.*

[9] Reuters (2023). US to spend $42 billion to make internet access universal by 2030.

[10] OHCHR (2022). Internet Shutdowns and Human Rights.

[11] Access Now (2023). Internet Shutdowns in Eastern Europe and Central Asia: Attacks on Human Rights.

[12] Gabriel Lara Ibarra, Niccolò Comini & Natalija Gelvanovska-Garcia (2022). Universal, affordable, and reliable Internet connectivity is a key ingredient for inclusive recovery.

[13] Internet Matters (2022). Online activism, social media, and young people.

[14] Tech Target. What is an ISP?

[15] Access Now (2018). The State of Internet Shutdowns around the World.

[16] Surfshark. How blocking works.

[17] Cybersecurity and Infrastructure Security Agency (2021). Understanding Denial-of-Service Attacks.

[18] *Ibid, n. 3.*

[19] *Ibid, n. 3.*

[20] *Ibid, n. 3.*

[21] *Ibid.*

[22] NIST. Glossary - Virtual Private Network.

[23] US Department of State. Internet Freedom Fact Sheet.

[24] Leo Komminoth (2023). Senegal's internet shutdown threatens business losses.

[25] Access Now (2022). Weapons of Control, Shields of Impunity: Internet Shutdowns in 2022.

[26] Association for Progressive Communications (2022). Internet Shutdowns and Human Rights.

[27] NetBlocks (2019). Evidence of social media disruptions in Ecuador as crisis deepens.

[28] Access Now (2022). Weapons of Control, Shields of Impunity: Internet Shutdowns in 2022.

[29] Access Now (2023).

[30] Access Now (2023). Who is shutting down the internet in 2023? A mid-year update.
 "Ethiopia: Communications Shutdown Takes Heavy Toll" (Human Rights WatchOctober 28, 2020) <https://www.hrw.org/news/2020/03/09/ethiopia-communications-shutdown-takes-heavy-toll> accessed April 24, 2023

[31] The African Internet Rights Alliance (2021). Study on Internet Shutdowns in Africa, 2021.A

[32] Omoleye Omoruyi (2023). Economic impact of internet shutdowns from 2019-2023 as governments get bolder.

[33] Robert Mitchell (2023). The Real Impact of Internet Shutdowns.

[34] Media Defence (2023). 15 Years of Impact: Internet Shutdowns.

[35] UNHRC (2021). *Resolution on the promotion, protection and enjoyment of human rights on the Internet (*A_HRC_RES_47_16-EN)*.*

[36] *Ibid at 12.*

[37] Freedom Online Coalition. About us.