STUDY ON INTERNET SHUTDOWNS IN AFRICA, 2021

September 2021

THE AFRICAN INTERNET RIGHTS ALLIANCE (AIRA)

The African Internet Rights Alliance (AIRA), comprised of:

- Amnesty International Kenya
- ARTICLE 19 Eastern Africa
- BudgIT Nigeria
- Co-Creation Hub (Cc-HUB)
- Centre for Intellectual Property and Information Technology Law (CIPIT)
- Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
- iHub
- Kenya ICT Action Network (KICTANet)
- Legal Resources Centre (LRC)

- Paradigm Initiative (PIN)

E: info@aira.africa
W: https://aira.africa

Tw: https://twitter.com/aira_africa
FB: https://www.facebook.com/African-Internet-Rights-Alliance-100119391805279/
LI: https://www.linkedin.com/company/aira-africa

Authored by
Sigi Waigumo Mwanzia, Victor Kapiyo, and Odanga Madung.

Designed by
Odanga Madung.

Support
This work was supported by the African Internet Rights Alliance through the Ford Foundation. We would like to thank the AIRA Policy Committee Reference group and the team at Akijul for providing crucial support, and members of AIRA for reviewing the report. The views expressed in this report are the authors' and do not necessarily reflect those of the individual AIRA members or the Ford Foundation. The African Internet Rights Alliance (AIRA) bears sole responsibility for the content. All errors remain our own.

Table of Contents

List of Abbreviations

ACHPR	African Commission on Human and Peoples' Rights
AfCFTA	African Continental Free Trade Area
African Charter/Banjul Charter	African Charter on Human and Peoples' Rights
AU	African Union
COST	Cost of Shutdown Tool, NetBlocks
CSO	Civil society organisation
DNS	Domain Name System
EAC	East African Community
EACJ	East African Court of Justice
EACO	East African Communications Organisation
ECOWAS	Economic Community of West African States
GDP	Gross Domestic Product
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and Communications Technology
ISP	Internet Service Provider
ITU	International Telecommunications Union
OHCHR	Office of the High Commissioner for Human Rights
PIL	Public Interest Litigation

REC	Regional Economic Communities
SSA	Sub-Saharan Africa
Telecom	Telecommunications
UN	United Nations
VPN	Virtual Private Network

Executive Summary

This section provides an overview of the report.

This report by the African Internet Rights Alliance (AIRA) reviews the trend of internet shutdowns in ten African countries. These include Cameroon, the Democratic Republic of Congo, Egypt, Ethiopia, Nigeria, Uganda, Sudan, Senegal, Zambia and Eswatini. It also documents the implications of, and analyses the recent jurisprudence on, internet shutdowns and provides recommendations to the AIRA Coalition to advance its advocacy against internet disruptions in Africa.

The Internet offers significant quantifiable and unquantifiable benefits to African users, in their capacities as both citizens and consumers. In their efforts to digitally transform and spur economic growth, increase productivity, and reduce the digital divide, governments and businesses also benefit from expanded internet access and use. Further, the Internet is central to the facilitation and exercise of a wide range of individuals' and communities' human rights, such as education and health, as evidenced during the ongoing COVID-19 pandemic. Despite these benefits, state actors, with support from internet service providers and telecom operators, are using internet disruptions to manage, regulate and even censor the use of, and access to, the Internet and internet-enabled communications platforms.

The following worrying trends and implications have been observed:

1. Between 2016 and 2021, 68 shutdowns have been documented in 29 African countries. This demonstrates that government-mandated internet disruptions are an established norm in the region, despite very little scientific or social evidence demonstrating their effectiveness.

2. A number of pointers and factors signal the likelihood of an internet shutdown occurring. These include jurisdictions with authoritarian regimes, the duration of a president's term in office, facilitating laws and policies, protests, national exams, and the election season.

3. In practice, shutdowns are typically ordered by the executive arm of government and implemented by private actors, namely telecom operators and internet service providers (ISPs). Six primary methods are used to implement full and partial shutdowns, including throttling, IP blocking, mobile data shutoffs, domain name system (DNS) interference, server name identification blocking, and deep packet inspection (DPI).

4. Private sector actors comply with internet shutdown orders from governments, relying on compliance with national law requirements and licensing agreement obligations. This reveals that political and legal contexts affects their baseline responsibility to respect human rights.

5. Strategic Public Interest Litigation (PIL) is a useful tool for contesting the legality of internet shutdowns, before national and regional courts. PIL has been used in Africa to push for the recognition of the right to access the Internet; to hold governments accountable for human rights violations; and to obtain redress for affected individuals and communities. However, various barriers impact the effectiveness of strategic PIL, including weakened legislative and judicial institutions, the enforceability of judicial orders, amongst others.

6. Internet shutdowns in Africa have negatively impacted civil and political rights and efforts to expand and maintain uninterrupted use of the Internet, amongst others. Further, internet shutdowns have also restricted offline civic spaces for CSOs and citizens who increasingly rely on access to the Internet and digital platforms for mobilisation purposes, e.g, during protests.

This report recommends that the AIRA adopt a multi-pronged approach to its research, advocacy and communications efforts, before, during and after an internet shutdown. The following are the key (summarised) recommendations to AIRA:

1. AIRA Coalition Recommendations

1. Build the capacity and technical expertise of its members to be able to track and monitor internet shutdowns, given the evolution of internet censorship tactics.
2. Leverage on, and utilise, members' existing relationships and contacts with relevant stakeholders to advance national and regional multi-stakeholder advocacy efforts.

2. Stakeholder Recommendations

a. Funders:

i. Seek general and long-term funding support for the coalition's work.

ii. Leverage on the monetary, and social capital of funders, based on their priorities.

b. Civil Society:

1. Adopt a multi-pronged approach to Internet shutdowns.
2. Leverage on members' network to encourage more CSOs in Africa to join and actively participate in existing campaigns and coalitions contesting Internet shutdowns.

c. Media

1. Leverage relationships with regional and international media (broadcasting, print and digital media) to enhance reporting on shutdowns..

2. Work with content producers to capture, simplify and translate the meaning of Internet shutdowns, measures to bypass Internet shutdowns, amongst others, to local populations.

d. Regional and International Mechanisms
    1. Identify strategic and joint advocacy opportunities at the regional and global levels that AIRA coalition members cannot individually tackle by themselves.
    2. Leverage on the ACHPR's Ordinary Sessions and NGO Forums for collective advocacy by AIRA Coalition Members.

e. Private Sector
    1. Work with organisations that have direct engagements with social media platforms, telcos and ISPs, and associations to advocate against internet shutdowns.
    2. Engage high-level officials and representatives of telcos and ISPs with regional reach and social media platforms at the regional level.

f. Government
    1. Proactively engage and build allies at the government level, especially within high-risk governments, who can advocate against Internet shutdowns.
    2. Petition national governments and REC's to abolish laws that permit Internet disruptions, and enact laws that guarantee digital rights and promote access to the Internet.

g. National and regional courts
    1. Partner with national and regional judicial training institutions to review the judicial education curriculum and incorporate emerging and technical digital rights and technology issues.
    2. Collaborate with key stakeholders, such as UNESCO, continental lawyers etc., working to strengthen the capacity of judiciaries within the region to develop education material for judicial officers.

This report is intended to act as a useful resource to member organisations of the AIRA, including presenting possible interventions and/or opportunities for engagement by the AIRA, in conjunction with other key stakeholders, on how to avert and/or prevent the Internet shutdowns.

1.0 Introduction

This section defines internet shutdowns; elaborates how shutdowns work in practice; and provides the study methodology.

1.1 Definition

In the past decade, there have been various definitions of what an internet shutdown is, given the evolution of techniques and technologies over time. Internet shutdowns are also referred to as "internet kill switches", "virtual curfews" or "network shutdowns".

According to the KeepITOn Campaign, coordinated by Access Now:

> *"An internet shutdown happens when someone — usually a government — intentionally disrupts the internet or mobile apps to control what people say or do. Shutdowns are also sometimes called "blackouts" or "kill switches".*

A more technical definition by Access Now describes an internet shutdown as:

> *"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 over internet infrastructure".*

AFRINIC notes that an internet shutdown is deemed to have occurred if:

> *"It can be proved that there was an attempt, failed or successful, to restrict access to the internet to a segment of the population irrespective of the provider or access medium that they utilize."*

Internet Freedom India defines an internet shutdown as:

> *"An absolute restriction placed on the use of internet services due to an order issued by a government body. It may be limited to a specific place and to specific period, time or number of days. Sometimes it can even extend indefinitely. An internet shutdown may be limited to mobile internet that you use on smartphones, or the wired broadband that usually connects a desktop - or both at the same time."*

According to the Digital Empowerment Foundation, "virtual curfews" or "internet shutdowns" occur when telecoms infrastructure, including mobile and internet networks, are shut off or disrupted deliberately rendering phone calls, text messaging services and internet-enabled services.

1.2 Shutdowns in Practice

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.

A joint report by Jigsaw and Access Now identifies six core methods that are used to implement full or partial internet shutdowns at the local level, with variances depending on the scope, scale, target and level (*see Table 1 below*). Notably, multiple methods may be used in an escalating manner to effect an internet shutdown, given resource and effectiveness considerations.

It is critical to note that various circumvention tools, including virtual private networks (VPNs), enable individuals to regain access to the Internet and to internet-based communications services during a shutdown. However, these tools are useful during partial, rather than full, internet shutdowns. For example, Ethiopia's nationwide shutdown in June 2021 was imposed on up to 98% of the country, rendering circumvention tools ineffective.

Table 1: Definition of Key Shutdown Terms

Term	***Definition***	***Detection (Easy/Hard)***	***Circumvention Tools***

Throttling	The 'intentional slowing of an internet service/data bandwidth by an ISP.' Here, "ISPs can slow – or "throttle" – connections to the point that loading websites becomes impractical or impossible."	Hard	VPNs, but not if the entire network is affected.
IP Blocking	The targeted blocking of access to specific websites and platforms in specific geographical locations, based on IP addresses and/or application.	Easy	Preemptive download of multiple VPNs Use of Content Delivery Networks (CDNs)
Mobile Data Shutoffs	The shutdown of mobile data services, especially on smartphones.	Easy	Use of other ICT devices, including laptops, tablets
DNS Interference	The use of a DNS resolver to block access to names on a block list. Consequently, a resolver can be configured to 'return no response, an invalid IP address, or the address of a different service entirely, redirecting the user to a location they didn't intend to reach.'	Easy	Using local facilities Use VPNs to send queries to an unmodified public server Use content delivery networks
Server Name Identification Blocking	The blocking of a secure connection, from hypertext transfer protocol (HTTP) to Hypertext Transfer Protocol Secure (HTTPS), following a server name identification request to a targeted service.	Easy	Multiple layers or encryption
Deep Packet Inspection (DPI)	The blocking of access to specific content using keywords and/or other content (filename, for example)	Hard	Multiple layers of encryption Use of ToR browser

1.3 Methodology

This study was conducted over two months between August and September 2021. The study collected data using three methods, including key informant interviews, online questionnaires, and the desk review of relevant literature. The research team conducted interviews and administered questionnaires to purposefully selected informants working in the region. These informants were drawn from the philanthropic sector, regional institutions, business sector, civil society organizations, human rights experts and AIRA members.

The relevant literature available in the public domain was reviewed, including data-sets, research reports, court decisions, laws, policies, and strategies. The study team used Google Spreadsheet, to collect and analyse the data on internet shutdowns in various African countries to inform the report.

The team adopted ethical, professional, and quality control standards that inculcated industry best practices during all the stages from conceptualization to the submission of the final report. We note that there were limitations to the study, such as the unavailability of data and translated information.

2.0 Mapping Internet Shutdowns in Africa

This section provides a historical context of internet shutdowns in Africa and maps the causal factors of shutdowns, pushback by civil society organisations, and the role of the private sector. It also provides illustrative case studies of internet shutdowns in select African countries, including Cameroon, Democratic Republic of Congo, Egypt, Eswatini, Nigeria, and Uganda.

2.1 Historical Context and Prevalence of Shutdowns In Africa

Government-mandated internet shutdowns are increasingly becoming an established norm in Africa, despite very little scientific or social evidence demonstrating their effectiveness. Internet shutdowns are often justified by reference to political and other concerns, including national security, public safety and order. As more individuals in the region gained access to the Internet and Internet-enabled communications services, the official rationale expanded to include the prevention of cheating during national exams, and limiting the spread of information disorders (mis-, dis- and malinformation), and hate speech.

Guinea implemented the first internet disruption in Sub-Saharan Africa (SSA) in 2007, following protests calling for former President Lansana Conté's resignation. This shutdown was a watershed moment for Africa's online rights and freedoms, and marked the earliest form of Internet censorship in SSA, under the guise of preventing mass mobilization and protests. This was subsequently followed by Egypt's nation-wide internet shutdown in 2011 - the first on the continent - in response to protests against former president Hosni Mubarak's authoritarian regime.

This country-wide shutdown revealed the mobilising power of the Internet and social media platforms during the Arab Spring protests. Additionally, Egypt's response heralded the 'era of the large-scale government-directed internet shutdown,' declining Internet freedoms and rising instances of Internet censorship. Instructively, at least 21 African countries shut down the Internet, between 2015 and 2017, despite evidence of unsuccessful attempts to silence dissidents and stop protests by curtailing online communications during the Arab Spring.

In 2019 alone, 14 African countries disrupted access to the Internet, suspended social media platforms and other communications services, or throttled connections. This is the highest number of shutdowns documented in Africa between 2015 to 2021 (*see Table 2 below*). Coincidentally, nearly 20 African countries held, or were expected to hold, elections at the local, legislative, general or presidential levels in 2019, effectively expanding the focus of shutdown monitoring from national examinations and public protests, to include electoral periods as a trigger point.

Table 2: Summary of Internet Shutdowns in Africa

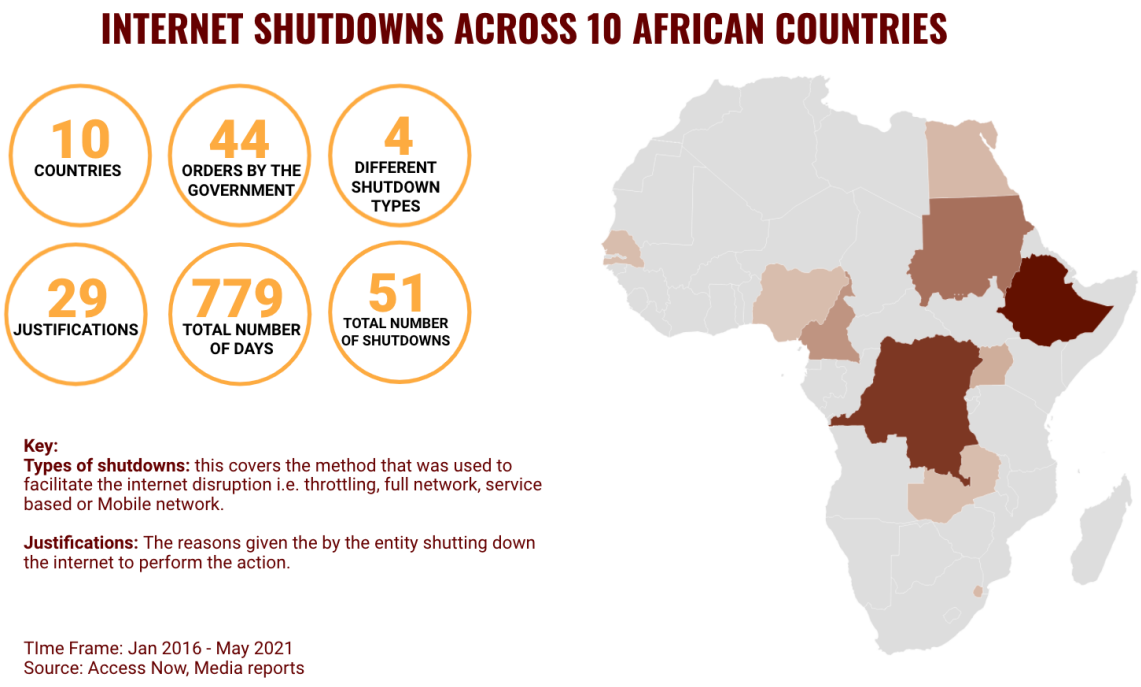
INTERNET SHUTDOWNS IN AFRICA		
Year	**No. of Shutdowns**	**Countries Affected/Involved**
2015	4	Burundi, Congo (Brazzaville), DR Congo, Niger.
2016	10	Chad, Ethiopia, Egypt, Gabon, Gambia, Niger, Mali, Republic of Congo, Uganda, Zimbabwe.
2017	7	Cameroon, Egypt, Equatorial Guinea, DR Congo, Ethiopia, Mali, Togo.

2018	12	Algeria, Cameroon, Chad, Côte d'Ivoire, DRC, Ethiopia, Mali, Mauritania, Sierra Leone, Sudan, Togo, Nigeria.
2019	14	Algeria, Benin, Cameroon, Chad, DRC, Egypt, Eritrea, Ethiopia, Gabon, Liberia, Malawi, Mauritania, Sudan, Zimbabwe.
2020	11	Algeria, Burundi, Chad, Egypt, Ethiopia, Guinea, Kenya, Mali, Sudan, Tanzania, Togo.
2021	10	Ethiopia, Eswatini, Chad, Congo, Gabon, Niger, Senegal, Nigeria, Uganda, Zambia.

Between 2020 and 2021, the number of countries which shut down the Internet fell slightly, with reports detailing disruptions in 11 and 10 countries, respectively. As Access Now observes, the decline in statistics 'can be attributed to the peculiar realities of the year,' including the emergence of the COVID-19 pandemic, but should not be the 'cause for any premature celebration', as the underlying causes could be attributed to the use of more sophisticated shutdown tools and technologies.

Across the region, longer shutdowns continue to be reported, as observed by the ongoing disruption of access to social media platforms in Uganda (Facebook, January 2021 to date) and Nigeria (Twitter, June 2021 - to date). Previously, Chad's disruption of access to social media platforms for a 472-day period was flagged as the longest between 2018 and 2019, compared to Cameroon's shutdown between January 2017 to March 2018, which lasted for a period of 240 days.

Figure 1: Internet Shutdowns in 10 African Countries



2.2 Causal Factors

The regulation of the Internet poses a unique challenge for governments across the region, owing to the decentralised architecture of the Internet, calls for a free and open Internet and the linkage of access to the Internet with individuals' ability to share, generate and access information. Various pointers and factors

signal the possible occurrence of an internet shutdown, including jurisdictions that have authoritarian governments, the duration of a president's term in office, facilitating laws and policies, protests, national exams, and the election season.

Authoritarian States: Research by CIPESA indicates that internet disruptions in Africa are mostly a preserve of authoritarian states i.e. the less the democratic credentials a government possesses, the higher the likelihood that it will order internet disruptions. Accordingly, 77% of the 22 African countries where internet disruptions were ordered between 2015 and 2019 were authoritarian. The authoritarian states included Algeria, Burundi, the Central African Republic (CAR), Cameroon, Chad, DR Congo, Congo (Brazzaville), Egypt, Equatorial Guinea, Ethiopia, Gabon, Libya, Niger, Togo, and Zimbabwe.

Longevity of President in Power: The duration which a president has spent in power increases the propensity and the likelihood of a shutdown in a country, according to findings by CIPESA. Presidents Teodoro Obiang Nguema (Equatorial Guinea), Paul Biya (Cameroon), Denis Sassou Nguesso (Congo-Brazzaville), late Idris Debi (Chad), late Robert Mugabe (Zimbabwe), and Yoweri Museveni (Uganda), had served for at least 30 years in office. Accordingly, as of January 2019, 79% of the African leaders who have been in power for more than 13 years, had ordered an internet shutdown at least once. What is also emerging is that the leaders who have taken over after the demise of some of the long serving rulers, have continued the repressive trends of shutting down the internet e.g. Prime Minister Abiy Ahmed (Ethiopia), Macky Sall (Senegal), Muhammadu Buhari (Nigeria), and Abdel Fattah Al-Sisi (Egypt).

Laws/Policies: African governments have used various laws and policies to implement and order internet shutdowns. According to Access Now, there still exist laws in nearly 30 countries where the Internet can be shut down or where a takeover of telecom platforms and networks can be implemented, by order of the law. Increasingly, laws developed to safeguard national security, preserve public order, regulate telecommunications and media, fight against terrorism, cybercrimes, hate speech and fake news have been used to enforce internet shutdowns.

For example, Article 52(1) of Rwanda's Law No. 44/2001 of 30/11/2001 Governing Telecommunications, empowers the minister in charge of telecommunications policy and law, to "interrupt or cause to be interrupted, any private communication which appears dangerous to the national integrity, contrary to law, public order or public morals". Similarly, Section 24 of Malawi's Electronic Transaction and Cyber Security Act, 2016 provides that public communications could be restricted in order to, among others, protect public order and national security, and facilitate technical restriction to conditional access to online communication.

Protests: In a number of countries, regimes have disrupted the Internet in response to protests, as evidenced in Cameroon, Chad, Ethiopia, Guinea, Liberia, Sudan, Togo, Uganda, and Zimbabwe, amongst other countries. As illustrated by CIPESA, internet shutdowns have been implemented following protests against government policies, e.g., constitutional amendments seeking to extend presidential terms for long-serving leaders, as observed in Chad (2019). These shutdowns are intended to prevent individuals from mobilising online, prevent the free flow of information online, 'plunge people into darkness', and help governments to perpetuate impunity, whilst concealing crimes and human rights violations.

Exam Season: A number of countries, including Algeria and Ethiopia, have disrupted access to the Internet as a precautionary measure to prevent cheating, curb plagiarism and other irregularities during national exams. As illustrated by Access Now, the government of Ethiopia is 'one of several countries known to have deployed internet shutdowns during school exams,' on the grounds that national exams 'are extremely important for a student's academic and professional career.'

Election Season: Internet shutdowns during elections are predictable, leading to organisations such as Access Now deploying targeted and preemptive advocacy efforts to push back against election-related shutdowns. For example, Uganda has implemented internet shutdowns during two general elections, in 2016 and 2021

respectively. In 2020 alone, shutdowns were implemented in various African countries, including Togo, Burundi, Guinea, and Tanzania, with an impact on the integrity of democratic processes.

In the last quarter of 2021, legislative, presidential or general elections are expected in Chad (October), Somalia (October), and the Gambia (December). According to the Open Technology Fund (OTF), 'almost a third of the national elections in sub-Saharan Africa were accompanied by an internet shutdown' between 2014 - 2016, under the guise of 'national security concerns and fears of the spread of fake election results.'

2.3 Pushback by Civil Society Organisations and Other Stakeholders

A number of initiatives and strategies have been deployed and used by various stakeholders to avert internet shutdowns in Africa, raise awareness about planned or ongoing disruptions, or collectively contest the legality of shutdowns. These strategies include:

A. Documenting Internet Shutdowns: Non-profit entities and privately-owned businesses, such as Open Observatory of Network Interference (OONI) and NetBlocks, conduct real-time investigations of internet shutdowns and avail publicly accessible data sets of Internet disruptions and interferences. These network measurement tools and datasets enable the documentation of shutdowns, and further facilitate a retrospective comparison of trends and patterns of shutdowns on the Continent. In 2021, OONI and the Internet Outage Detection and Analysis (IODA) explored the viability of Mozilla's Firefox to investigate internet shutdowns by 'analysing datasets of potential outage signals gathered through regular Mozilla telemetry.' In Uganda, this research revealed that the 'absence of Mozilla telemetry' between 13 - 18 January 2021 provided a 'strong indication that Uganda experienced a widespread Internet connectivity shutdown.' In turn, this research revealed that tracking Mozilla telemetry data is a valuable resource for the Internet freedom community. Additionally, the #KeepItOn database on Internet shutdowns provides useful data of the trends on internet shutdowns across the world, including in several African countries.

B. Research and Reports on Internet Shutdowns in Africa: The documentation of the trends and the issues surrounding internet shutdowns is a notable achievement by CSOs. Through its OPTIMA Project, Internews has, since 2019, developed resources, training, research and tools for CSOs, journalists, lawyers, academics, and activists to better prepare for, respond to, and advocate against internet shutdowns. The SALC report on 'Navigating Litigation During Internet Shutdowns in Southern Africa' provides useful insights and guides for legal practitioners and activists. Through their various research reports, CIPESA and Access Now have provided varied analyses of the trends on internet shutdowns in Africa. Moreover, Access Now's Shutdown Lawsuit Monitor provides useful information on petitions, lawsuits, appeals, and other court actions against telcos and governments for internet shutdowns.

C. Strategic Public Interest Litigation: In Cameroon, Veritas Law with the assistance of Media Defence, filed a case at the Constitutional Council for the government to restore access after an internet shutdown that lasted 93 days. Soon after the filing of the case, the President ordered that access to the internet be restored without the need for a judicial determination. A second case relating to the shutdown was filed by Access Now and Internet Sans Frontières seeking remedies for the shutdown. Similarly, in Zimbabwe, the Zimbabwe Lawyers for Human Rights and the Media Institute of Southern Africa - Zimbabwe Chapter filed an application challenging the internet shutdown in the country in January 2019. The Zimbabwean High Court ordered mobile operators in the country to immediately and unconditionally resume the provision of internet services and ensure unrestricted access to the internet for all subscribers.

D. **Digital Rights Partnerships:** To enable a unified and non-duplicitous approach to the protection and promotion of digital rights on the continent, CSOs have either entered into bilateral partnerships or formed loose or formal coalitions to promote Internet freedom and decry Internet censorship. For example, in 2021, the Internet Society and the CIPESA, entered into a formal partnership committing to the measurement, tracking and reporting on the 'health of digital infrastructure', including the Internet, in Africa. Coalition groupings, such as the African Declaration on Internet Rights and Freedoms, the AIRA, and the #KeepItOn coalition, have brought together multi-stakeholders in Africa and beyond to collectively contest Internet shutdowns in Africa. The #KeepItOn Coalition was formed in 2016 and its membership comprises more than 240 organizations in 105 countries around the globe. The coalition's primary objective is to drive the #KeepItOn campaign which aims to fight internet shutdowns through grassroots advocacy, direct policy-maker engagement, technical support and legal interventions. The campaign has been successful in tracking and documenting 155 internet shutdowns in 29 countries in 2020.

E. **National and Regional Convenings:** To enable collaborative action against internet shutdowns, CSOs have organised national and regional convenings. These have enabled information sharing on evolving government practices and tactics to disrupt access to the Internet, including innovative strategies to hold States accountable for violating digital rights and freedoms, and the mobilisation of collective action to push back against Internet shutdowns. For example, in 2019, the West Africa Media Excellence Conference and Awards hosted an experience-sharing and advocacy-learning session on Internet shutdowns, in the lead up to 5 West African elections in Burkina Faso, Côte d'Ivoire, Ghana, Guinea and Togo (2020). Further, annual convenings by CSOs, including those hosted by AIRA members, provide useful platforms for stakeholders. For example, the Africa Digital Rights and Inclusion Forum (DRIF), Forum on Internet Freedom in Africa, and Africa Internet Governance Forum (IGF) have enabled stakeholders to collaborate, advocate, and highlight the situation of digital rights in Africa, including the effects and impacts of internet shutdowns across the continent.

F. **Training of Litigators**: Building the capacity of litigators remains an important aspect in promoting effective digital rights litigation. CSOs, such as the Media Legal Defence Initiative (MLDI), have conducted several training and litigation surgeries. These have helped to build the capacity of internet activists and lawyers to collaborate and effectively push back against regressive legal frameworks that restrict internet access through strategic PIL.

2.4 The Private Sector Involvement

It is acknowledged that African countries with access to, and control over, the internet's physical infrastructure state have greater incidences of internet shutdowns. This is illustrated by Ethiopia's control over the sole telecommunications provider, EthioTelecom, resulting in Ethiopia having the most number of shutdowns in the region (*see figure 1 above*). Despite this, private sector actors, typically ISPs and telecom companies, have willingly complied with internet shutdown orders from governments, despite the crucial role they play to expand communications services in the region and their baseline responsibility to respect human rights in all situations.

Research by the OTF identifies three ways in which governments ensure that privately-owned (foreign) companies comply with their internet shutdown requests. These include the 'general business environment in authoritarian developing countries' where 'big companies seek to maintain close relationships with the

government to facilitate their business affairs.' The second mechanism is 'through the board of directors', with OTF noting that the board composition and leadership of some ISPs consists of 'local business elites with close ties to the government, even if shareholders are predominantly from abroad… These people are commonly referred to as 'facilitators' as they serve as channels for the government to leverage the companies' corporate actions and strategies.' Thirdly, OTF observed that 'the friendship between authoritarian rulers across borders' and diplomatic channels have enabled private companies run by 'friendly foreign governments…to facilitate government control of the companies.'

The exact circumstances of compliance by private companies with shutdown orders is still blurry, due to failures to disclose the terms and conditions of their operating licenses or to issue statements following the receipt of shutdown orders. However, a few statements issued by private and foreign-owned companies, such as Vodacom, reveal compliance with national laws and adherence to contractual clauses in licensing agreements. Access Now's Telco Action Plan states that private sector actors must 'preemptively reject requests from governments and partners to restrict users' access, freedom of expression, or privacy' and must ensure that 'users' access to telecommunications networks is maintained at all times.'

A few examples of private sector compliance with shutdown requests in the region, is provided below.

DRC: During the 2015 internet shutdown, Vodacom maintained that telecom companies complied with a shutdown order which was 'issued in accordance with Article 46 of the Telecommunications Law of the DRC which gives the state the authority to prohibit the use of telecommunications installations.'

Egypt: During Egypt's 2011 internet shutdown, four ISPs (Telecom Egypt, Link Egypt, Vodafone/Raya, and Etisalat Misr) and three mobile phone companies (Vodafone Egypt, Mobinil, and Etisalat), complied with a shutdown order, which plunged the entire country into darkness.

Eswatini: During Eswatini's 2021 presidential elections, Eswatini MTN, Eswatini Post and Telecommunications, and Eswatini Mobile suspended access to social media and other online platforms, in response to a directive from the eSwatini Communications Commission.

Sudan: During Sudan's 2019 shutdown, Zain Sudan complied with a government directive to disrupt access. This was overturned by the court which issued an order to Zain Sudan to restore access to the Internet for Abdel-Adheem Hassan.

Uganda: During Uganda's 2021 elections, MTN Uganda disrupted access to their internet services, with reports that the telecom company would 'compensate Ugandans who were affected during the five-day internet shutdown in the country.' However, no official statement was released by MTN Uganda.

2.5 Illustrative Case Studies

Out of the ten African countries observed, all countries have disrupted access to the Internet, or internet-based communications services, including social media, as illustrated in Figure 2. Between 2016 - 2021, Ethiopia, Sudan, and Cameroon shutdown the Internet for a cumulative period of 677 days, with disruptions being ordered by the executive government, including state governments and ministries. Access Now observed that telecom regulators frequently refrain from issuing official statements or justifications about internet shutdowns, despite their mandate to regulate the communications sector.

Figure 2: Map showing Details of Internet Shutdowns in Select Countries in Africa

Across the ten countries, despite the steep economic cost of internet shutdowns, governments still resort to internet shutdowns in response to a variety of events, including elections and protests. For example, Zambia disrupted access to social media platforms, including WhatsApp, Twitter, Instagram, and Facebook, during the 2021 presidential elections. Eswatini disrupted internet connectivity in response to protests which started in May 2021.

3.0 Review of Recent Court Decisions

This section summarises the central arguments made by petitioners, responses by respondents and the judgments of select national and regional courts. It also reviews the emerging role of the courts in relation to internet shutdowns.

3.1 Overview of Litigation on Internet Shutdowns

Since 2011, the legality of internet disruptions continues to be contested before national and regional courts by different groups of petitioners. These include 'public spirited lawyers, human rights groups, media persons and law students', relying on the support of various coalitions and funding partners. For example, in 2021 in the countries under review, two ongoing cases contesting Internet disruptions in West and East Africa have been filed before the ECOWAS and the EACJ courts respectively. These include a petition filed by 5 CSOs and 4 individual petitioners challenging Nigeria's Twitter ban (ECOWAS), and a reference filed by one apex CSO body contesting Uganda's internet shutdown during the 2021 general election (EACJ).

Out of the 10 African nations reviewed in this report, Egypt's High Administrative Court was the first to deal with a judicial dispute in 2011. This case was filed by three telecommunications companies (i.e., Vodafone, Mobinil and Etisalat) and Egyptian officials (current and former) in 2011, who, ostensibly, contested the legality of the Internet and cell phone service disruptions. The court fined former regime leaders, including ousted President Mubarak, for this disruption. Further, the court ruling was a scathing indictment of the complicit actions of the 'ministries of interior, telecommunications and mass communications', and telecom companies

and Internet service providers operating in Egypt, including Vodafone. According to the judgment, these entities reportedly 'performed a series of experiments on how to sever connections as early as April 2008' and again in October 2010, three months before the Egyptian revolution.

> *Courts have the potential to initiate social change through decisions that reform legal rules, enforce existing laws and articulate public norms. Courts are popularly called "the last hope of the common man" and with good reason because where all else fails, the courts are where justice is sought, where human rights are upheld and existing laws are interpreted.*

3.2 Key Arguments Raised by Petitioners

Parties: A number of PIL cases have been filed against governments and private sector actors, typically Internet Service Providers (ISPs) and telecom operators. Strikingly, the EALS, in *East Africa Law Society vs The Attorney General of the Republic of Uganda & The Secretary General of the East African Community* (2021), enjoined the Secretary General of the East African Community as a respondent. Here, the EALS argued that the Secretary General, by failing to 'investigate the Ugandan Government's violations of the Treaty for the Establishment of the East African Community' prevented a 'possible referral of the matter to the Council of the East African Community and/or this Honourable Court for resolution.'

Infringement or Violation of Human Rights: Petitioners also stressed a violation of fundamental rights, including the rights to freedom of speech and expression, access to the Internet, access to information and to the press, and media freedom. In other cases, petitioners also argued an infringement of the right to freely participate in the affairs of government, freedom of association, freedom of assembly, the right to self-determination, and economic rights.

In the *East Africa Law Society vs The Attorney General of the Republic of Uganda & The Secretary General of the East African Community* (2021), the petitioners also relied on a denial of access to internet-based services such as payment systems, banking services, online markets, travel or transport services, and access to health services, which are necessary for everyday living and daily transactions.

In *Global Forum et al vs CAMTEL & 4 Others*, the petitioners argued that the internet shutdown in Cameroon infringed on the right against discrimination based on language. In *Unwanted Witness Ltd vs The Attorney General & 4 Others (2021),* the petitioners argued that the internet shutdown in Uganda violated the right to property, the right to education, and the right to fairness in administrative decisions hearings.

A variety of arguments were adduced by petitioners in the *Unwanted Witness, Media Rights Agenda, Amnesty International, East Africa Law Society*, *Global Forum,* and *Melusi Simelane v MTN Eswatini, Eswatini Mobile and others* cases to support the augment that internet shutdowns are an illegitimate and disproportionate restriction of fundamental rights. Generally, petitioners noted that internet shutdowns fail to meet the tests of necessity and proportionality under international law, serving as evidence of their unlawfulness. Further, petitioners noted that these limitations violated rights and freedoms protected under national constitutions, and regional and international frameworks, such as the ICCPR and the African Charter.

Rule of Law: Petitioners in a majority of cases argued that the state had breached its obligations to respect, promote and fulfil human rights under various treaty mechanisms. For example, in the *East Africa Law Society vs The Attorney General of the Republic of Uganda & The Secretary General of the East African Community* (2021), the petitioner emphasised that the internet shutdown in Uganda ran contrary to the Treaty for the Establishment of the East African Community. Specifically, the petitioner detailed a breach of various

principles, including good governance, democracy, the rule of law, public accountability and transparency, and social justice.

To support the arbitrariness of the ongoing Twitter suspension in Nigeria, petitioners in the *Media Rights Agenda et al vs The Federal Republic of Nigeria (2021)* argued that the justification for the suspension was not provided under law, failed to provide for the scope of the ban, consequently failing to guarantee access to the court, amongst other redress mechanisms. To support this argument, the petitioners further stressed that this lack of a strict legal framework permitted the government to exercise complete discretion while issuing the Twitter ban, without any public or judicial oversight, transparency or accountability.

Economic Impact: In the cases against the Nigerian and Ugandan governments, petitioners argued that the livelihoods and reputations of persons whose employment and businesses relied on the internet had been impacted, thereby causing extensive financial loss and hardships. Petitioners noted that this violated individuals' right to practice a profession.

To support this argument, petitioners demonstrated the negative impact on the economy generally, and on small and large businesses specifically. Petitioners have used a wide variety of tools to gather and present evidence supporting this argument, including adducing feedback from 23 people responding to an online poll and empirical evidence from the OHCHR.

3.3 Orders Sought in Cases

Primarily, petitioners have called on courts to issue a **declaration** that an internet shutdown, and any supporting directives from the government, violated the rights to freedom of expression and access to information, guided by international law. Further, they have called for a declaration that rights under a specific regional treaty have been violated. For example, in the *Media Rights Agenda* case, the petitioners called for a declaration that journalists' rights under the Revised ECOWAS Treaty had been violated. Similarly, the applicant in the *East Africa Law Society* case, urged the court to issue a declaration that the respondents had violated various provisions of the Treaty for the Establishment of the East African Community.

Petitioners have also called for both permanent and mandatory **injunctions**, guided by international law**.** These either require governments to immediately withdraw and lift restrictions on access to the Internet or bar the government from imposing Internet shutdowns in the future. In the *Media Rights Agenda et al vs The Federal Republic of Nigeria (2021),* the petitioners contested the government's threat to criminally prosecute a person found to be using Twitter and sought an order to restrain the imposition of such measures.

Additionally, the applicant in *East Africa Law Society vs The Attorney General of the Republic of Uganda & The Secretary General of the East African* called on the EACJ to order the Ugandan government to implement legal and administrative reforms to prevent the repetition of unlawful internet restrictions.

Additionally, petitioners in the *Media Rights Agenda* case have called on courts to issue **adequate reparation**, in the form of restitution, compensation and any other applicable measures, to persons adversely affected by the government sanctioned internet shutdown. Lastly, petitioners have called on the courts to exercise their discretion and issue **any other remedy/relief** deemed fit.

3.4 Responses by Governments

Lack of Locus Standi: The first defense adduced by governments in internet shutdown cases is the lack of *locus standi* (i.e. the right to bring an action in court). For example, in *Amnesty International Togo and et al vs the Republic of Togo*, the Togolese Republic argued that the 1st to 7th applicants, various CSOs established and

based in Togo, lacked *locus standi* on grounds that they were not natural persons or victims. On the other hand, the *locus standi* of the 8th applicant, a Togolese journalist working in the Togolese Republic, was challenged on the ground that she failed to declare the capacity in which she brought the action. The ECOWAS court held that all applicants had sufficient locus, given the direct impact of the internet shutdown on their operations (CSOs) and their right to freedom of expression (journalist).

Conversely, the Cameroon Constitutional Council struck out the petition filed by Global Concern Cameroon in July 2018. The Court argued that the petitioner lacked *locus* on grounds that Article 47 (2) of the Cameroon Constitution limited the right to approach the Constitutional Council to the "President of the Republic, the President of the National Assembly, the President of the Senate, one-third of the members of the National Assembly or one-third of the Senators, and Presidents of Regional Executives."

National Security/Public Order: The second defense presented by governments is the safeguarding of national security and the preservation of public order, on grounds that these are permissible limitations of derogable rights, such as the rights to freedom of expression, association, assembly, amongst others. This argument was presented by the Togolese Republic in *Amnesty International Togo and et al vs the Republic of Togo*, which also noted that 'some form of control of the internet' was necessary to curb hate speech and incitement and prevent a civil war.'

In *Media Rights Agenda et al vs The Federal Republic of Nigeria (2021)*, the applicants noted that the Nigeria government, in its public statements, justified the suspension of Twitter on grounds that the platform was being used for 'activities that are capable of undermining Nigeria's corporate presence.' The government further stated that the platform facilitated the spread of misinformation and false news, without accountability.

3.5 Responses by Private Sector

Adherence to Contractual Obligations: The primary defense raised by telecom operators and ISPs to justify compliance with shutdown orders is adherence to contractual obligations. In *Global Forum et al vs CAMTEL & 4 Others,* Viettel Cameruoun stated that their obligations under licensing and other contractual documents required adherence to instructions from the government related to the 'security of the state.'

3.6 Precedent Established by Courts

The Right to Access the Internet: Instrumentally, the ECOWAS Court and Cameroon's Constitutional Council have held that the right to access the Internet is a right within the context of the right to freedom of expression. In the *Amnesty International Togo and et al vs the Republic of Togo* decision, the ECOWAS Court found that access to the Internet is a derivative right and a component to the exercise and enjoyment of the right to freedom of expression, and thus requires the protection of the law. This statement is crucial, as it confirms that legal grounds must be adduced before any interference is imposed over individuals' access to the Internet.

Despite Cameroon Constitutional Council striking out the matter on grounds of admissibility, the Council also affirmed that the right to internet access 'forms part of the right to freedom of expression and access to information'. Here, the Court observed that the 'Internet is one of the principal means by which individuals exercise their rights to freedom of expression and access to information, providing as it does, essential tools for participation in activities and discussions concerning political issues and issues of general interest.'

Violation of International Law and Human Rights: The ECOWAS Court and Cameroon's Constitutional Council have both pronounced themselves on the permissibility of national security and public order arguments. The

courts relied on the legality principle under international human rights law to arrive at a finding that the right to freedom of expression had been violated.

In the *Amnesty International Togo and et al vs the Republic of Togo* decision, the ECOWAS court held that the derogation of the right to freedom of expression relying on the national security justification may have had merit as a valid defense, if this had been done in accordance with the law, including providing the conditions for derogation. Here, the Court noted that in the absence of this law, preventing internet access amounted to a violation of the right to freedom of expression by the Togolese Republic.

Similarly, the Cameroon Constitutional Council held that the laws on the maintenance of law and order, amongst other laws, did not 'permit the complete shutdown of the Internet as a measure to restore [law] and order,' did not sanction the disruption, interference or complete shutdown of the Internet, and was 'arbitrary and unjustified by law. The Council arrived at the decision that the partial and complete shutdowns of the Internet was an illegitimate measure which violated the right of freedom of expression of the petitioners, and Cameroon users generally.

Conversely, the Ugandan Constitutional Court dismissed the Unwanted Witness petition, contesting the 2016 internet shutdown, on grounds that this was justifiable under national law, for the purpose of national security.

Directions: The ECOWAS Court provides the most illustrative examples of the types of punitive measures which can be imposed on governments to prevent internet shutdowns from taking place in the future, and to provide redress to impacted petitioners. In this matter, the Court issued an order of violation of the right to freedom of expression by the Togolese Republic, which gave rise to a compensation award of CFA 2 million (US$ 3,555) to each applicant.

Further, the Court also issued directions to the government to 'take all necessary measures to guarantee non-occurrence of this situation in the future' and to 'enact and implement laws, regulations and safeguards in order to meet its obligations with respect to the right of freedom of expression in accordance with international human rights instruments.'

3.7 Critical Challenges

Generally, interviewee's noted that funding constraints impacted their ability to pursue long-term strategic PIL, offset legal fees, gather evidence, and support their arguments with support from technical experts. Many of the CSOs interviewed observed that they lacked know-how about legal processes, and did not have access to resources, including repositories with submissions and judgments for past and ongoing PIL cases. On the other hand, interviewees detailed glaring digital rights knowledge, skills and competency gaps among presiding lawyers and judges. Further, CSOs noted that the lack of laws which expressly declare that 'shutdowns are illegal created room for subjective interpretation, which makes the outcome of litigation less predictable.' Lastly, CSOs noted the lack of collaboration by actors in the space resulted in disjointed advocacy efforts by activists, CSOs, lawyers, and concerned citizens.

3.8 Role of the Courts

National and regional courts provide channels of redress for individuals, communities and their representatives, before, during and after the disruption of access to the Internet and Internet-based communications. Additionally, judicial pronouncements by national and regional courts on Internet shutdowns in Africa provide persuasive precedent on States' compliance with international, regional and national laws on human rights online, private sector obligations to respect human rights and promote consumer protections, and the general protection of human rights online.

Crucially, positive judicial decisions condemning Internet disruptions reinforce the narrative that access to the Internet is a human right, whilst negating the legality of broad justifications provided by States, such as national security and public order. However, negative decisions fuel the perception that the intentional disruption of the Internet and Internet-based communications is permissible under the law.

Notably, national and regional mechanisms tasked with interpreting the law and ensuring government accountability and transparency, operate within specific judicial and political environments, with an impact on the effectiveness of strategic PIL. At the national level, weakened legislative and judicial institutions are unable to properly deter and contest executive impunity and supremacy.

Additional factors which need to be taken into consideration before PIL is filed include the independence of national and regional courts; the effectiveness of national, regional and international human rights frameworks; opportunities for engagement due to *locus standi* and the exhaustion of local remedy requirements (before regional courts/mechanisms); the capacity of judicial officers; the enforceability of judicial pronouncements; the time taken to determine Internet disruption cases, amongst others.

Crucially, one interviewee noted that delays to resolve petitions, such as the three-year delay in the Unwanted Witness petition (2016), created an impression that 'national courts don't do anything...and can't deliver much in terms of enforcement.' However, other interviewees noted that the courts in the region are ready to hear and determine internet shutdown cases, providing the ECOWAS preliminary ruling on Nigeria's Twitter ban and the 2020 ruling on Togo's Internet shutdown as examples.

In conclusion, courts generally provide a useful platform for stakeholders to contest the legality, proportionality and necessity of internet shutdowns, at the national, regional and international levels. Stakeholders, such as the AIRA, should proactively continue filing strategic PIL to, as a first point of call, ensure that any legal or regulatory provisions justifying shutdowns are declared illegal.

4.0 Key Emerging Impacts

This section reviews the emerging issues and implications of internet shutdowns, with a focus on the impact on civil and political rights, access to the Internet, socio-economic development and State responsibilities to respect, promote and fulfil human rights.

4.1 Impact on Civil and Political Rights

Internet shutdowns and disruptions interfere with the exercise and enjoyment of civil and political rights including: freedom of expression, access to information, freedom of the media, freedom of assembly and association, the right to protest and to political participation. These rights are guaranteed in national constitutions, regional instruments such as the African Charter on Human and Peoples' Rights (African Charter/Banjul Charter), and International Instruments such as the Universal Declaration on Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR).

As outlined above, shutdowns are often implemented during election periods, protests, and to control public discourse by stifling dissent and enforcing censorship of those calling out the ruling elite on human rights violations, corruption, impunity, lack of transparency and accountability in governance, among others. It also affects the work of key groups such as bloggers, civil society, human rights defenders, journalists, media, online

activists, opposition leaders, and the general public, given its restrictions on communication and the free flow of information.

Most of the time, the laws, methods, justifications and institutions through which they are ordered and enforced are not always clear, or compliant with the rule of law. As a result, internet shutdowns continue to undermine democracy and electoral processes; nurture and perpetuate impunity; cover up for human rights violations; and deny people the opportunities and platforms to exercise their democratic rights and participate in governance.

National constitutions, regional and international instruments require states to take positive steps to ensure the realisation and enjoyment of rights of their citizens. The calls for respect for internet freedoms and the steps that need to be taken have also been articulated in resolutions, standards and reports of various UN bodies, regional and international treaty monitoring bodies and special mechanisms, as highlighted in the appendices below. However, the reality is that these are barely complied with as digital authoritarianism in the continent continues to claw back on the rights of citizens.

Ultimately, the internet and digital technologies remain critical avenues for promoting human rights and for citizen participation in governance and democratic processes. Shutting down the Internet violates human rights protections as guaranteed in national constitutions and regional and international instruments. It also undermines the quality of democratic participation and subverts constitutionalism on the continent.

4.2 Impact on Access to the Internet

According to the GSMA, mobile networks are integral to how people live and how businesses live. During the COVID-19 pandemic, increases in the adoption and use of mobile services such as mobile data, and money transfer services were recorded. The available statistics indicate that these services have indeed become a lifeline for society and have kept people and businesses connected, enabled work, learning and other daily activities.

The GSMA report indicated that SSA had 495 million mobile subscribers in 2020, which is expected to grow to 615 million in 2025. Mobile internet users stood at 303 million in 2020, and are expected to grow to 474 million by 2025. The total SIM connections stood at 930 million in 2020, and is expected to grow to 1.12 billion by 2025, indicating a penetration rate of 90%, up from 77% in 2020. Further, smartphone adoption continues to grow from the 48% recorded in 2020 to 64% expected in 2025.

According to the International Telecommunications Union (ITU) broadband coverage in Africa with 4G coverage stood at 44.3% in 2020, while 3G and 2G stood at 33.1% and 11% respectively. However, 4G coverage in the continent remains higher in urban areas (77%) while rural areas stood at 22%. The coverage in Africa is still way lower than the global average, which stands at 84.7% for 4G and 8.5% for 3G. The ITU data also reveal that at the end of 2019, more than half of the world's population was using the internet.

Crucially, almost 70% of the world's youth are using the internet. Moreover, internet users in all African countries as at December 2020 stood at 590 million, indicating a penetration rate of 43%, compared to a global average of 64.2%. Further, 255 million of these users are on Facebook. With respect to costs, the Alliance for Affordable Internet (A4AI) noted that only of the 45 African countries (North African and Sub-Saharan) it tracked, only 10 met its standard for 'affordable Internet'. According to the 2020 report, Africa recorded the lowest average Affordability Drivers Index (ADI) score, despite a 6.7% increase from 2019.

The importance of ICTs in the continent has been recognised at the regional level. The African Union (AU) for example, in its continental development strategy, Agenda 2063 recognises the importance of ICTs and envisages a highly connected Africa with ICTs being tools for business, social interaction and governance. The

implementation of the Agenda is also linked to the achievement of the Sustainable Development Goals, including SDG 2 (zero hunger), SDG 3 (good health and wellbeing), SDG 7 (affordable and clean energy), SDG 9 (industry, innovation and infrastructure), SDG 11 (sustainable cities and communities), SDG 12 (responsible consumption and production), and SDG 17 (partnerships for the goals).

Further, the AU in its *Digital Transformation Strategy for Africa* seeks to harness digital technologies and innovation to transform African societies and economies to promote Africa's integration." By 2030, the Strategy aims to have a digitally empowered citizenry, able to access the internet safely and securely at a minimum speed of 6 mb/s all the time wherever they live in the continent, at an affordable price of no more than USD 1cts per mb. The AU wants to achieve this through a smart device manufactured in the continent at the price of no more than USD 100, and to benefit from all basic e-services and content of which at least 30% is developed and hosted in Africa.

The African Economic Outlook report for 2018 presents a comprehensive estimate for Africa's infrastructure needs based on the cost of achieving specific service level targets for each sector by 2025. For the ICT sector, the targets are universal mobile coverage, 50% of population within 25 km of a fiber backbone, and a fiber to home or premises internet penetration rate of 10%. These raise an annual financing need of between US$ 4 - 7 billion. While the African continent has witnessed significant growth in ICTs, the continent still lags in connectivity. Currently, 75% of the population are still offline, with only 15% of the households in Africa with a home internet connection as of 2020.

Despite low levels of internet penetration in the continent, African states have adopted several measures and programmes to promote access to the internet and mobile telephony. Therefore, disrupting connectivity goes against the vision and targets set not only by individual states, but also commitments taken by States at the regional level.

4.3 Impact on Socio-Economic Development

The ICT sector contributes significantly to the gross domestic product (GDP) of a country. Therefore, when the Internet is shut down, it significantly affects the digital economy of a country. It is worth noting that a digital economy provides several benefits including: improving the efficiency and transparency of government and generating impressive savings; helping low-income countries improve the environment for small and medium enterprises, including through better access to financing; and opening up the service sector, a growing share of the economy of many low-income countries.

In 2020, the mobile industry in Sub-Saharan countries contributed US$132 billion to GDP, and it is expected to grow to US$155 billion by 2025. According to McKinsey, the Internet's contribution of GDP in Africa will average 5%-6% in Africa representing US$300 billion. According to the World Bank, 200 million users made 27.55 billion mobile money transactions in SSA and the Middle East and Northern Africa during 2020, making up 66.5 percent of all transactions made worldwide. Of the US$797 billion transacted through mobile money in 2020, US$490 billion was exchanged in SSA.

A recent study revealed that commitments to ICT infrastructure in Africa has been on the rise, and increased by 37% from US$1.7 billion in 2016 to US$2.3 billion in 2017. In 2018, a record commitment of US$7.1 was recorded. However, the Infrastructure Consortium for Africa noted that the 'funding gap' is an estimated US$3 billion a year, with an overall continental infrastructure need of between US$52 - 92 billion.

The economic cost of internet disruptions is not precisely known. However, a study by CIPESA developed a framework to estimate the impact of disruptions in SSA, and applied it to select countries in Africa that had experienced shutdowns between 2015 and 2017. Table 3 below shows the estimated economic impact of a

total internet blackout and app disruption per day in US$ across selected countries in SSA as established in the study.

Table 3: Estimated economic impact of a total internet blackout and app disruption per day in US$

Country	Net direct economic effect per day (a)	Net indirect economic effect per day (b+c)	Total economic cost of internet disruption per day	Total cost due to app disruption per day
Burundi	82,384	84,032	166,416	41,604
Cameroon	994,703	676,398	1,671,102	417,775
DR Congo	958,867	978,044	1,936,911	484,228
Ethiopia	1,982,856	1,516,885	3,499,741	874,935
Gabon	584,119	297,901	882,019	220,505
Gambia	26,427	26,956	53,383	13,346
Niger	205,726	209,840	415,566	103,891
Republic of Congo	214,617	218,909	433,526	108,381
Togo	120,548	122,959	243,507	60,877
Uganda	1,049,092	713,383	1,762,475	440,619
Kenya	4,125,464	2,191,230	6,316,695	1,895,008

Based on the foregoing, the highest daily cost was estimated to be in Kenya, at US$6.3 million, followed by Ethiopia at US$3.5 million, and DR Congo at US$1.9 million. The highest estimated daily total cost due to app disruptions was in Ethiopia at US$874,935, followed by DR Congo at US$484,228 and Kenya at US$440,619. According to the report, Internet shutdowns in SSA have cost the region up to US$237 million between 2015 and 2017.

In March 2018, African countries recently adopted the Agreement establishing the African Continental Free Trade Area (AfCFTA), which entered into force in May 2019. The AU Digital Transformation Strategy for Africa aims to build a secured Digital Single Market in Africa by 2030 where free movement of persons, services and capital is ensured and individuals and businesses can seamlessly access and engage in online activities in line with Africa's Continental Free Trade Area (AfCFTA). This cements the position that ICTs can be leveraged as part of the implementation of AfCFTA to bolster cross-border commerce, attract investments, automate processes, simplify trade logistics and reduce costs of doing business within the continuent. Harnessing these benefits will be possible only if internet disruptions are avoided.

From the foregoing, it is clear that ICTs make significant contributions to the digital economy in Africa. As the uptake of ICTs increases, the contributions of ICTs to GDPs are set to increase significantly over the next five years. These increases present additional opportunities to spur trade, such as through the AfCFTA, which will lead to greater reliance on the internet and digital technologies.

4.4 Impact on State Responsibilities

Under international and regional law, states have an obligation to respect, promote and fulfil human rights, both online and offline. As illustrated in Table 4 below, it is generally acknowledged that mass communications disruptions do not comply with international law, with internet shutdowns amounting to a violation of states' obligations to protect and promote human rights. According to the 2019 report by the Special Rapporteur on the rights to freedom of peaceful assembly and of association, the 'general norm should be to permit the open and free use of the Internet and other digital tools.'

International and regional mechanisms and rights experts maintain that access to the internet is integral to the facilitation of the rights to freedom of expression and access to information. Consequently, any restrictions on the Internet must satisfy the three-part test permitting the limitation of the right to freedom of expression under international law. Further, mechanism holders insist that any laws which are enacted to restrict the right to freedom of expression, must be accompanied by remedies and safeguards against abuse.

Regional and international human rights mechanisms play a crucial role in ensuring that governments do not interfere with the 'right of individuals to seek, receive and impart information through any means of communication and digital technologies' through measures such as the disruption of access to the internet and other digital technologies. Crucially, to hold African Union States Parties to account, the ACHPR's Special Rapporteur on Freedom of Expression and Access to Information has issued numerous statements and reports in response to internet shutdown allegations, through letters of appeal addressed to Heads of States, press releases and resolutions.

Notably, one interviewee observed that the ACHPR's 2019 Activity Report, which flagged out the 'continuing trend of Internet and social media shutdowns in Africa, including in Chad, Sudan, the Democratic Republic of Congo, Gabon and Zimbabwe', was instrumental. Notably, this report helped to hold the 5 governments to account and 'elicited formal responses from States Parties to allegations on violations of freedom of expression and access to information, including internet shutdowns.'

Table 4: Summary of International and Regional Law and Standards

Instrument	**Relevant Provisions**
Binding Instruments	
Universal Declaration of Human Rights (UDHR)	Rights and freedoms set forth in the declaration without distinction (article 2); equality before the law and to equal protection of the law (article 7); an effective remedy by the competent national tribunals (article 8); privacy (article 12); freedom of thought, conscience and religion (article 18); freedom of opinion and expression (article 19); freedom of peaceful assembly and association (article 20); take part in the government of his country, directly or through freely chosen representatives (Article 21(1)); equal access to public service in his country (article 21(2); work (article 23); education (article 26); and, to freely participate in cultural life (article 27).

International Covenant on Civil and Political Rights (ICCPR)	Equality before the courts and tribunals (article 14); privacy and its protection by the law (article 17); freedom of thought, conscience and religion (article 18); right to freedom of opinion and expression (article 19); peaceful assembly (article 21); freedom of association (article 22); political participation (article 25); equality before the law and equal protection (article 26).
The International Covenant on Economic, Social and Cultural Rights (ICESCR)	rights to: work (article 6); form and join trade union, and to strike (article 8); physical and mental health (article 12); education (article 13); take part in cultural life and enjoy the benefits of scientific progress and its applications (article 15).
The African Charter on Human and Peoples' Rights (Banjul Charter):	rights to: equality before the law, and equal protection of the law (article 3); dignity (article 5); conscience (article 8); receive information and to expression and opinion (article 9); association (article 10); assembly (article 11); participation in governance (article 13); property (article 14); work (article 14); health (article 16); education (article 17); equality (article 19); self-determination (article 20); development (article 22); and to a general satisfactory environment favorable to their development (article 24).
Persuasive Instruments	
Declaration of Principles on Freedom of Expression in Africa 2019	Principle 17 (regulatory bodies for broadcast,telecommunications and the internet); principle 37 (access to the internet); principle 38 (non-interference); principle 39 (Internet intermediaries).
Statements	**Relevant Statement(s)**
The Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/HRC/17/27), 16 May 2011.	Para 67: 'Unlike any other medium, the Internet enables individuals to seek, receive and impart information and ideas of all kinds instantaneously and inexpensively across national borders. By vastly expanding the capacity of individuals to enjoy their right to freedom of opinion and expression, which is an "enabler" of other human rights, the Internet boosts economic, social and political development, and contributes to the progress of humankind as a whole.' Para 68: "the full guarantee of the right to freedom of expression must be the norm, and any limitation considered as an exception, and that this principle should never be reversed". Para 69: Any restrictions on the Internet must pass a three-part, cumulative test: (1) it must be provided by law, which is clear and accessible to everyone (principles of predictability and transparency); (2) it must pursue one of the purposes set out in article 19, paragraph 3, of the International Covenant on Civil and Political Rights...; and (3) it must be proven as necessary and the least restrictive means required to achieve the purported aim (principles of necessity and proportionality). In addition, any legislation restricting the right to freedom of expression must be applied by a body which is independent of any political, commercial, or other unwarranted influences in a manner that is neither arbitrary nor discriminatory. There should also be

	adequate safeguards against abuse, including the possibility of challenge and remedy against its abusive application. Para 70: the lack of transparency surrounding the measures made it difficult to "ascertain whether blocking or filtering is really necessary for the purported aims put forward by States". The Special Rapporteur thus called upon States that currently block websites to, among others, "provide lists of blocked websites and full details regarding the necessity and justification for blocking each individual website", and an explanation "on the affected websites as to why they have been blocked". Also, that "any determination on what content should be blocked must be undertaken by a competent judicial authority or a body which is independent of any political, commercial, or other unwarranted influences". Para 78: While blocking and filtering measures deny users access to specific content on the Internet, States have also taken measures to cut off access to the Internet entirely. The Special Rapporteur considers cutting off users from Internet access, regardless of the justification provided, including on the grounds of violating intellectual property rights law, to be disproportionate and thus a violation of article 19, paragraph 3, of the International Covenant on Civil and Political Rights. Para 79: the Special Rapporteur called upon all States to "ensure that Internet access is maintained at all times, including during times of political unrest". Further, States were urged to "to repeal or amend existing intellectual copyright laws which permit users to be disconnected from Internet access, and to refrain from adopting such laws". Para 85: Given that the Internet has become an indispensable tool for realizing a range of human rights, combating inequality, and accelerating development and human progress, ensuring universal access to the Internet should be a priority for all States. Each State should thus develop a concrete and effective policy, in consultation with individuals from all sections of society, including the private sector and relevant Government ministries, to make the Internet widely available, accessible and affordable to all segments of population.
Joint Declaration on Freedom of Expression and the Internet, June 2011	Principle 1: Freedom of expression applies to the Internet, as it does to all means of communication. Restrictions on freedom of expression on the Internet are only acceptable if they comply with established international standards, including that they are provided for by law, and that they are necessary to protect an interest which is recognised under international law (the 'three-part' test). Principle 6: Access to the Internet a. Giving effect to the right to freedom of expression imposes an obligation on States to promote universal access to the Internet. Access to the Internet is also necessary to promote respect for other rights, such as the rights to education, health care and work, the right to assembly and association, and the right to free elections. b. Cutting off access to the Internet, or parts of the Internet, for whole populations or segments of the public (shutting down the

	Internet) can never be justified, including on public order or national security grounds. The same applies to slow-downs imposed on the Internet or parts of the Internet. c. Denying individuals the right to access the Internet as a punishment is an extreme measure, which could be justified only where less restrictive measures are not available and where ordered by a court, taking into account the impact of this measure on the enjoyment of human rights. d. Other measures which limit access to the Internet, such as imposing registration or other requirements on service providers, are not legitimate unless they conform to the test for restrictions on freedom of expression under international law.
The Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue - Sixty-sixth session of the UN General Assembly, (A/66/290), 10 August 2011	Para 61: Although access to the Internet is not yet a human right as such, the Special Rapporteur would like to reiterate that States have a positive obligation to promote or to facilitate the enjoyment of the right to freedom of expression and the means necessary to exercise this right, which includes the Internet. Moreover, access to the Internet is not only essential to enjoy the right to freedom of expression, but also other rights, such as the right to education, the right to freedom of association and assembly, the right to full participation in social, cultural and political life and the right to social and economic development. Para 63: Indeed, given that the Internet has become an indispensable tool for full participation in political, cultural, social and economic life, States should adopt effective and concrete policies and strategies, developed in consultation with individuals from all segments of society, including the private sector as well as relevant Government ministries, to make the Internet widely available, accessible and affordable to all. Para 88: It is not only important but imperative that States adopt effective and concrete policies and strategies, developed in consultation with individuals from all segments of society, including the private sector and relevant Government ministries, in order to make the Internet widely available, accessible and affordable to all, based on the principles of non-discrimination of any kind, including on the grounds of race, colour, sex, language, disability, economic origin or any other status. Paras 82 - 92: • Take proactive measures to ensure that Internet connectivity is available on an individual or communal level in all inhabited localities of the State, by working on initiatives with the private sector, including in remote or rural areas. Such measures involve the adoption and implementation of policies that facilitate access to Internet connection and to low-cost hardware, including in remote and rural areas, including the subsidization of service, if necessary. • Actively promote broadband access given the increasing amount of multimedia content online. • Support policies and programmes to facilitate connection to the Internet through the use of mobile phones given that mobile

	technology is increasingly being used, and is more accessible in developing States. • In particular developed States, to honour their commitment, expressed, inter alia, in the Millennium Development Goals, to facilitate technology transfer to developing States and to integrate effective programmes to facilitate universal Internet access in their development and assistance policies.
General Comment No. 34, Article 19: Freedoms of Opinion and expression, 102nd Session of the Human Rights Committee (CCPR/C/GC/34), September 2011	Para 11: the guarantee to freedom of expression "includes the expression and receipt of communications of every form of idea and opinion capable of transmission to others, subject to the provisions in article 19, paragraph 3, and article 20." Para 12: provides that Article 19(2) protects all forms of expression (including spoken, written and sign language and such non-verbal expression as images and objects of art) and the means of their dissemination (including books, newspapers, pamphlets, posters, banners, dress and legal submissions). These include "all forms of audio-visual as well as electronic and internet-based modes of expression". Para 15: States parties should take account of the extent to which developments in information and communication technologies, such as internet and mobile based electronic information dissemination systems, have substantially changed communication practices around the world... States parties should take all necessary steps to foster the independence of these new media and to ensure access of individuals thereto. Para 43: Any restrictions on the operation of websites, blogs or any other internet-based, electronic or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines, are only permissible to the extent that they are compatible with paragraph 3. Permissible restrictions generally should be content-specific; generic bans on the operation of certain sites and systems are not compatible with paragraph 3. It is also inconsistent with paragraph 3 to prohibit a site or an information dissemination system from publishing material solely on the basis that it may be critical of the government or the political social system espoused by the government.
Resolution 66/184 on Information and communications technologies for Development - Sixty-sixth session of the UN General Assembly (A/RES/66/184) 22 December 2011	This Resolution acknowledged the "positive trends in global connectivity and affordability in the field of information and communications technologies, in particular the steady increase in Internet access to one third of the world's population, the rapid diffusion of mobile telephony, the increased availability of multilingual content and Internet addresses and the advent of new services and applications, including m-health, mobile transactions, e-government, e-education, e-business and developmental services, which offer great potential for the development of the information society."
United Nations Human Rights Council Resolution HRC/RES/20/8 of 16 July 2012	This Resolution recognised that "the global and open nature of the Internet as a driving force in accelerating progress towards development in its various forms." Further, it affirmed that "the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice." It also calls upon all States "to promote and facilitate access to the

	Internet and international cooperation aimed at the development of media and information and communications facilities in all countries."
United Nations Human Rights Council Resolution A/HRC/32/L.20 of 27 June 2016	The Resolution expressed the deep concern of the Council of the "human rights violations and abuses committed against persons for exercising their human rights and fundamental freedoms on the Internet, and by the impunity for these violations and abuses," and "by measures aiming to or that intentionally prevent or disrupt access to or dissemination of information online, in violation of international human rights law." The Resolution further stressed the "importance of applying a human rights-based approach when providing and expanding access to the Internet and for the Internet to be open, accessible and nurtured by multi-stakeholder participation". The Resolution called upon States to among others: address security concerns on the Internet in accordance with their international human rights obligations to ensure protection of freedom of expression, freedom of association, privacy and other human rights online, including through national democratic, transparent institutions, based on the rule of law, in a way that ensures freedom and security on the Internet so that it can continue to be a vibrant force that generates economic, social and cultural development; and consider formulating, through transparent and inclusive processes with all stakeholders, and adopting national Internet-related public policies that have the objective of universal access and enjoyment of human rights at their core.
Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association (May 2019) A/HRC/41/41	Summary: International law protects the rights to freedom of peaceful assembly and of association, whether exercised in person, through technologies of today, or through technologies that will be invented in the future. Existing international human rights norms and principles should not only dictate State conduct, but also be the framework that guides digital technology companies' design, control and governance of digital technologies. International law protects the rights of freedom of peaceful assembly and of association, whether exercised in person, or through the technologies of today, or through technologies that will be invented in the future. Para 11: Technology serves both as a means to facilitate the exercise of the rights of assembly and association offline, and as virtual spaces where the rights themselves can be actively exercised. Indeed, such technologies are important tools for organizers who seek to mobilize a large group of people in a prompt and effective manner, and at little cost, and also serve as online spaces for groups of people that are marginalized by society and are confronted with restrictions when operating in physical spaces. Para 63: The Special Rapporteur calls on digital technology companies to meet their responsibilities to respect internationally accepted human rights standards, including the rights to freedom of peaceful assembly and of association. To that end, the effective implementation of the Guiding Principles on Business and Human Rights should be a priority for these companies. Models that include an independent impact assessment

	oversight, such as the ones promoted by the Global Network Initiative, should be scaled up.
Resolution **ACHPR/Res.362 (LIX) 2016 on the Right to Freedom of Information and Expression on the Internet in Africa, adopted during the 59th Ordinary Session, held from 21 October to 04 November 2016**	The African Commission expressed its concern over the "emerging practice of State Parties of interrupting or limiting access to telecommunication services such as the Internet, social media and messaging services, increasingly during elections." The Commission called on States Parties to "respect and take legislative and other measures to guarantee, respect and protect citizen's right to freedom of information and expression through access to Internet services."
Press Release by the Special Rapporteur on Freedom of Expression and Access to Information in Africa on the Continuing Trend of Internet and Social Media Shutdowns in Africa **- January 2019**	The Special Rapporteur, through this release noted that "internet and social media shutdowns violate the right to freedom of expression and access to information contrary to Article 9 of the African Charter on Human and Peoples' Rights." The Rapporteur also stated that the internet and social media had "given voice to the people of Africa who may now discourse on social, economic and political issues far more than ever before, and states should not take away that voice." The Rapporteur noted what happened in countries such as the DRC, Sudan and Zimbabwe, and stated that citizens should not be "penalised through shutdowns when they demonstrate calling for economic or political reforms or indeed during contested electoral campaigns or polling" The Rapporteur also reiterated the Joint Declaration of Expression and Internet adopted in 2011 and stressed that States had "an obligation to promote universal access to the internet as it facilitates the fulfilment of other rights." Further, the Rapporteur called on African states to "take all measures to guarantee, respect and protect the right to freedom of expression and access to information through ensuring access to internet and social media services."

5.0 Recommendations

This section considers the necessary actions that the AIRA could take to avert internet shutdowns on the continent. It also recommends action which the AIRA can take, as a Coalition and in collaboration with other key stakeholders i.e. funders, civil society, media, regional and international mechanisms, private sector, governments, national, and regional courts.

5.1 AIRA Coalition Recommendations

- Build the capacity and technical expertise of members to be able to track and monitor Internet shutdowns, given the evolution of internet censorship tactics. This study developed an initial framework that can be scaled and adopted by AIRA to support the continued compilation and

aggregation of information on internet shutdowns in Africa. AIRA can expand this framework through regular monitoring of African countries within AIRA Members' geographical scope.

- Leverage on, and utilise members' existing relationships and contacts with relevant stakeholders, to advance national and regional multi-stakeholder advocacy efforts, relationship-building, skills development, amongst others. AIRA should consider promoting inter-stakeholder collaboration to effectively combat internet shutdowns.
- Conduct stakeholder mapping to identify key stakeholders that AIRA can leverage for advocacy at the regional and international levels.
- Develop a regional litigation strategy to inform advocacy before national and regional courts.
- Develop and articulate consistent, comprehensive, and collective messaging, and a uniform position on internet shutdowns. This messaging should also include AIRA's call to action to all relevant stakeholders that should be disseminated widely by AIRA and AIRA members.

5.2 Stakeholder Recommendations

- Funders:
    - Seek general and long-term funding support for the coalition's work, including the recruitment of technology experts e.g. on policy experts, web activists, researchers, developers, scientists, educators, data scientists, engineers, amongst others.
    - Leverage on the monetary and social capital of funders, based on their priorities.
    - Have more collaborative discussions, dialogues and actions between partners and donors to leverage on collective action (e.g., collective agreement on priority areas for intervention around shutdowns).

- Civil Society:
    - Adopt a multi-pronged approach to Internet shutdowns, including through grassroots advocacy, technical support, civil society mobilization, grant-making, legal interventions, direct policy-maker engagements and convenings. The following convenings are critical: FIFAfrica, Digital Rights and Inclusion Forum (DRIF), RightsCon, national, regional and global Internet Governance Forums (IGFs).
    - Continue monitoring, tracking, and reporting on internet shutdowns in collaboration with the technical community, to generate up-to-date evidence across more African countries. AIRA could contribute data to the #KeepItOn coalition and the OONI open data resource on internet censorship.
    - Leverage on members' network to encourage more CSOs in Africa to join and actively participate in existing campaigns and coalitions contesting internet shutdowns (e.g., the AIRA, the African Declaration on Internet Rights and Freedoms Coalition, the #KeepItOn Coalition).
    - Develop joint communication strategies to ramp up online and offline advocacy against internet shutdowns. This includes relying on open letters, articles, blogs, reports and submissions to raise awareness about the trends and developments and urge state and non-state actors to adopt the relevant measures and policies to prevent disruption.
    - Request policy makers to conduct and publish cost-benefit risk analyses and human rights impact assessments weighing national security considerations alongside the real impact of shutdowns (e.g., technical impact, economic, human rights).
    - Monitor the legislative process, including any laws which could impact the realisation of digital rights, and push back against these before enactment.
    - Take preemptive action in courts where the likelihood of shutdowns is likely to take place and reactive action to contest provisions justifying Internet shutdowns.

- Build a database of existing PIL lawyers on the Continent, relying on the support of bench and bar associations, and other CSOs. AIRA could collaborate with regional and national bar associations, such as the PALU, EALS, ICJ, to conduct regional training for lawyers on digital rights litigation. AIRA can also consider leveraging on their annual conferences to build the capacity of litigators.
- File or support strategic Public Interest Litigation with wide continental impact as an advocacy strategy to challenge and change laws, policies and practices that perpetuate internet disruptions.
- Provide sustained support (e.g., resources, expertise, protection) to petitioners and petitioner groups filing strategic Public Interest Litigation.
- Equip users at risk and those impacted by shutdowns with relevant circumvention tools and resources to get back online.

- Media
  - Leverage relationships with regional and international media in broadcasting, print and digital media. AIRA should prioritise the enhancement of reporting on shutdowns and the public's general understanding of digital rights, including highlighting the resumption of service in Africa.
  - Work with content producers to capture, simplify and translate the meaning of Internet shutdowns, effects and impact of shutdowns, measures to bypass Internet shutdowns, tools to report Internet shutdowns in real-time, amongst others, to local populations. AIRA should consider using opinion pieces, adverts and programmes on radio and TV stations, infographics, cartoons, short clips, amongst others, to disseminate this messaging both online and offline.

- Regional and International Mechanisms
  - Identify strategic and joint advocacy opportunities at the regional and global levels that AIRA members cannot individually tackle by themselves. AIRA should consider engaging and partnering with RECs, the EACO and the African Telecommunications Union to commemorate key dates whilst simultaneously advocating for positions on Internet shutdowns. Critical dates include: the African Telecommunications and ICT Day, International Day for Universal Access to Information, World Press Freedom Day, African Human Rights Day, International Day of Democracy.
  - Support AIRA Members to develop shadow and alternative reports with relevant information on internet freedom violations to regional and international treaty-body monitoring mechanisms (e.g., by convening a collective meeting to discuss continental trends and findings).
  - Promote and elaborate Part IV of the Declaration of Principles on Freedom of Expression and Access to Information in Africa on Freedom of Expression and Access to Informa-tion on the Internet.
  - Leverage on the ACHPR's Ordinary Sessions and NGO Forums for collective advocacy by AIRA Coalition Members, including relying on Members' Observer Status to articulate a joint position on shutdowns.
  - Follow up on the responses to allegations on violations of digital rights made by States (e.g., formal responses issued by States Parties responding to the ACHPR's Activity Report submitted to the AU Policy Organs).
  - Follow up on the implementation of recommendations made by regional and international bodies to States on internet disruptions.

- Private Sector
    - Work with organisations that have direct engagements with social media platforms, telcos and ISPs, and associations (e.g., GSMA, GNI and FOC) to advocate against internet disruptions. AIRA should consider supporting Access Now's campaign to negotiate and publish crisis protocols with governments, alternative communications channels and workarounds to mitigate the impact of Internet disruptions.
    - Engage high-level officials and representatives of telcos and ISPs with regional reach (e.g. Orange, Vodafone, MTN, Airtel etc.) and social media platforms (e.g. Facebook, Twitter, TikTok) at the regional level. AIRA could form partnerships to advance positions on key digital rights issues.

- Government
    - Proactively engage and build allies at the government level, especially within high-risk governments, who can advocate against Internet shutdowns.
    - Petition national governments and REC's to abolish laws that permit internet disruptions, and enact laws that guarantee digital rights and promote access to the Internet.
    - Engage and work with relevant departments, ministries and agencies within national governments and REC's and sensitise them on the impact and effect of Internet disruptions.

- National and Regional courts
    - Partner with national and regional judicial training institutions to review the judicial education curriculum and incorporate emerging and technical digital rights and technology issues.
    - Collaborate with key stakeholders, such as UNESCO and continental lawyers working to strengthen the capacity of judiciaries in the region. AIRA should collaboratively develop education material for judicial officers, including compilations of relevant human rights instruments, case digests, judicial bench books, and training manuals and disseminate the same to the training institutions, judicial associations and bar associations.
    - Collaborate with national and regional judicial training institutions to build the capacities of judicial officers. AIRA could organise regional Trainer of Trainers training in collaboration with key partners and stakeholders to empower judicial officers with knowledge on digital rights and emerging threats, such as internet shutdowns.

Appendix 1: Resources

1. The Economy and the Internet: What Lies Ahead?
2. Who Controls the Internet?: Illusions of a Borderless World-Jack Goldsmith, Tim Wu, OUP
3. In the Service of Power: Media Capture and the Threat to Democracy-Anya Schiffrin-Center for International Media Assistance, 2017
4. Mapping the Digital Divide in Africa: A Mediated Analysis-Bruce Mutsvairo, Massimo Ragnedda Amsterdam University Press, 2019
5. Social Media and Politics in Africa: Democracy, Censorship and Security-Maggie Dwyer, Thomas Molony, Bloomsbury Academic, 2019
6. How to Win Elections in Africa: Parallels with Donald Trump-Chude Jideonwo, Adebola Williams BookBaby, 2018

7. Digital Democracy, Analogue Politics: How the Internet Era is Transforming Politics in Kenya-Nanjala Nyabola, Bloomsbury Academic, 2018
8. Africa-internet.pdf
9. Report: The State of Internet Freedom in Africa 2020
10. An Overview of Internet Shutdowns in Africa | Ikigai Law
11. Internet shutdowns in Africa threaten democracy and development
12. Internet and Social Media Shutdowns on the African Continent | Global Risk Insights
13. What we do (not) know about Internet shutdowns in Africa | Democracy in Africa
14. An explainer for when the internet goes down: What, who and why? | African Arguments
15. Policy Brief: Internet Shutdowns
16. An Explainer for When the Internet Goes Down: What, Who, and Why?
17. Shutdown Lawsuit Monitor (SLaM): tracking legal actions around internet shutdowns
18. Telco Action Plan Respecting Human Rights: Ten Steps and Implementation Objectives for Telecommunications Companies
19. The Current Shutdown
20. Ending internet shutdowns to #KeepItOn
21. Navigating Litigation During Internet Shutdowns In Southern Africa