**Sub-Saharan Africa Internet Freedom Landscape.**

Open Technology Fund, November 2017 Annual Summit in Valencia Spain.

**A Conference Report**

**Contributors: All conference attendees mostly from Sub Saharan Africa with specific contributions from Julie Owono on West and Central Africa. Compiled and edited by Arthur Gwagwa assisted by Shamiso Mungofa.**

*November 2017*

This is a broad overview of the Sub Saharan Africa (SSA)Internet freedom landscape prepared for the Open Technology Fund[1] November 2017 Annual Summit in Valencia Spain. The report singles out the increasing trends in internet shutdowns especially targeted at social media as the main current threat against digital rights. This is running concurrently with the continued trend of the criminalisation of legitimate speech which has encroached to online spaces. The proliferation of cybercrime laws which pits national security against personal security of the individual is one of the emerging trends. The extent to which states are increasing the technical capabilities to match the laws is an area that requires urgent investigation. The report is meant to guide further detailed research and foster multi-stakeholders' discussions on internet security and freedom in the region.

## HIGHLIGHTS

### 1. Current and emerging threats

### Access to Internet and the necessary infrastructure

- **Complete Internet Shutdowns (Total blackouts)**

Since the beginning of 2016, a number of African governments have shut down the Internet especially in the lead up to elections or during periods of civic unrest.[2] Most notably in 2017, Cameroon enforced a 93-day blackout in its English-speaking regions amid mounting protests[3] and in 2017,Togo repeatedly shut down the internet to stifle growing resistance to the long ruling Gnassingbe family dynasty.[4]

[1] https://www.opentech.fund/

[2] https://beta.theglobeandmail.com/news/world/regimes-increasingly-shutting-down-internet-to-control-protests/article36223534/?ref=http://www.theglobeandmail.com&

[3] https://qz.com/964927/caemroons-internet-shutdown-is-over-after-93-days/

[4] https://beta.theglobeandmail.com/news/world/regimes-increasingly-shutting-down-internet-to-control-protests/article36223534/?ref=http://www.theglobeandmail.com&

- **Partial shutdowns**

In a significant number of instances, some governments resorted to partial shutdowns which mostly targeted social media. Mali did so during protests around constitutional reform and Somaliland, the 2017 elections. The current shift from websites to social media shutdown is largely attributed to slow internet adoption, the prevalence of mobile phone usage coupled with websites that may not be mobile phone- compatible.

- **Attempts to shut down the Internet**

Ghana's government discussed the possibility of shutting down the internet ahead of the December 2016 elections. Kenya had similar discussions ahead of its August 2017 general elections and Lesotho attempted and failed twice to shut down social media in the run up to the June 2017 elections.

- **Just in Time temporary disconnections**

Namibia and Swaziland applied 'just in time' temporary disconnections or event-based denial of selected content or services. As explained by Deibert and Rohozinski,[5] these techniques can be difficult to verify, as they can be made to look like technical errors applied in ways that assure plausible, for example during important anniversaries. In the case of Namibia, internet has often been temporarily disconnected in regions where the president is visiting. In Swaziland's case, this has occurred during visits by foreign dignitaries and during the high court hearings of important human rights cases which potentially exposed the country's bad human rights record.

**Restrictions of content on the Internet**

- **Blocking and Filtering**

Currently there is no confirmed and technically-verified widespread blocking and filtering of websites except in Ethiopia where the situation is ongoing, in Rwanda before and during the 2017 election, South Sudan in 2017 and Nigeria where a list of 21 URLs mostly run by the indigenous people of Biafra (who seek independence from Nigeria) were reportedly blocked around November 2017.

- **Criminalisation of hate speech, slander, defamation and other forms of critical speech.**

[5] Ronald Deibert and Rafal Rohozinski, "*Control and Subversion in Russian Cyberspace*," in Ronald Deibert et al., eds., Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace

A number of governments relied on expanded use of defamation, slander, and ‘‘veracity’’ laws to deter bloggers and independent media from posting material critical of the government or specific government officials. Such criminalisation now covers hate speech in the case of Kenya and also in Nigeria where the federal government has been debating a hate speech law and even considering classifying hate speech under terrorism. This has often overlapped with reliance on national security concerns to clamp down on speech deemed as subversive. In Zimbabwe, an American citizen was detained over a tweet which allegedly slandered the president[6].

**Next Generation Controls through content manipulation.**

**Propaganda and Disinformation[7] and Fake News[8]**

**Fake News in SSA.**

State censors used claims of “fake news” as motive to censor the internet most recently[9], in Kenya. Ironically, during Kenya’s August 2017 election, some politicians benefitting from such news did not shut down the internet even despite their earlier undertaking to do so.

**Censorship by Proxy and Intermediary Liability**

A number of African governments also used other means at their disposal to suppress online speech, including pressuring companies to take down content through the imposition of liability on intermediaries for not complying with information or surveillance requests and censorship of content.

**Surveillance and use of malware**

[6] https://www.reuters.com/article/us-zimbabwe-usa-goblin/zimbabwe-police-charge-u-s-citizen-with-anti-government-plot-idUSKBN1D31BS

[7] Although propaganda is an old phenomenon both off and online, its intersection with disinformation and fake news has been convoluted, especially in Africa. Disinformation is “dissemination (in the press, on the radio, etc.) of false reports intended to mislead public opinion.” Propaganda generally connotes the selective use of information for political effect. Whether and to what degree these terms overlap is subject to debate. While the use of disinformation is not new, the digital revolution has greatly enhanced public vulnerability to manipulation by information—a trend which is predicted to continue.

[8] Fake news generally refers to misleading content found on the internet, especially on social media. One analysis lays out five types of fake news, including intentionally deceptive content, jokes taken at face value, large-scale hoaxes, slanted reporting of real facts, and coverage where the truth may be uncertain or contentious. More often than not, fake news does not meet the definition of disinformation or propaganda. Its motives are usually financial, not political, and it is usually not tied to a larger agenda.

[9] http://www.aljazeera.com/indepth/opinion/2017/08/kenya-latest-victim-fake-news-170816121455181.html

**Use of malicious software (Malware) in crime investigation**

A significant number of countries have or are in the process of passing cybercrime laws. A problem that emerges from this is the extent to which the use of malware/spyware in computer remote searches will comply with best practice once most countries' cybercrime laws come into force. Use of malware has been reported in countries like Ethiopia. To address the question of the problems that may arise from the cybercrime laws, it might be necessary to find out if states are trying to catch the law up to practice or whether technological development will follow the passage of the laws. There is also a need to explore how dual use technologies such as middle boxes work, e.g., what they are being used for.

**Surveillance**

A number of governments are using surveillance powers. In the case of Kenya, surveillance is preferred over censorship whereas in Ethiopia, it is used alongside censorship. Future research should try to further examine how surveillance relates to censorship. Also, an understanding of the surveillance market will help shed light on where repressive governments are obtaining their surveillance technologies from. In the case of censorship and surveillance, states are out to balance the national and individual liberty.

## 2. Current needs and possible solutions

**Awareness Raising**

In order to respond to the current and emerging trends, digital rights activists and donors should undertake several important steps. Firstly, raise awareness—online and elsewhere on the ongoing issues in countries such as Cameroon. In raising awareness, there should be solidarity among organisations such as that between Access Now and Internet Sans Frontières in Cameroon. This should also include building bridges with traditional democracy defenders.

**Awareness Raising**

In order to respond to the current and emerging trends, digital rights activists and donors should undertake several important steps. First, raise awareness—online and elsewhere on the ongoing issues in countries such as Cameroon. In raising awareness, there should be solidarity among organisations such as that between Access Now and Internet Sans Frontières in Cameroon. This should also include building bridges with traditional democracy defenders.

Contributor at the Summit stated that:

In raising awareness, internet rights activists and technologists need to work with regular civil society to make them understand the internet. We need to build and go beyond our work to step out of our comfort zone and make that connection, translate it into reality and make them understand what is at stake. Digital is central to their organizations and their work.

There is a bridge to build between our world in tech and the democracy defenders. People know they are being surveilled and they seem to be okay with it. Should we be working alternative platforms? We need to use all the other technologies that exist.

**Circumvention and censorship measurement**

Digital rights activists should take steps to measure internet censorship especially reliance on technical means such as the OONI software. Secondly, they should raise awareness and train users at risk on circumvention and other privacy and security enhancing tools. Taking Cameroon as an example, during its two successive blackouts, Cameroonians used circumvention technology such as VPN apps to access and share information, organized community support networks, to sharing their stories to provide crucial evidence of human rights interference and abuse.

**Demonstrating the economic impact of shutdowns**

Activists must work proactively and creatively with tech companies to convince African leaders of the devastating economic impact[10] that internet shutdowns, and other related disruptions, have had on African economies.[11] One study[12], for example, found that the internet shutdown in Cameroon cost business in the affected regions US$1.39 million in lost sales—an enormous sum in a country with a per capita GDP of just over $1000.[13] However, this economic argument will not resonate with everyone. Repressive regimes such as Cameroon's Paul Biya will always prioritize regime survival above all else. However, this approach might work with more pragmatic governments and help to build an important counter-narrative that appeals to different segments of society who share a collective interest in advancing their personal well-being.[14]

**Further Technical Research/Alternative Infrastructure**

In instances of complete shutdowns such as in Cameroon, the use of VPNs, orbots, tor, tails and other common Internet censorship circumvention tools have been ineffective. There is need for further research work that sets out to understand technically, how the Internet was cut off and to explore alternatives such as mesh networks, alternative

[10] https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf
[11] http://www.africanews.com/2017/02/18/cameroon-internet-shutdown-costs-139m/
[12] http://www.africanews.com/2017/02/18/cameroon-internet-shutdown-costs-139m/
[13] https://data.worldbank.org/indicator/NY.GDP.PCAP.CD?locations=CM
[14] https://www.cfr.org/blog/what-zimbabwes-cybersecurity-ministry-says-about-human-rights-country

infrastructure, circumvention if there is blocking is easy but blackout is really hard. The Serval project[15] is a good example trying to build alternative infrastructure outside the usual internet like meshnets.

### Need for funding

Funders need to coordinate better how they can slice up all the pieces that they need to fund. Digital rights activists just need to use the current leverage they have with funders and identify those willing to customise their funding. This could be in the forms of a coalition of well-coordinated funders.[16]

## SUB-REGIONS

## EAST AFRICA

### Introduction: Regional Snapshot

Although the internet offers opportunities to CSOs and advocates to engage with the public, share information, and advocate for citizens' rights, it also offers the possibility for regional, state and non-state actors to interfere with their work, surveil them, and censor their voices especially in challenging and closed political environments. In Burundi, for example, although the country has introduced a number of protections for freedom of speech and the right to privacy, ambiguously worded laws provide opportunities for governmental bodies to systematically restrict internet freedom in the country.

### Detailed Case Studies

## ETHIOPIA

Ethiopia, just like Rwanda, provides an insight on the conflictual process through which ICTs are already shaped and reshaped by a variety of actors in developing countries.[17] When it comes to development and in particular, the role of ICTs, both countries are two faced and present two images: One is a closed, authoritarian state, governed through fear by an ethnic

[15] https://github.com/servalproject
[16] Participant recommendation. OTF Summit, Valencia, Spain, November 2017
[17] https://www.academia.edu/34498994/The_Politics_of_Technology_in_Africa

minority whilst the other, especially in the case of Ethiopia, is a developmental state that has achieved sustained 'double digit' growth and has significantly improved access to basic services.[18]

## Current Landscape

Ethiopia has continued to rely on judicial and extra judicial means to stifle freedom of expression and privacy including online. For instance, in April 2017, the Ethiopian Supreme Court ruled that two members of the Zone-9 bloggers' collective who were facing terrorism charges under the draconian Anti-Terrorism Proclamation (ATP) should face a new trial for offences against the Constitution, partly for learning how to encrypt their messages.[19] Amnesty International responded that, "Learning how to encrypt messages is not a crime, but a freedom protected under the right to privacy and freedom of expression."[20]

In October 2016, the Ethiopian Prime Minister Hailemariam Desalegn declared a nationwide six-month state of emergency. Among other measures, the state authorities also blocked social media access, and intensified the practice of internet censorship. By March 2017, the parliament had used the ongoing unrest in the country to justify unanimously extending the state of emergency another four months. Such limits on embodied and digital freedoms are merely an escalation of the rigorous security measures that Ethiopians have long faced. Authorities have also subjected these vulnerable groups that include activists, journalists, minority groups, opposition party members, and expatriates to targeted embodied and digital surveillance to further stymie their abilities to communicate, organize, and dissent.[21]

## Current Threats

*State Monopoly of ICTs (Digital or Networked Authoritarianism).*

The state's monopolization of information and communications technologies (ICTs) and media channels has become another key means of augmenting its authority. The country's sole telecommunications service provider, Ethio Telecom, is state-owned and controls all access to phone and internet networks. The government can determine which websites and

[18] https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/6623/6424
[19] https://www.amnesty.org/en/press-releases/2017/04/ethiopia-fresh-trial-for-two-zone-9-bloggers-flies-in-the-face-of-justice/
[20] https://www.amnesty.org.uk/press-releases/ethiopia-new-trial-bloggers-accused-encrypting-messages-flies-face-justice
[21] https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/6623/6424

services to censor, and when to obstruct access altogether. Although most radio and television stations are already affiliated with the government, it can also jam signals to block objectionable content from airing.[22]

*Low Internet Access*

This maintenance of state control is partly responsible for Ethiopia having far lower rates of digital adoption than its neighbours. While the state has enlisted the services of Chinese telecom firms Huawei and ZTE and Swedish firm Ericsson, the rural infrastructure remains underdeveloped. This setback has compounded other contributing factors of diminished access, like the prohibitive cost of broadband, inferior connectivity speeds and network coverage, and propensity for outages.[23]

*Data Retention regimes such as SIM Card Registration and Surveillance*

The process of data retention when people register their SIM cards alerts users that their communication practices will make them identifiable, and invariably chills the willingness to discuss sensitive issues on the phone. Authorities like the National Intelligence and Security Services (NISS) have almost unrestricted access to the Ethio Telecom's comprehensive ZSmart database. This database, which Chinese company ZTE installed at the Ethiopian government's behest in 2009, can disclose phone records and other metadata. It can also reveal the contents of text messages and recorded conversations.[24]

*Monitoring of Internet Cafes*

As internet cafés gain popularity in urban areas, the government is also scrutinizing these locations more intensely. The state's primary concern is that the shared computers can anonymize users and enable critics to gather and distribute information in more secure settings. The cafés are subject to many onerous requirements, such as a complex, months-long screening process required to obtain an operator's license and a ban on Voice over Internet Protocol (VoIP). One operator stated that an official ordered him to make every monitor simultaneously visible and to report any suspicious behaviour. Another operator said that officials threatened to confiscate her equipment and imprison her, because a customer had accessed online material that criticized the government. Other officials have demanded details on specific users and the sites they visited and have themselves monitored cafes in plainclothes disguises.[25]

*Filtering and Blocking*

[22] https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/6623/6424
[23] https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/6623/6424
[24] https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/6623/6424
[25] https://www.hrw.org/report/2014/03/25/they-know-everything-we-do/telecom-and-internet-surveillance-ethiopia

Agencies like the Ministry of Communications and Information Technology (MCIT) and the Information Network Security Agency (INSA) are also monitoring online content to prevent online government criticism. Most prevalently, they use their control of telecom networks to filter the internet and block over 100 websites.[26] Through a combination of targeting Internet Protocol (IP) addresses and domains and deep-packet inspection, the state censors sites pertaining to opposition parties, human rights, diasporic dissent, and even the recent drought. It also blocks digital security tools like the anonymizing Tor browser, virtual private networks (VPNs), and the Electronic Frontier Foundation's guide to circumventing surveillance.[27]

*Harassment and Threatening of Bloggers*

As blogs and social media networks gain momentum in Ethiopia, officials are also increasingly monitoring and blocking these platforms' content. One user reported that he faced state harassment for posting an OLF flag on Facebook, while others stated that authorities forced them to change or remove their posts.[28] In the most notorious case, six bloggers from the Zone 9 Collective were even arrested and charged with terrorism for their online speech.[29]

*Warrantless seizure of phones*

The most common method of lower-level and rural forces is to physically confiscate detained opponents' mobile devices. The officials then conduct warrantless searches of these detainees' contacts, messages, and phone logs to use that information in interrogations.

*Military-like approach ostensibly justified as counter-terrorism measures*

National Intelligence and Security Services (NISS), which oversees enforcement against terrorism and other domestic threats, conducts some of the most complex and formidable monitoring methods. Thus, even in a political and digital authoritarian regime, only certain organizations attain the fullest extent of authorization.

*Network Shutdowns*

In moments of unrest, the mass tracking of digital communications intensifies and often precipitates the shutdown of social networks or full internet and mobile access. In addition to such broad applications of digital surveillance, police and government agents disproportionately target populations that they consider a challenge to the EPRDF's unilateral authority. This narrower, more forceful attention directed against people like opposition party

[26] https://freedomhouse.org/report/freedom-world/2017/ethiopia
[27] https://freedomhouse.org/report/freedom-world/2017/ethiopia
[28] https://www.hrw.org/report/2014/03/25/they-know-everything-we-do/telecom-and-internet-surveillance-ethiopia
[29] https://advox.globalvoices.org/behind-bars-in-ethiopia-campaign-to-free-the-zone9-bloggers/

members, critics, journalists, and ethnic Oromo can be coupled with threats, arrests, torture, and imprisonment.

The state can also limit or block landline and mobile phone access during politically sensitive moments. Because users predominantly access the internet through their mobile phones, the shutdown of mobile networks serves a potent dual function of censorship.

*Extraterritorial Surveillance*

The Ethiopian government has also covertly adopted advanced surveillance technologies to target opponents outside of the country. In 2013, Citizen Lab security researchers discovered FinSpy, a remote monitoring system, on the computers of three members of the diaspora (Marquis-Boire et al. 2013).[30] Among its capabilities, FinSpy can extract files from a computer's hard drive; enable live microphone and webcam surveillance; record communications taking place over email, chat, and Voice over Internet Protocol (VoIP); and monitor every feature of Skype (Finspy n.d.).[31]

**Emerging Trends**

*Authoritarian Dilemma*

The historical antecedent has led to a shifting of the country's political landscape: the growing centrality of information and communication technologies (ICTs) has aggravated the problem often referred to as the "Dictator's Dilemma." This quandary presents authoritarian governments with the choice between increasing digital freedoms that can facilitate national development and participation in the global information economy, and restricting digital freedoms to try to tamp down internal dissent and preserve the regime's power.[32]

*Next Generation of Controls- Surveillance*

To address the dilemma pointed above, particularly to promote higher rates of digital adoption; Ethiopia is increasingly enacting "next-generation techniques" of control as alternatives to the widespread denial of digital access.[33] These are "more subtle, flexible, and even offensive in character" There is an intensification of surveillance as one such

[30] https://citizenlab.ca/2014/04/citizen-lab-collaborates-human-rights-watch-internet-censorship-testing-ethiopia/

[31] https://citizenlab.ca/2014/04/citizen-lab-collaborates-human-rights-watch-internet-censorship-testing-ethiopia/

[32] https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/6623/6424

[33] https://www.academia.edu/34498994/The_Politics_of_Technology_in_Africa

mechanism of control. While surveillance does not supplant internet filtering and operates alongside it, the multiscalar enactments of monitoring arguably authorize the expansion of digital usage. Because the state has monopolized internet access and controls the telecom infrastructure, intelligence agencies maintain the ability to opaquely monitor the country's residents online.[34]

*Surveillance keeps people offline*

Paradoxically, the prevalence of surveillance is also a substantial hindrance to the adoption and use of digital technologies in Ethiopia. Because of the covert, unpredictable nature of surveillance, both its real and perceived abuses meaningfully chill the ranges of self-expression and communication. State incursions also obstruct the flows of domestic and global information exchange, accelerate social divisions among citizens, and ultimately restrict the full capacity of sustainable development.

## Current Needs

There is still need for more comprehensive scholarly exploration of digital surveillance in this national and regional context.

Second, developers should explore more sophisticated circumvention techniques since the Ethiopian government currently blocks digital security tools like the anonymizing Tor browser, virtual private networks (VPNs), and the Electronic Frontier Foundation's guide to circumventing surveillance.

## Possible Solutions

Digital rights activists, organisations such as Human Rights Watch, Access Now and Amnesty International should collaborate with democrats within Ethiopia and other progressive technological corporations to put pressure British companies like Gamma to refrain from selling tools such as FinSpy to repressive states like Ethiopia. Use of such technologies without proper accountability and transparency structures poses a challenge: If you sell it to a country that obeys the rule of law, they may use it for law enforcement. If you sell it to a country where the rule of law is not so strong, it will be used to monitor journalists and dissidents.[35]

A good example of such a 'push back' campaign is the one recently led by Access Now and Citizen Lab[36] which subsequently led the Blackstone Group to drop its plans to invest in NSO Group and its surveillance technology and to publicly commit to a plan

[34] https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/6623/6424

[35] https://ecadforum.com/2016/10/22/access-now-urges-companies-not-to-sell-technology-to-ethiopia/

[36] https://www.accessnow.org/blackstone-hit-brakes-nso-spyware-deal/

ensuring its current and future investments will not facilitate human rights violations. Pressure should similarly be applied on ISPs.

> "Since licenses agreements reveal the extents that ISPs are required to do, customers can push back to ensure that ISPs only do as much as they are required to. Digital rights activists, developers and those who back their work should hold corporations to account. This may include, for example, ensuring that they still comply with the EU laws on privacy and accountability in the countries they operate in. Pressure must be applied on intermediaries and making them take responsibility of what happens on their platform such as what Psiphon and Signal are trying to do.[37]

## RWANDA

### Current Landscape

Rwanda held general elections on 4 August 2017 during which the government neither shut down the internet nor engaged in the wholesale blocking of access to social networking platforms and all critical platforms. A number of foreign run critical online publications remained accessible. However, a number of websites that were blocked in the past and leading to the election, especially critical online publications in vernacular, remained blocked and only accessible through circumvention.

### Current Threats

According to a recent report[38], the Rwandan government and its agencies have routinely but in a targeted manner repressed freedom of expression and privacy online in the following ways:

- Restricting content on the internet including arbitrary blocking, throttling or filtering of content, and prosecuting dissidents or forcing them into exile.
- Pressuring communication service providers to comply with its orders to take down content and requiring them to ensure that their systems are technically capable to enable communications interception upon request, despite having a law that purports to protect intermediaries.
- Utilizing propaganda to shape online narratives, particularly of the ethnic conflict that started from 1959 culminating in the 1994 genocide.

[37] Participant recommendation. OTF Summit, Valencia, Spain, November 2017

[38] https://www.opentech.fund/article/new-report-investigates-internet-censorship-during-rwandas-2017-presidential-election

- Relying on reminding people of the 1994 genocide to generate and allow a single official narrative, ostensibly as a measure towards non-recurrence and justify social control including online.

## Emerging Threats

*Blocking during political events*

During the period leading to the 2017 elections, although the government of Rwanda did not block websites on a wholesale scale, it used technical means to block and filter web content on topics that ranged from human rights, to genocide and national governance. Out of the 10 websites tested[39], half of them, mostly run by Rwandans who fled the country to seek asylum in other countries, were blocked. These included Inyenyeri News, The Rwandan, and Le Prophete.

The same report[40] also observed patronage in the manner such websites were blocked; for example, while websites for Umusingi Online news and Ireme formed part of the legacy websites that were once blocked, where accessible as the government unblocked them when their owners negotiated a settlement.

*Surveillance:* The government also exercised network surveillance by monitoring communications on social media such as WhatsApp and on emails presumably to obtain intercept evidence to build cases in politically-motivated treason cases.

*Regulation-based social control*: It also relied on legal, regulatory frameworks and extra judicial social control to neuter online debate on issues that matter to the average Rwandan, especially to minority groups. We recorded no less than five cases of dissidents who had been prosecuted and sentenced to long custodial sentences for their views on governance and genocide. Those who were not prosecuted managed to flee to seek asylum elsewhere.

*Faux Democracy:* As part of the current authoritarian resurgence, they create a facade of democracy to maintain a veneer of legitimacy. Rwanda did this by creating fake political parties and news media and GONGOs to simulate democratic institutions to prevent authentic democracy from ever taking root.

## Current Needs

[39] new-report-investigates-internet-censorship-during-rwandas-2017-presidential-election
[40] https://www.opentech.fund/article/new-report-investigates-internet-censorship-during-rwandas-2017-presidential-election

- Capacity building on how to access the internet including tools to circumvent website blocks, connection blackouts and widespread censorship.
- Awareness of privacy and security threats and protective measures including how-to-guides, instructional apps and other efforts to increase the efficacy of internet freedom tools
- Privacy enhancement interventions including the ability to be free from repressive observation and the option to be anonymous when accessing the internet.
- Security from danger or threat when accessing the internet including encryption tools.
- Translation of the above tools into local languages as the majority of Rwandans does not speak English.

**Possible Solutions**

Assess and support users who are most at risk to improve digital defences through capacity building and training on the deployment and use of privacy and security enhancing technologies. Through user manuals and one-on-one and group-based mentoring, introduce them to circumvention tools such as VPNs, Tor Browser and Tor Bridges but also technologies such as the Deflect, Deflect Labs and CENO projects to enable freedom of expression and association online.

## KENYA

### Historical Antecedents

Kenya is a very good example of the internet's facilitation of economic stability, growth and a decisive contribution to human development. At the same time, the state's response to actual or perceived cases of cyber-terrorism, online crime, and other forms of Internet misuse demonstrate how Internet governance remains a challenge in need of urgent attention in the country. Although Kenya has come a long way in introducing liberal market reforms that have immensely benefited the technology sector, policy challenges remain[41]. In particular, there have been serious signs of relapse in the form of laws introduced as measures that restrict civil liberties, ostensibly as anti-terrorism measures, as well as to diffuse ethnic tensions. Unlike Rwanda and Ethiopia, OONI network measurements[42] that have been collected from Kenya over a period of 5 months in 2017 showed no signs of internet filtering. Even though network measurements were collected from 4 different vantage points on an almost daily basis over the period of 5 months, they found almost no signs of internet censorship in Kenya. While it is positive that almost no signs of censorship were detected, OONI acknowledge that their methodology presents various limitations, as outlined in the report.

[41] https://www.academia.edu/34263366/An_Assessment_of_the_Evolution_of_Kenya_s_ICT_Law_and_Policy_Framework

[42] https://ooni.torproject.org/post/kenya-study/

However, like Ethiopia, networking surveillance is very pervasive, and sometimes with chilling effects.[43]

A crucial issue at hand in Kenya, and one that has been the subject of intense debate, is whether the August 2017 election failed simply due to technological challenges or due to a systemic lack of good governance and respect for democratic rights. Critics hold that, "When human rights violations take place within a technological context, it can lead poll observers, monitors and even seasoned election experts to draw false conclusions that can entrench wholly undemocratic and illiberal practices."[44] For instance, in Kenya, many have identified the problem as one of a lack of proper oversight of election technology.[45]

**Current Landscape**

Kenya held elections in August followed by the Kenyan Supreme Court's ruling nullifying the re-election of President Uhuru Kenyatta.[46] It was the first time in Kenyan history that an election result was annulled as the result of irregularities in ballot counting, the unreliability of the electronic voting machines, and the absence of transparency at Kenya's Independent Electoral and Boundaries Commission (IEBC), which oversaw the vote. Following the nullification, another election was held on 26 October which the opposition, NASSA refused to take part in amid protests by its supporters.

**Current Threats**

*Criminalisation and silencing of legitimate expression by the state*

Following the violence that followed the disputed presidential election in 2007[47], which haunted Kenya's 2013 elections, the overarching message online and offline was[48] "peace at all costs," including online platforms.

In the aftermath of the 2007 election, the government enacted laws, such as the National Cohesion and Integration Act of 2008[49] to control hate speech on national security grounds. Similarly, in 2017, it passed social media regulations[50] banning political messages in languages other than Kiswahili and English and the use of language that was deemed

[43] https://medium.com/privacy-international/press-release-new-privacy-international-investigation-exposes-the-role-of-kenyan-government-f08dff4f0630
[44] https://www.worldpoliticsreview.com/articles/23290/is-kenya-s-election-debacle-a-failure-of-technology-or-governance
[45] http://www.nation.co.ke/oped/blogs/dot9/walubengo/2274560-4092456-jtddif/index.html
[46] http://www.nation.co.ke/oped/blogs/dot9/walubengo/2274560-4092456-jtddif/index.html
[47] https://www.theguardian.com/world/2017/aug/10/kenya-election-observers-urge-defeated-candidates-to-accept-result
[48] https://www.huffingtonpost.com/susan-benesch/kenya-elections_b_2921096.html
[49] http://kenyalaw.org/lex/actview.xql?actid=No.%2012%20of%202008
[50] http://www.dw.com/en/kenya-warns-of-social-media-crackdown-ahead-of-polls/a-39783282

offensive. This was to prevent political speech in other languages frequently spoken in Kenya and to probably facilitate government monitoring of online speech. It attracted the ire of human rights groups, some of whom felt these regulations were heavy handed and could be open to abuse.

Laws restricting online expression clash with Kenya's reputation as one of the most vibrant and fast-growing tech sectors in Africa. Researchers at Kenya's Strathmore Law School recently pointed out that Kenya's internet "is underpinned by authoritarian measures that curtail online rights" despite "liberal market reforms [that] enhanced the technical and regulatory capabilities of its ICT sector to drive economic growth[51]."

The latest election also showed that liberal ideals have been sacrificed at the altar of economic progress, peace and stability. This in part has led Freedom House to rate Kenya as a "partly free" society on most human rights and governance indicators.[52]

**Surveillance of HRDs.**

Privacy International Report reveal that the Kenyan Government uses wide ranging extrajudicial surveillance.[53] The National Intelligence Service has powers to order "covert operations," without court approval or review to enter any place, or to search or seize any record or communication. In fact, the bill would grant broad authority to "do anything considered necessary to preserve national security." This also includes the surveillance of social media including WhatsApp groups.[54]

**Propaganda, Disinformation and Fake News**

*Social Media groups*

Technology impacted on both content and dissemination of content during Kenya's 2017 elections. For instance, social media platforms such as WhatsApp, Twitter, and Facebook facilitated the spread of propaganda and fake news. In turn, the government attempted, in

[51] http://blog.cipit.org/2017/07/04/new-cipit-research-an-assessment-of-the-evolution-of-kenyas-ict-law-and-policy-framework/
[52] https://freedomhouse.org/report/freedom-world/2017/kenya
[53] https://medium.com/privacy-international/press-release-new-privacy-international-investigation-exposes-the-role-of-kenyan-government-f08dff4f0630
[54] https://qz.com/1068651/whatsapp-is-at-the-center-of-an-argument-in-kenya-over-hate-speech/

various ways, to regulate online information, including through regulations, surveillance, and direct online engagement with critics.[55]

Much of the fake news, however, was spread through private groups on WhatsApp, which kept it hidden from the open web and also in many cases rendered stories more powerful as they were spread through trusted networks. At the same time, much of the fake news and negative campaigning was very professionally done, for example, the purveyors of fake news understood the political landscape and appropriately packaged their videos and memes in a targeted and convincing fashion.[56]

The false narratives are also augmented by the endless stream of misinformation, propaganda, and made-up stories currently being shared on social media—a trend that is now worrying both analysts and mainstream media outlets.[57]

*Role of Data Analytics companies- Computational Propaganda*

It was reported that Cambridge Analytica may have been responsible for much of the content in support of Uhuru Kenyatta.[58]

*Local political brigades and operatives and fake sites*

Local Kenyan political operatives have also been registering fake news websites like Foreign Policy Journal[59] (fp-news.com) or CNN Channel 1(cnnchannel1.com) to propagate false stories during the election. FP News carries stories like how Western think tanks believe President Uhuru Kenyatta would win a majority[60] of the vote, even when polls showed that the race was tight.[61] Another article reported on how the opposition leader Raila Odinga was orchestrating[62] the recent attacks on white-owned ranches[63] and conservations in Kenya. In fact, a majority of the articles on the site are against Odinga, drawing either false conclusions[64] about his past, distorting or selectively omitting facts[65], or providing no context.[66] (Quartz Africa, 2017)

[55] https://cyber.harvard.edu/events/2017/10/Mutungu
[56] https://cyber.harvard.edu/events/2017/10/Mutungu
[57] https://qz.com/1011989/fake-news-and-misinformation-are-upstaging-kenyas-upcoming-high-stakes-election/
[58] http://www.aljazeera.com/programmes/listeningpost/2017/08/fake-news-shape-kenya-elections-170805081741474.html
[59] http://fp-news.com/
[60] http://fp-news.com/incumbent-president-uhuru-kenyatta-will-win-58-western-think-tanks-predict/
[61] https://www.the-star.co.ke/news/2017/05/31/uhuru-raila-in-tight-race-ipsos-opinion-poll-shows_c1571200
[62] http://fp-news.com/british-authorities-and-ranchers-raila-odinga-behind-laikipia-land-invasion/
[63] https://qz.com/947071/in-laikipia-drought-induced-violence-is-threatening-kenyas-tourism-and-conservancy-efforts/
[64] http://fp-news.com/odinga-lost-the-ballot-printing-tender-and-now-he-is-on-a-revenge-mission/
[65] http://fp-news.com/u-s-embassy-report-raila-odinga-behind-2billion-maize-scandal/
[66] https://qz.com/1011989/fake-news-and-misinformation-are-upstaging-kenyas-upcoming-high-stakes-election/

*Impact of Fake News*

According to critics, in a high-stakes election like this one, the explosion of false stories upends the role of mainstream media, considered the most trusted institution in the country.[67] This presents a challenge to the journalism fraternity, different from the 2007 elections, when local language radio stations took part in inciting the violence[68] that led to the death of more than 1,000 people.[69]

**Emerging Threats**

*Role of Biometrics*

The 2017 elections gave hope as the French-based company Safran Identity & Security provided Kenya's Independent Electoral and Boundaries Commission (IEBC) with "complete and secure" voting kits to verify and authenticate the voting processes.[70]

Nevertheless, the elections did not go according to plan following the opposition's allegations of deliberate interference with the electronic voting system.[71] According to the court papers[72], when the opposition requested access to the electronic systems for verification purposes, the IEBC refused, arguing that releasing such information was "likely to compromise the integrity and security of the information technology systems."
In this case, the IEBC relied on national security to deny their citizens information that is necessary to carry out their civic duties, such as demanding accountability and transparency, also can extend to the technological sphere.

Although the Court was of the view that 'technologies are imperfect and recommended the IEBC to put in place a complementary system for use when technology fails, the crux of its decision to annul the election was based on the IEBC's failure to follow the clear and transparent technological process whose aim is to ensure a verifiable transmission and declaration of results system.[73]

Such failure was therefore tantamount to a failure to adhere to the rule of law which might lead candidates and citizens to perceive the election not to be free and fair thus leading to instability. Put otherwise, good governance as demonstrated by adherence to the rule of law leads to stability.

[67] https://www.standardmedia.co.ke/article/2000196323/survey-media-the-most-trusted-institution
[68] https://www.theguardian.com/journalismcompetition/making-peace-not-war
[69] https://qz.com/1011989/fake-news-and-misinformation-are-upstaging-kenyas-upcoming-high-stakes-election/
[70] https://www.safran-group.com/media/kenya-selects-safran-identity-security-accompany-its-2017-elections-20170427
[71] http://foreignpolicy.com/2017/08/09/opposition-claims-kenyas-election-was-hacked-fueling-fears-of-unrest/
[72] http://www.judiciary.go.ke/portal/page/election-petitions
[73] https://qz.com/1011989/fake-news-and-misinformation-are-upstaging-kenyas-upcoming-high-stakes-election/

## Current Needs

In future elections, Kenya must put in place both human and technological measures to safeguard the integrity of the vote and its accurate reflection of the will of the people as elections can decide the political course of nations for years, even decades. While it is reassuring to know there is a judicial system to turn to in case procedures fail, it should not o have to come to that to ensure adequate accountability in one of a country's most crucial democratic processes.

## Possible Solutions

*Biometric Technology*

Building the capacity of civil society, political opposition on biometric technology and latest good practice in electronic voting and understanding biometrics.[74] In future elections, donors and election monitors should seek to improve the oversight of the IEBC and ensure that the commission and its staff independently discharge its constitutional mandate. Voters' right to privacy should also be protected during the use of biometric technology.[75]

*Addressing Fake News*

The production and impact of fake news can be reduced through civic education and campaigns. Corporations fought back against fake news through ads during the Kenyan election.[76]

On a positive note, the fake news opened up debate on issues that matter to the Kenyans such as truth, justice, and reconciliation. Also, fake news may have prevented an internet shutdown around the election. "All indications were that there would be a shutdown', but in the end the government did not shut it down and one of the reasons could be that it was benefitting from much of the false content, that fake news was motivating more people to go to the polls, and that the political cost for shutting down the internet may have been too high.[77]

Sharing timely and factual information is also an important strategy. For instance, Sambuli says that sharing timely and factual information with audiences helps forestall misinformation from running amok. The media was still a primary source of information for many Kenyans, and she said they should not squander the opportunity to step in during these

[74] http://blog.cipit.org/category/cipit-insights/
[75] http://blog.cipit.org/2017/12/15/cipit-research-investigates-misuse-of-biometric-voter-data-and-impact-on-kenyans-privacy/
[76] https://cyber.harvard.edu/events/2017/10/Mutungu
[77] https://cyber.harvard.edu/events/2017/10/Mutungu

critical times. “Asking how, why and other probings go a long way in assessing accuracy and credibility of information, which is everywhere these days.[78]

*Propaganda and Disinformation*

Computational propaganda can be addressed through better algorithm design rather than through censorship. Some critics who hold this view say that democratic governments concerned about new digital threats need to find better algorithms to defend democratic values in the global digital ecosystem. Democracy has always been hard. It requires an exquisite balance between freedom, security and democratic accountability. This is the profound challenge that confronts the world’s liberal democracies as they grapple with foreign disinformation operations, as well as home-grown hate speech, extremism, and fake news. Fear and conceptual confusion do not justify walking away from liberal values, which are a source of security and stability in democratic society. Private sector and government actors must design algorithms for democracy that simultaneously optimize for freedom, security, and democratic accountability in our digital world.[79]

## DJIBOUTI

### Current Landscape

Despite its very limited territory (23, 200 square kilometres) and its population of less than 1 million people, Djibouti is a country of great interest given its unique geostrategic location in the Horn of Africa. As well as a state of the art port, it hosts a major meeting point for undersea fibre optic cable systems connecting Europe, the Middle East, and Asia, to Africa. Djibouti hosts military bases for France, the United States, Japan and NATO, as well as other foreign forces (Belgium, Germany) that are located in the country to support anti-piracy efforts. It is an active and cooperative counterterrorism partner with the U.S and Western countries and was recently labelled as the “superpowers’ playground”

Despite hosting undersea cables and a data centre that serves the region Djibouti had 105,000 Internet users in 2016, Internet penetration: 8 %, Mobile penetration: 22%, Internet access at home: 3%, and High -speed connection: US$63 per month (twice the price charged in Ethiopia)

### Current Threats

[78] https://qz.com/1011989/fake-news-and-misinformation-are-upstaging-kenyas-upcoming-high-stakes-election/

[79] https://www.cfr.org/blog/protecting-democracy-online-disinformation-requires-better-algorithms-not-censorship

*National laws related to human rights online*

Following the November 2015 Paris attacks, the Council of Ministers adopted the introduction of the emergency state on the 24th November 2015. This measure was reportedly used against opposition leaders, human rights defenders and journalists including online. An example is Decree n° 2015 - 3016 PR/PM forbidding gatherings and reunions in public space in order to fight against terrorism. ((« Décret interdisant les rassemblements et les réunions sur la voie publique en tant que mesure de lutte contre le terrorisme »).

*Privacy*

Although the constitution and law prohibit such actions, the government did not respect these prohibitions. The law requires authorities to obtain a warrant before conducting searches on private property, but the government did not always respect the law. Government critics claimed the government monitored their communications and kept their homes under surveillance. The government monitored digital communications intended to be private and punished their authors.

*Censorship and freedom of expression*

Despite Article 15 of Djibouti's Constitution and section 3 of the 1992 Freedom of Communication Law freedom of speech is not upheld in practice, as demonstrated by the fact that individuals who criticized the government publicly or privately could face reprisals. Under the 1992 Freedom of Communication Law, media offences can be punished by jail terms and heavy fines. Restrictions of age and nationality are applicable to those holding senior positions at media outlets.

*Surveillance*

The 2004 Law for the reform of the ICT sector (« Loi n°80/AN/04/5ème L Portant Réforme du Secteur des Technologies de l'Information et de la Communication ») states in its article 4 that "telecom service providers as well as their staff must respect the obligations of the current law and previous regulations, with regard to the respect of the secrecy of correspondence…".

**Emerging Threats**

There is a culture of secrecy and a lack of transparency in the management of the Djibouti Data Centre, which some suspect is also being used by foreign powers and the Djibouti authorities for bulk data retention and surveillance as part of the counter-terrorism efforts.
Allegations of tapping of undersea cables by super powers have also been reported in Djibouti as Djibouti hosts foreign military bases and supports the counter-terrorism efforts.

**Current Needs and Possible Solutions**

There is need for research to further explore the issue of targeting, attacking and exploitation of the networks that maintain communications infrastructure, especially allegations of tapping of undersea cables. The research should also examine how this impacts on the development of an open, secure and accessible internet.

There is need to deploy OONI probes to ascertain the exact state of information controls in technical terms. Perhaps such probes might reveal how far the government has gone in setting up its proposed Eagle programme which would facilitate information controls, especially surveillance

The government should operate in an accountable and transparent manner, for example, to address the current culture of mistrust and fear between the ministry of Telecommunications on one hand and the government, on the other. According to the interviews I carried out with the ministry in September 2016, senior officials in the ministry were reluctant to disclose information without ministerial approval. This polarisation reflects Djibouti's ethnic tension, for instance while the President is of Ethiopian background, some telecoms directors are of a Somalian origin. To address this, there is a need for ongoing engagement with civil society, the media fraternity and government to promote a culture of openness in cyber governance and governance in general.

**TANZANIA**

Whilst the Tanzanian government has been pushing forward with policies and initiatives aimed at improving internet access in rural and underserved areas alongside other infrastructure developments, it has also enacted laws that threaten internet freedom in the country. Most prominent of these laws is the 2015 Cybercrimes Act, which has been used to clamp down on freedom of expression online. However, on March 8, 2017, a court in Tanzania ruled[80] that requests for disclosure of user information for law enforcement purposes pursuant to the Cybercrimes Act (2015) are not arbitrary. On the issue of intermediary liability, Tanzania's proposed Electronic and Postal Communications (Online Content) Regulations, 2017 which specify obligations of service providers and users of online platforms including social media, discussion forums, and online broadcasts (radio and television) to regulate content.[81]

[80] https://cipesa.org/2017/04/tanzania-court-deals-a-blow-to-intermediary-liability-rules/
[81] https://cipesa.org/2017/11/analysis-of-tanzanias-electronic-and-postal-communications-online-content-regulations-2017/

## SOUTHERN AFRICA

### General Overview

Most Southern African countries are working on cyber security and cybercrime laws coordinated under the International Telecommunications Union (ITU) Harmonization of the ICT Policies in Sub-Saharan Africa (HIPSSA) project, in terms of which the ITU has sponsored drafts of cyber security laws for the Southern African Development Community (SADC) region, and allocated its consultants to work with the respective countries.[82]

Although Southern African based human rights organisations such as MISA have audited the draft laws, the extent of states' spying capabilities is not yet very clear, for example, how they are designed technically, how they will operate in practice and the extent to which they will impact or likely impact the privacy and security of HRDs. While most HRDs have sought to challenge such laws wholesale, such an approach does not take into account that targeted hacking, with a search warrant and under suitable conditions, is a useful investigative tool. However, such searches must be targeted, both to comply with legal requirements and to avoid some of the technical risks. Depositing malware to investigate victims' machines is a very tricky business; it should never be attempted lightly.[83] The proposed laws raise the fear of potential overreach and abuse of state powers especially in respect of remote searches on multiple devices. Secondly, although some governments argue that the internet has offered terrorists a means to organise; the securing of national security interests ought to be done in accordance with international law, for example, the respect of the right to privacy and freedom of expression online.

In the Southern African context, cyberspace is increasingly presenting important opportunities and challenges for governance. States, the private sector and civil society have a stake in this dynamic environment. While there is a consensus about the enormous potential for advancing development, the control of cyberspace and management of crime and terrorism is still being debated, and sometimes fiercely.[84]

Also, as seen in the current SIM card registration regimes adopted by a number of southern African countries, there is also still is a lack of understanding of the severity of intrusion caused by blanket retention/mass surveillance of data (and the potential cybercrime issues that that raises, beyond the human rights concerns). This lack of understanding tends to lead to calls for all electronic data to be stored or monitored. Data gathering capabilities ought to

[82] https://www.academia.edu/33876234/Africa_Cyber_Crime_and_Cyber_Security_Fact_Sheet_and_Issues
[83] https://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/1/
[84] https://oldsite.issafrica.org/events/is-south-africa-geared-up-for-new-cyberspace-challenges

be authorised on the basis of a judicial warrant, rather than gathered *apriori* with judicial warrants being necessary only to access the data.[85]

**Detailed Case Studies**

**ANGOLA**

**Current Landscape**

- Low rates of penetration and structural inequalities, such as poverty among the political dissidents have meant that to some extent internet use has not become a major threat to the Angolan political establishment.
- HRDs and Journalists have traditionally faced various forms of hindrances to exercising these rights, including judicial harassment, arbitrary arrests and detention, threats and other forms of intimidation, in particular when they report on issues related to corruption, good governance, police brutality and other topics deemed too sensitive by the authorities.

**Current Threats**

- Denying internet access to the poor majority especially in the secessionist Cabinda province.
- Applying the new laws and other normative pressures and regulations to inculcate an environment of self-censorship.
- Digital surveillance of dissidents and those with who they are in contact as part of a government's broader signals intelligence programme.
- Our OONI tests confirmed the presence of middle boxes which could potentially be used for internet censorship but no block pages were detected.
- Slowing down and attacks of the website of Raphael Marcos, the government has yet to block access to online content.

**Emerging Threats**

- There was a policy shift that began in 2016 when the former President announced in his new year's speech, plans to regulate social media and the creation[86] of the "Angolan Social Communications Regulatory Body" to ensure compliance with new media laws.
- The Government passed 5 draconian laws to govern online speech. Passed under the guise to advance Angolan citizens' rights to freedom of expression, education and to regulate unacceptable social media practices, these laws pose a serious threat to

[85] https://www.academia.edu/11336932/Protecting_the_right_to_privacy_in_Africa_in_the_digital_age
[86] https://www.theguardian.com/world/2016/aug/19/angola-passes-laws-to-crack-down-on-press-and-social-media

freedom of expression. They are designed to control and censor any attempt by political activists to use social media and the internet to blow the whistle on the most egregious examples of corruption, nepotism and the abuse of power.

- While some independent journalists have been regularly reporting on these topics over the past years, most of the others are driven to self-censorship, compelled by the criminalisation of press offences by the authorities.
- Angola saw a change of leadership in August 2017. This may not change the current threat level as the same political party is in place. However, for how long the new president will continue protecting the former president's interests is still being debated. In November 2017, the President fired[87] the daughter of the former president as chief of the state oil company Sonangola.
- Also, instead of totally muzzling free speech online, the government is now known to respond to criticism on social media, for example Dos Santos's daughter's response to a famous Angolan activist Luaty Beirao.

**Current Needs**

- Need for support to civic platforms such as Jiku which is a crowd sourced platform that maps the constituencies through Google maps. This was also used by activists to report on election-related human rights violations. Another app is ZUELA founded by the Friends of Angola based mostly in the U.S.A to help Angolan activists to document research.
- Support HRDs with training on circumvention methods such as encryption of phones and emails and how to use social media in a way that does not expose them to further risk. Amnesty International has been training in methods such as use of wire, signal, and jitsu instead of Skype.

**Possible Solutions**

- Those working on digital rights need to take advantage of the current authoritarian shifting in Angola. This has been prompted by international pressure and in light of economic pressures caused by falling oil prices.
- At legislative level, internet rights activists should push the government to repeal the country's criminal defamation laws and stop using them to harass journalists.
- However, a deep rooted political shift is needed to ensure a separation of powers not only between the judiciary, the Executive and legislature but the independence of the

[87] https://www.bloomberg.com/news/articles/2017-11-15/angola-new-president-fires-dos-santos-daughter-as-sonangol-boss

fourth estate including allowing the internet to play its crucial role in society including the advance of freedom of expression.

## ZIMBABWE

### Current Landscape

Zimbabwe underwent a "coup" which led President Mugabe to resign as President. Ahead of his resignation, the country had started taking a number of measures to stifle digital rights. In October 2017, the government in Zimbabwe, which is already one of the most in the world, signalled its intentions to further crackdown on human rights in the lead up to next year's anticipated elections. This latest move came in the form of a newly created Ministry of Cyber Security, Threat Detection and Mitigation.[88] According to a government spokesperson, its mission will focus on eliminating "abuse and unlawful conduct" in cyberspace like "a trap used to catch rats."[89] The move has widely been viewed—among both domestic and international activists—as yet another attempt to curb freedom of speech online and further entrench the long-abusive regime of Robert Mugabe, in power since 1980.[90] The fact that the new ministry has since been incorporated under the existing ministry of Information and Communication Technology may not mitigate the repression of free speech online. Recently, the Zimbabwe Defence Forces warned against social media abuse.[91]

Ahead of the announcement of the new ministry, "Zimbabwe's ruling party, ZANU-PF, was in the midst of unprecedented internal fractures[92] and repeated leadership crises.[93] This effort to further monitor and curtail the online activities of Zimbabweans and intimidate critics was seen as an early indication that Mugabe and his coterie remained intent on maintaining power at all costs beyond 2018. With the resignation of Mugabe, internet rights activists should continue monitoring whether there will be a policy shift under the new government.

Reports have also shed light that on the day the military took over the streets of Zimbabwe, the former First Lady, Grace Mugabe "put in a call shortly after 7 p.m. to a cabinet minister asking to get WhatsApp and Twitter shut down" when she realised that "social media buzzed with pictures of armoured vehicles driving along roads to Harare, sparking

[88] https://bulawayo24.com/index-id-news-sc-national-byo-91782.html
[89] http://nehandaradio.com/2017/10/11/mugabe-explains-functions-cyber-security-ministry/
[90] https://www.cfr.org/blog/what-zimbabwes-cybersecurity-ministry-says-about-human-rights-country
[91] http://www.thezimbabwean.co/2017/12/chiwenga-latest-security-forces-warn-misguided-elements/
[92] https://www.ft.com/content/f23e4366-eac5-323b-96ae-40ef71ac81e3
[93] https://www.theguardian.com/global-development/2017/oct/17/the-president-sleeps-with-one-eye-open-mugabe-reshuffles-as-power-games-begin

frenzied speculation about a coup."[94] However, the minister replied that such a move was the responsibility of state security minister Kembo Mohadi.

## Current Threats

*Public Order and State Security Laws*

Zimbabwe has had a tenuous and tense relationship with new technologies, leading them since at least the 1990's to implement a raft of laws and regulations based on public order and state security and abuse of the judicial processes meant to restrict free speech and independent media.[95]

*Strict Media Regulation*

Between 1995 and 1998, the government barred the first mobile service provider, Econet Wireless, from operating in the country, until a 5-year legal battle ultimately led to the lifting of the unconstitutional ban and is again restricting its subsidiary, Kwese TV in an ongoing court battle.[96]

*Suppressing Encryption*

The government's technophobia[97] can be traced back to 2012 when opposition activists were charged with treason for privately watching Arab Spring videos.[98] In 2013 government realised its vulnerability when it failed to deal with encryption and anonymity technologies when a form of 'WikiLeaks' under the Facebook handle Baba Jukwa[99] followed by over 100,000 people took hold in Zimbabwe exposing state corruption. These developments occurred despite the current legal prohibition on encryption, for instance, the Blackberry Messenger had long been banned in the country.

This prompted the government to treat the internet as a serious challenge to 'national security' thus leading to the army and security sector involvement in cyberspace governance-securitisation of cyberspace.

[94] https://uk.news.yahoo.com/special-report-treacherous-shenanigans-inside-story-mugabes-downfall-094026170.html
[95] https://www.academia.edu/31116879/Analysis_of_Internet_Censorship_in_Zimbabwe.doc
[96] https://www.newsday.co.zw/2017/09/baz-appeals-kwese-tv-licencing/
[97] http://www.thezimbabwean.co/2015/12/technophobic-officials-in-govt/
[98] http://www.telegraph.co.uk/news/worldnews/africaandindianocean/zimbabwe/9153948/Six-Zimbabweans-arrested-for-watching-Arab-Spring-video.html
[99] http://www.newzimbabwe.com/opinion-17488-A+closer+legal+look+at+Baba+Jukwa+case/opinion.aspx

*Anti-Social media stance*

In July 2016, a local pastor Evan Mawarire set up an online page called #ThisFlag movement through which he used social media to organize a stay-at-home demonstration[100], the biggest anti-government protest in a decade.

Ever since,the government has been threatening to regulate social media through its Ministry of Information Technologies[101] and to deal with those who post messages that cause economic alarm and despondency[102] as well as to view social media as a national threat.[103]

*Self-Censorship*

Overall, the criminalization of free speech in Zimbabwe has led to a toxic environment of self-censorship[104] and has put undue pressure on internet providers to monitor and intercept critical content on both social media applications and via private email accounts.

*Biometrics and Elections*

The government relied on computer technologies to deny Zimbabweans and the opposition Movement For Democratic Change access to the electronic voters' roll in 2013[105] leading to an election that was neither verifiable nor produced evidence to convince the losing candidate that he lost fair and square as well as giving him an opportunity to challenge the result in court.

**Emerging Threats**

*Repressing civic movements online*

Momentum towards a more concerted crackdown on free speech in Zimbabwe has been building for some time. In 2016, the country's telecom authority issued[106] a "public warning" on the "gross irresponsible use of social media and telecommunication services" at a time

[100] https://www.reuters.com/article/us-zimbabwe-politics/zimbabwes-mugabe-creates-cyber-ministry-in-cabinet-reshuffle-idUSKBN1CE28U?il=0
[101] https://www.techzim.co.zw/2016/07/minister-ict-says-zimbabwean-government-will-consult-citizens-need-regulate-social-media-arises/
[102] https://www.dailynews.co.zw/articles/2017/09/26/mugabe-s-govt-presses-panic-button
[103] https://www.reuters.com/article/us-zimbabwe-politics/zimbabwes-mugabe-creates-cyber-ministry-in-cabinet-reshuffle-idUSKBN1CE28U?il=0
[104] https://freedomhouse.org/report/freedom-press/2017/zimbabwe
[105] https://www.newsday.co.zw/2017/06/zec-refuses-release-2013-voters-roll/
[106] https://bulawayo24.com/index-id-news-sc-national-byo-91782.html

when new citizen-led civic movements[107] were attracting international attention and gaining resonance with Zimbabweans across the political spectrum. For example, a video in which a pastor vents[108] his frustration with the state of the country went viral last year, triggering a movement known as #ThisFlag in which other Zimbabweans share their exasperation. The pastor now faces[109] subversion charges and a potential twenty-year prison sentence.

*Emulating China, Korea and Russia- Digital Authoritarianism*

It is thus no surprise that leaders in Zimbabwe have unabashedly looked to China[110] and North Korea[111] for "successful" models to emulate.

*Weaponization of the Cyber security Ministry*

On 03 November 2017, Zimbabwean authorities arrested Martha O'Donovan, an American citizen, who works for Magamba TV, during a dawn raid at her Harare residence under a search warrant. They confiscated all her electronic devices including her laptop, reportedly investigating a case of undermining the authority of or insulting the President when she posted a tweet on her profile during the recently held Shoko Festival., The tweet referred to a certain Goblin, whose wife and step sons imported a Rolls Royce vehicle. However, the reported offensive and insulting tweet does not make any mention of the President's name.

**Current Needs**

Awareness and capacity in civil society and Telcos to push back against government-led repression of free online speech and privacy.

**Possible Solutions**

- In order to respond to this trend, digital rights activists and donors should undertake several important steps. First, raise awareness—online and elsewhere—about the latest encroachment on privacy, free speech and political expression in Zimbabwe.
- Secondly, activists need to convince donors to invest in projects that better assess and respond to cyber security threats and other technological challenges to human rights: support cyber security trainings to enhance the capacity of civil society actors to operate in repressive spaces.
- Deployment of tools to navigate around website blocks, connection blackouts and widespread censorship.

[107] https://www.dailymaverick.co.za/article/2016-12-13-2016-african-person-of-the-year-pastor-evan-mawarire/
[108] https://www.theguardian.com/world/2016/may/26/this-flag-zimbabwe-evan-mawarire-accidental-movement-for-change
[109] http://edition.cnn.com/2017/09/25/africa/zimbabwe-pastor-mawarire-jailed/index.html
[110]http://www.sundaynews.co.zw/govt-to-regulate-social-media/
[111] https://www.dailynews.co.zw/articles/2017/10/11/mugabe-explains-functions-of-cyber-security-ministry

- Similarly, encouraging telecoms to push back against government pressure to censor the internet will be crucial; evidence[112] from Lesotho suggests that this strategy can be successful.

## ZAMBIA

### Current Landscape

The parameter of hate speech mostly on online platforms has dominated[113] internet freedom discussions in Zambia. As one Zambian blogger pointed out on Facebook, "Zambians are in the habit of treating every speech as hate speech even when one is simply stating facts."

### Current Trends

*Public Order Laws*

Both administrations of Presidents Sata and Lungu legalised content controls through the enforcement of existing public order, secrecy and morality laws. This includes, for example, anti-pornography, slander and defamation in the online environment in an uneven and partial manner.

*Connectivity*

The country also faced connectivity problems due to poor internet resources infrastructure. Although the country continued to block and filter "offensive" websites during the period under review, the picture changed in the period leading up to and including the 2016 elections.

*Blocking*

Out of a total of 1,303 websites tested for censorship in Zambia during and following its 2016 general election period, only 10 of those sites *presented* signs of DNS, TCP/IP and HTTP interference.[114] Previously blocked news outlets appeared to be accessible throughout the duration of the testing period

No block pages detected as part of this study could confirm cases of censorship. The findings[115] illustrate that connections to the websites of the World Economic Forum, the Organization of American States (OAS), and an online-dating site (pof.com) failed

[112] https://www.opentech.fund/article/new-report-analyzes-internet-censorship-during-lesothos-2017-general-elections
[113] https://www.daily-mail.co.zm/tag/hate-speech/
[114] https://explorer.ooni.torproject.org/country/ZM
[115] https://explorer.ooni.torproject.org/country/ZM

consistently from Zambia's MTN network across the testing period, while failure rates from control vantage points were below 1%, indicating these sites might have been blocked.

Pornography and sites supporting LGBT dating also appeared to be inaccessible throughout the testing period, and such blocking can potentially be legally justified under Zambia's *Penal Code* and Electronic Communications and Transactions Act 2009.[116] However, it remains unclear why connections to other websites, such as Pinterest, may have been tampered with during Zambia's 2016 general elections.

The network tests run in Zambia[117] aimed at identifying "middle boxes" capable of performing internet censorship did not reveal the presence of censorship equipment. However, this does not mean that censorship equipment is not present in the country, just that these particular tests were not able to highlight its presence.

**Emerging Trends**

The results from the technical measurements appear to confirm views from some of our interviewees that the government had realised the futility of mass blockades, but instead chose to resort to a number of third generation controls in the run up to the 2016 presidential elections: First, it created an environment that promoted mass blogging- the intent of such information revolution or campaigns is to effect cognitive change rather than to completely deny access to online information or services. However, the ultimate source of these campaigns is difficult to attribute.[118]

*Access to Information*

Government also delayed the passage of an access to information law, thus creating an environment where it can either allow or deny access to information at whim. In addition, towards the elections, government also used a range of methods, ranging from "responsiveness" on social media and media monitoring, as it valued vertical information flows and/or denial as part of its grand strategy to retain political power. On a positive note, the current and previous governments supported Internet Government Forums, and actively take part in them.

*Criminalisation of legitimate expression, including that of defamation.*

The Zambian government is not consistently taking steps to protect human rights on line. For example, there are specific restrictions on online content, which include criminalisation of legitimate expression, including that of defamation.

[116] http://www.zambialaws.com/Principal-Legislation/electronic-communications-and-transactions-act.html
[117] https://explorer.ooni.torproject.org/country/ZM
[118] https://cipesa.org/2016/07/analysis-of-the-relationship-between-online-information-controls-and-elections-in-zambia/

Such criminalisation contributes to an environment of self-censorship. Second, although the law does not impose intermediary liability on ISPs, Zambia does not have a framework that provides detailed guidance on the issue, thereby leaving the door open for future governments to impose such liability. Third, Zambia, like most African countries, lacks laws that adequately protect the right to privacy, treatment of private data, and facilitation of access to information.

**Possible Solutions**

See Rwanda as both countries have broad similarities.

**SWAZILAND**

**Current and Emerging Threats**

*Deliberate denial of Internet Resources*

Despite being a small, predominantly rural country with a proportionately small population, Swaziland severely lacks proper communication facilities including the internet. The internet facilities are very poor, and the population does not enjoy much internet coverage. Since the internet is not firmly established in Swaziland, there is not a well-developed internet governance framework in the country.

Despite the fact that internet in Swaziland dates back to early 1995, cyber security awareness is a new phenomenon and there is little discourse on it so far, save for such basics as digital security training, which has been carried out.

*Just in time disconnections that assure plausible deniability*
The Swaziland government, mostly through ISPs, disrupts and disconnects network infrastructure for political and partisan reasons. There are recorded cases of *"just on time"* denial of service, especially to disrupt trade union activities that may expose the monarch to international censure.[119]

*Blocking & Filtering*

There have also been incidents of internet blocking and filtering, especially those of the political opposition and trade union.[120]

*Social media controls*

[119] https://www.academia.edu/35088682/Detecting_Just_in_time_cyber_information_controls_applied_in_ways_that_assure_plausible_deniability

[120] https://www.academia.edu/31116896/Internet_Censorship_in_Swaziland_Policy_and_Practice

Further, the Swazi government criminalises and attributes political meaning to online speech. Government officials announced plans to censor any information shared on the internet via social media platforms. If passed, the law will ban Facebook and Twitter users from criticising its autocratic ruler, King Mswati III.

*Subversive speech and Terrorism*

Further, the Swaziland Constitution does not grant absolute rights for freedom of expression. The freedoms are limited by broad interpretations of statutes that restrict expression in the interest of public order and safety, national security, morality, and health. For instance, the Sedition and Subversive Activities Act and the Suppression of Terrorism Act (STA) 2008 are used by officials to suppress freedom of expression on the internet and induce an environment of self-censorship.

The political environment in Swaziland, presided over by an absolute monarch and characterised by culture of deference and fear, contributes to a culture of self-censorship. It is because of this environment that not much is known or written on Swaziland.

**Current Needs and Solutions**

As a small emerging internet market, there is need for continued multi stakeholders' discussions on internet access and connectivity and their importance to development and creating open societies. Also, there is need for discussions on cyber security as its awareness is a new phenomenon and there is little discourse on it so far, save for such basics as digital security training, which has been carried out.

## LESOTHO

**Current Landscape**

The current government, which came into power on 3 June 2017, has not announced its plans on internet policy and social media. However, at a policy level, Lesotho has been slowly working on data protection and cyber security legislative frameworks since 2012. Once operational, the data protection legislation will introduce progressive provisions to protect usage of private data. Similarly, the pending computer crime and electronic transactions bills include progressive provisions, including measures to protect intermediaries within Internet ecosystems from liability for third party content.[121]

[121] https://www.opentech.fund/article/new-report-analyzes-internet-censorship-during-lesothos-2017-general-elections

The universal service fund investment has extended 3G and 4G mobile network reach, which has increased the use of social media and internet-based radio stations, and had a catalytic effect on freedom of expression and the opening up of political space. There is need to mainstream an understanding of human rights in cyber security alongside these infrastructural developments. While the Regulator has often factored human rights considerations into its decision making, other stakeholders, such as law enforcement branches and the government, require further training and political will to apply human rights and the principles that underpin them, such as the need for transparent and inclusive decision making.

## Current Threats

*Threats to Social media*

The Lesotho government maintained a hostile stance towards social media, and attempted to shut it down twice during the election period. It sought to take this measure in response to an increase in the use of social media and online publishing platforms. The Regulator subsequently invited Facebook to meet government officials and the Regulator to explain why it was important to keep social media and indeed the internet open, because as it turned out, the government did not understand what Facebook was, let alone its important role in society.

*Blocking and filtering*

Technical network measurements we carried out during the election period did not reveal clear evidence that the government had successfully blocked website pages. This could be attributed to three main factors. Firstly, Lesotho has very few standalone websites providing local content, and it is difficult for the government to filter or block the more commonly-used websites. Secondly, the government lacked the technical capabilities to shut down the internet or social media.

Finally, the Lesotho Communications Authority resisted a government directive to shut down social media, insisting on due process and the need to respect freedom of expression. Given that the government has previously censored and shut down print and broadcast media, it is highly likely that it would have shut down social media if it had the capacity to do so, and if the regulator had complied with its directive.

## Emerging Threats

*A lack of transparency on Cyberspace Governance*

The previous government's attempt to shut down social media stems from its culture of excessive secrecy, which in turn is motivated by paranoia and the Internet's prospective capabilities.

*Undermining Anonymity & Encryption Standards*

In the case of Lesotho, one of the main concerns for law enforcement is that of people who post anonymously on social media. To deal with this perceived threat, they have proposed to prevent anonymous activities. Nevertheless, whereas law enforcement agencies are averse to social media activities that may undesirably expose their activities, the Regulator has often said 'No' to interference of free communication.

*Cyber & Data Security Posture & Human Rights Implications*

Although Lesotho passed the Data Protection Act in 2013, it has not implemented it since it is still yet to establish the Office of the Data Protection Commissioner. The Act, inter alia, provides for the following statement of objectives:
"Principles for regulation of processing of personal information in order to protect and reconcile the fundamental and competing values of personal information privacy under the proposed Act and sector-specific legislation and other related matters.'

*Intermediary Liability and Freedom of Expression*

On a positive note, the proposed cyber security laws exempt intermediaries from liability under certain circumstances. Part VI of the Computer Crime and Cyber Bill, 2013 leaves room for exoneration from liability on the part of the Access Provider, Hosting Provider, Cacheing Provider, Hyperlinks Provider and Search Engine Provider under specified conditions therein; while Part VII provides for limited liability for acts and omissions committed in good faith and without gross negligence in line with the provisions of the Act.

*Internet Access and Connectivity & Free Flow of Information*
*Universal Service Fund (USF), Base Stations and Internet-based Radios*

In 2016, the Internet was not widely available and almost non-existent in rural areas of Lesotho due to lack of communications infrastructure and high cost of access. According to the International Telecommunication Union, approximately 16 percent of the population had access to the Internet in 2015.

**Possible Solutions**

Despite being a closed society, the Lesotho Regulatory Authority is open to suggestions on how to mainstream human rights in internet governance. An entry point would be training in human rights and cyber security.

The Regulator was aware of some of the critical issues that ought to be considered in the application of the cybercrime law in a manner that respects human rights online.
While the Regulator has a good understanding of cyber security and international safeguards to protect human rights online, such knowledge is lacking in the country's intelligence and law enforcement.

It is also important that in 2012/2013, a representative of the Lesotho Regulator was one of the Respondents in a Comprehensive Study on Cybercrime for the UN Office on Drugs and Crime. This is an indication that Lesotho has access to international best practice.
The Regulator is also a member of both the Internet Society and ITU and, according to the Regulator, "we do take note of best practice and recommendations from these bodies."

## DEMOCRATIC REPUBLIC OF CONGO (DRC)

### Current Landscape

According to a report by Symantec some private entrepreneurs made moderately priced internet access available through internet cafes in large cities throughout the country[122]. Data-enabled mobile telephones were an increasingly popular way to access the internet. According to the International Telecommunication Union, 3.9 percent of individuals in the country used the internet during the year. The Republic of the Congo has a draft "Law on the Fight against Cyber Crime" to govern electronic transactions; protect personal data, and copyright rights. Ministry of the Interior is responsible for cyber security issues while a unit within the National Police investigates cyber-crimes and enforces crime laws.

### Current Issues

*Internet Shutdowns, partial shutdowns, throttling and slow down*

Ahead of anticipated protests on December 19, the government ordered internet providers to prohibit the sharing of video, images, or sound over social media, on penalty of revocation of their operating licenses. Companies were responsible for either isolating and prohibiting this feature or shutting down all related data services. Companies reopened full use of internet features by December 28.[123]

[122] https://www.thegfce.com/documents/publications/2017/03/10/report-cyber-trends-in-africa
[123] https://www.reuters.com/article/us-congo-politics/protests-erupt-in-congo-as-kabilas-mandate-expires-idUSKBN14800C

A senior telecoms official based in Kinshasa reported that On 7 August 2017, the Congolese authorities, again, ordered the slowing down of internet capacity so that it could not be used to transmit images via social media. The move came as opposition grew against President Joseph Kabila, who refused to step down at the expiration of his mandate, with nationwide strikes planned.[124]

*Interception of Communications*

In April 2017, two aid workers were killed in the DRC. The video depicting the slaughter of the aid workers which was shared on WhatsApp by rebels was intercepted by the secret service and sent to the journalists, which raised suspicion that the later were implicit in the killing. It is still not known who killed them but the circumstances around the interception went unexplained.

*Limiting Access to Internet*

Price spikes- Government ordered ISPs to hike the prices as a form of discouraging people from accessing the internet.

.

*Criminalisation of Legitimate Expression in digital spaces*

Despite the fact that the general elections were postponed, ICT tools and digital space is being harnessed for political purposes, for example, the Lucha and Filimbi groups were formed and are being used to spread information on political processes although some of the group members have been allegedly tortured. These groups are in the position to tell about the sort of threats they are facing and what tools government is using to counter their activities.

National authorities report that the hacking of electronic mailboxes and the dissemination of false information on social networks was atop the list of cyber incidents last year. According to a report by Symantec, the officials also pointed out that it was difficult to know whether the perpetrators of the incidents were located within or outside of the country.[125]

**Current Needs**

Internet San Frontières, Access Now and Arthur Gwagwa have done awareness raising on circumvention tools. [126] Also, Rudi International www is leading the efforts in this part of the

[124] https://www.reuters.com/article/us-congo-violence-internet/congo-orders-internet-slowdown-to-restrict-social-media-telecoms-source-idUSKBN1AN2DE

[125] https://www.thegfce.com/documents/publications/2017/03/10/report-cyber-trends-in-africa

[126] https://www.academia.edu/31091240/Keeping_the_Internet_accessible_in_Sudan_South_Sudan_and_the_Democratic_Republic_of_Congo_through_circumvention_tools_in_the_event_of_a_shutdown_An_Open_Technology_Fund_funded_Campaignhttps://www.academia.edu/31091240/Keeping_the_Internet_accessible_in_Sudan_South_Sudan_and_the_Democratic_Republic_of_Congo_through_circumvention_tools_in_the_event_of_a_shutdown_An_Open_Technology_Fund_funded_Campaign

country through different digital security trainings as well as ICT policy trainings for civil Society actors.[127] There is now need to upscale this circumvention work. This work should not be reactionary to political events such as protests but must be done proactively.

Finally, activists should push parliament to pass laws that support citizens' digital rights online.[128]

## WEST AND CENTRAL AFRICA

The Media Foundation For West Africa June 2017 report which monitored internet freedom situation in 2017 up to June in eight target countries - Benin, Côte d'Ivoire, Ghana, Mali, Niger, Nigeria, Togo and The Gambia had the following findings:

- Internet freedom environment is generally unrestrictive with minimal internet-specific laws regulating or repressing online expression. Inadequate infrastructure, high cost of data and poor quality service were also found to be challenges in the landscape. The monitoring also recorded six online expression violations and four other incidents relating to redress, regulation and Facebook blackout.
- None of the countries monitored had specific laws regulating or repressing online expressions and activities except Nigeria which has a cybercrime law that seeks to respond to cyber-security-related activities online. Unavailability of adequate infrastructure for internet access across the countries, cost of data and quality of service were some of the pertinent issues reported from all the countries.
- Also, with the exception of Mali, none of the other countries reported any known mass surveillance, filtering, blocking or shutdown of internet resources or social media in the period under review. In terms of online violations, only two of the countries, Mali and Nigeria, recorded incidents of violations.[129]

## CAMEROON

### Current and emerging threats

**Online censorship** - In January 2017, the dispute in Cameroon over the use of English and French appeared to be deepening. In a bid to curb protests, the government imposed a 93-day blackout in its English-speaking regions amid mounting protests.[130] The protests began in October 2016 as strikes by lawyers and teachers. The lawyers complained that the influence

[127] https://rudiinternational.org/
[128] https://cipesa.org/2017/06/dr-congo-parliament-urged-to-pass-laws-that-support-citizens-rights-online/
[129] Access full report on https://www.ifex.org/africa/2017/11/02/peace-through-pluralism/
[130]https://qz.com/964927/caemroons-internet-shutdown-is-over-after-93-days/

of the French language was overbearing and wondered why French-speaking judges who do not understand English have been transferred to English-speaking regions.

In September 2017, the minister said they would not shut down the internet for the second time.

However by 1 November, a whole month later, people in the English-speaking regions of Cameroon were still being deliberately cut off from major internet messaging platforms.[131] They were struggling to share news, go to school, provide professional development, or just stay in touch with the people they love. As tensions rose, the discriminatory blackout created a blanket of impunity for police violence against protesters. Reports say that at least 17 persons died during the October 1, 2017 unification celebrations in NW and SW.[132]

In addition, anti-terrorism, fake news and hate speech laws are used to stifle free expression online, and through ICT tools: 3 men were sentenced to jail for sharing a joke on Boko Haram via SMS.[133] They were judged by a military tribunal, on the basis of the anti-terrorism law adopted in 2014. In January 2017, amidst Internet shutdown, millions of mobile phone users received a state sponsored SMS reminding them that the sharing of fake news online could bring them to jail.[134]

Surveillance - In April 2017, after Internet was restored in the NW and SW regions, the Minister of Post and Telecoms warned that the government was implementing sophisticated online surveillance methods.[135]

**Current Needs and Possible Solutions**

Please see the 'Current Needs' and 'Possible Solutions' under the Broad overview on page 2 of this report.

## GABON

**Current and emerging threats**

**Online censorship** - Gabon is a country located in Central Africa, neighbouring Cameroon. The country faces a serious political crisis since August 2016, when the opposition accused the presidential party of rigging the presidential elections. The government imposed a one week long total Internet blackout, before resorting to an

[131] http://www.dw.com/en/internet-blacked-out-for-english-speaking-minority-in-cameroon/a-37271549
[132] https://qz.com/1092006/cameroon-anglophone-crisis-police-kill-15-southern-cameroons-independence-protestors/
[133] https://apnews.com/f82661728798477da0b012aea203f0be/3-cameroon-men-jailed-10-years-over-boko-haram-joke
[134] https://internetwithoutborders.org/fr/regional-internet-blackout-in-cameroon/
[135] https://internetwithoutborders.org/fr/internet-back-in-anglophone-cameroon-but-more-surveillance/

"internet curfew[136]", and blocking of social media websites. Recent reports suggest that throttling is used at times of protests: this throttling is often explained by the Government as related to physical or technical issues on submarine cables.

**Cybercrime and National security as justifications to fight against online political rights** - During the August 2016 presidential election, democracy and human rights defenders, who had put in place election monitoring platforms, were arrested over cybercrime charges: they were accused of hacking election data, for putting in place a citizen monitoring platform to crowd source election results data, and ensure their integrity

Surveillance - In 2016, reports emerged[137] on a contract signed by the Government with Italian firm Hacking Team[138], which specializes in "Hacking Suit for governmental interception".

**Current needs**

Gabon has a very dynamic civil society, especially in its diaspora. They need capacity building on circumvention/anonymity tools.

There needs to be more research on the state of surveillance in the country: what company sells what tools to the Government.

**Possible solutions**

Training of civil society (circumvention, network measurement, anonymity) and more research on censorship and surveillance in the country.

## MALI

**Current and emerging threats**

**Internet shutdowns** - Although Mali is perceived as a democracy, the Government, in 2016 and 2017 used censorship methods observed in less democratic countries: in August 2016, Facebook and Twitter were blocked amid protests in the country[139]. In June 2017, the Government throttled and then blocked access[140] to these same social media

[136] https://qz.com/781752/gabon-has-been-imposing-a-12-hour-a-day-internet-curfew-as-its-political-crisis-grows/
[137] https://internetwithoutborders.org/fr/government-in-gabon-threatens-to-shutdown-the-internet/
[138] http://www.hackingteam.it/
[139]https://internetwithoutborders.org/fr/internet-sans-frontieres-calls-on-the-government-of-mali-to-keep-the-internet-on/
[140] https://internetwithoutborders.org/fr/internet-sans-frontieres-calls-on-the-government-of-mali-to-keep-the-internet-on/

platforms: the country was witnessing waves of protests against a proposed constitutional reform.

### Current needs

Civil society is very dynamic in Mali, and has an incredible capacity to organize rapidly to respond to all attacks against digital rights through campaign. Network measurements are needed to document and explain the censorship events, which are likely to continue in the upcoming months and years.

### Possible solutions

Enlarge the community of OONI testers in the country. Engage with the Government of Mali on the importance of Internet freedoms in its efforts to develop a digital economy in the country.

## NIGERIA

### Current and Emerging Threats

*Blurred boundary between hate speech and acts of terrorism*

The federal government has been mooting a bill that would see hate speech including online classified as acts of terrorism. In 2016, the Acting President Yemi Osinbajo declared that henceforth those found to be promoting hate speech would be treated as terrorists.

> "The Federal Government has today drawn the line on hate speech. Hate speech is a species of terrorism. Terrorism as it is defined popularly is the unlawful use of violence or intimidation against individuals or groups especially for political ends." [141]

*Facilitation of Terrorism*

An amendment[142] to The Nigerian Terrorism Act passed second reading as at Nov. 2016. Section 5(2) creates an offence of incitement to commit terrorism through the internet and other electronic means. Section 3 of the bill sets a lower standard of proof as it is not necessary to prove that the suspect actually collected the information to facilitate terrorism.

[141] https://www.academia.edu/34339122/Africa_Hate_and_Incitement_Speech_Policy_Brief_2017.pdf
[142] http://placng.org/wp/2016/11/bills-to-amend-terrorism-act-2011-and-2013-passes-second-reading-in-the-house/

While Nigeria has genuinely suffered acts of terrorism from the Boko Haram, for example, labelling hate speech as an act of terrorism, particularly given the weak due process provisions under section 3 is worrisome. Although there has been no progress on the proposed laws, critics believe these mostly directed on the problems being caused by secessionists from the Eastern parts Nigeria.

During the debates on hate speech in Nigeria, Arthur Gwagwa provided guidance on international standards on hate and incitement speech.[143]

*Blocking & Filtering*

There are emerging reports[144] that an agency of the Federal Government of Nigeria, the Nigeria Communications Commission, is taking steps to block the domain names of several identified websites allegedly threatening national security in Nigeria. Paradigm Initiative, a Nigerian based pan African Internet rights organisation issued press release[145] on the situation and published a report on recent censorship events[146] in Nigeria with a list of 21 URLs which are reportedly blocked in Nigeria.[147] These URLs include a popular Nigerian news outlet, as well as multiple sites run by the indigenous people of Biafra (who seek independence from Nigeria).

*Surveillance (Transparency and Accountability in cyberspace governance)*

According to Paradigm Initiative[148], the Ministry of Science and Technology proposed to or has launched two new satellites by the National Space Research and Development Agency (NASDRA) which the Ministry supervises. They had information that these satellites have snooping capabilities which clearly infringes on the constitutionally guaranteed rights of Nigerians to privacy.

Questions arose on the secrecy and a lack of transparency on governance of cyberspace and implications on FOE and privacy which prompted Paradigm Initiative to file a freedom of information request under the Nigerian Freedom of Information Act of 2011 accompanied with a threat for judicial review if the request were turned down.

**Possible Solutions**

Engagement of stakeholders through the NetRights, a pan African coalition of internet rights activists, which was set up by Paradigm Initiative to assess and intervene on internet freedom issues in Sub-Saharan Africa.

[143] https://www.academia.edu/34339122/Africa_Hate_and_Incitement_Speech_Policy_Brief_2017.pdf
[144] http://www.tribuneonlineng.com/fg-clamps-online-newspapers-others/
[145] https://pinigeria.org/foi-eavesdrop-satellite-ng/
[146] https://pinigeria.org/president-buharis-secret-war-on-free-speech/
[147] http://www.itrealms.com.ng/2017/11/leaked-ncc-writes-telco-to-block-21-pro.html
[148] https://pinigeria.org/foi-eavesdrop-satellite-ng/

## THE GAMBIA

### Current Challenges

As a transitional society and nascent democracy, it is too early to tell to what extent the current government has dismantled the old restrictions since a policy shift may take time to implement. Most donor agencies, such as the European Union, are currently evaluating their human rights, governance and democracy work in the country. Internet rights activists should continue monitoring the extent to which the government policy shift is having a positive impact on freedom of expression including online. In doing so, they should locate the internet freedom agenda within the larger democratic project.[149]

### Landscape when there was a power shift in March 2017.

Adama Barrow, current president, defeated Jammeh in a shock election in December 2016 that saw the country tether on the brink of a political turmoil as Jammeh refused to hand over power. According to human rights groups, freedom of expression both offline and online had suffered seriously under Jammeh. Under Jammeh, the internet in The Gambia was one of the most strictly regulated across Sub Saharan Africa. According to the authoritative annual freedom on the internet by global human rights institution, Freedom House, The Gambia was among the most restrictive countries in Africa and worldwide. In 2014, the country was ranked as the second most repressive in Africa, falling few points below Ethiopia, which is considered the worst in Sub-Saharan Africa.

### Legacy Cases of President Jammeh's era requiring monitoring

### Content Controls

One area that requires monitoring is the access to foreign websites as Internet users have previously reported they often could not access the websites of foreign online publications such as Freedom Online. The Africa Market and Telecommunications Report for 2016 reported 18.6 percent of individuals used the internet during the year. In August the government reportedly restricted public access to Voice Over Internet Protocol services, including Skype and other popular social media applications, such as

[149] Comments by Gambian Digital security trainer, Poncelet ILeleji,2017, OTF Summit, November 2017, Valencia, Spain.

Face Time, Facebook video messaging, and WhatsApp. These restrictions did not remain in place at year's end.

## Internet Shutdown

*The Gambia: Internet Shutdown during 2016 Presidential Election*

In December 2016, OONI and CIPIT performed OONI network measurement tests in the Gambia to examine whether websites were blocked during its 2016 presidential election.[150] But merely a few hours after they connected their probe to perform tests, it stopped working completely.

They suspected that this was due to an internet shutdown. To confirm this, they referred to third-party data to examine whether a country-wide internet blackout was taking place.

In this report,[151] they summarized some key findings pertaining to the internet shutdown that appears to have occurred in the Gambia on the eve of its 2016 presidential election.

## Internet access

The Gambia has been expanding on its access to the Internet and other information and communication technologies (ICTs). It launched its first IXP in 2014.[152]

Despite heavily investing in the ICTs sector to leapfrog to a middle income economy by the year 2020, the country has a relatively small online population with only about 20 percent internet penetration. But to date, telecommunications and internet costs in the country remain among the most affordable on the continent.

## Criminalization of Expression

Since 1994, president Jammeh tightened regulations around press freedom and freedom of speech. By the time he was forced out of office in 2017, a staggering number of over 200 journalists had fled the country, mostly running for their lives.

The Information and Communication Act 2009, amended in 2013 at the time of convergence, restricts freedom of speech online. The 2013 amendments introduced severe punishment for the offences of spreading "false news" on the internet, for "caricatures" of government figures or public officials, and for posts deemed "derogatory".

[150] https://github.com/TheTorProject/ooni-probe
[151] https://ooni.torproject.org/post/gambia-internet-shutdown/
[152] http://www.africanbusinesscentral.com/2014/07/18/gambia-launches-first-internet-exchange-point-ixp/

## The Security of Internet Users

On the issue of security, there were several incidents of technical violence against internet users in the country. It is not uncommon that activists are subject to technical attacks either on their computers or user accounts on social media. There is wide suspicion of government listening in on people's telephone conversations, especially journalists, activists and opposition politicians. But the extent of the real capabilities of the authorities to intercept calls remains largely unknown. The country has a mandatory sim card registration system making it difficult for anonymous communications.

## Internet Governance

Information and communications technologies (ICTs) in The Gambia are regulated as public utilities by the Public Utilities Regulatory Authority (PURA) established in 2001.

The ISOC Gambia Chapter launched on 12 May 2012.[153] When Barrow came into power, ISOC has been visiting the Gambia, for example, Dawit Bekele, the Internet Society's Regional Bureau Director for Africa, paid a visit to The Gambia from 17-18 September 2017 to meet the regulator, civil society and government minister responsible for telecommunications.

## Possible Solutions

As pointed above, there is need to support current efforts being driven by OSIWA, Amnesty International, the Open Technology Fund and other partners.

Collaborations and resource coordination are needed to address issues that include: digital security, data protection, online harassment, online surveillance, cyber bullying, hate speech, online child safety, data protection.[154]

# SENEGAL

## Current and Emerging threats

Although Senegal is considered to be one of the most stable and oldest democracies in West Africa, it recently made the headlines among digital rights violators.

[153] https://www.internetsociety.org/blog/2017/10/supporting-internet-development-gambia/

[154] Comments by Gambian Digital security trainer, Poncelet ILeleji,2017, OTF Summit, November 2017, Valencia, Spain.

**Anti-terrorism and Criminalization of online speech** - Like many countries of the Economic Community of West African States (ECOWAS), Senegal has increased its vigilance against potential terrorist attacks; this necessity, given the numerous attacks in neighbouring Mali, raises questions about the potential effects on freedoms.

In its 2016-2017 report on Senegal, Amnesty International refers to the adoption of the Law No. 2016-29 of November 8, 2016, which amends the Criminal Code to include in its Chapter III a vague definition of terrorism. According to this definition, "offenses related to information and communications technology" are treated as acts of terrorism.

Title IV of the Code gives a definition of "ICT-related offenses": the production and delivery of "immoral" content on the Internet is now considered as a misdemeanour.

In June 2016, Senegalese rapper Major Déesse was arrested following a complaint from the Committee for the Defense of moral values: she was accused of having published, on the social network Snapchat, a video in which she allegedly damaged the "moral and religious values" of Senegal. The case was later on dropped.

The image of President Macky Sall is another limit to freedom of expression online: in May 2017, four young people were taken to court, accused of insulting the President of the Republic, for sharing in a group WhatsApp a montage featuring the head of state.

On 3 August 2017, a famous Senegalese singer was arrested, for "insulting the head of state and spreading fake news": she shared a video in a WhatsApp group, in which she criticizes the President. Following her arrest, the prosecutor warned the "bad people who use social networks (...) to broadcast obscene, offensive and even ethnic images".

**Current needs & Possible Solutions**

Civil society groups should work to push legislative reforms and also ensure that anti-terror laws are applied with due regard to the protection of freedom of expression under international law.