Safeguarding Civil Society

Assessing Internet Freedom and the Digital Resilience of Civil Society in **East Africa**

SMALL MEDIA CIPESA DEFEND DEFENDERS CIPIT

SMALL MEDIA

CIPESA

DEFENDDEFENDERS
East and Horn of Africa Human Rights Defenders Project

CIPIT
CENTRE FOR INTELLECTUAL PROPERTY AND INFORMATION TECHNOLOGY LAW

Credits

-

RESEARCH TEAM

James Marchant, Tom Ormson // ***Small Media***
Ashnah Kalemera, Juliet Nanfuka Nakiyini, Wairagala Wakabi // ***CIPESA***
Moses Karanja // ***Strathmore University, CIPIT***
Neil Blazevic, Mark Kiggundu, Donatien Niyongendako // ***DefendDefenders***

Egide Havugiyaremye // ***Burundi Researcher***
[Anonymous] // ***Rwanda Researchers***
John Kaoneka, Maxence Melo, Yahya Poli // ***Tanzania Researchers***
Andrew Gole // ***Uganda Researcher***

We offer special thanks to our teams of committed internet freedom researchers who undertook interviews and collected crucial data for this project, several of whom have chosen to remain anonymous. This research would not have been possible without their hard work and dedication.

DESIGN TEAM

Richard Kahwagi, Surasti Puri // ***Small Media***

Introduction

Over the past decade, East Africa has seen a tremendous boom in connectivity and online participation that is beginning to transform how citizens across the region communicate, express themselves, and establish communities. In a similar manner, the growth of internet access in the region is beginning to empower civil society organisations (CSOs) to engage with the public, share information, and advocate for citizens' rights in sometimes challenging and closed political environments. Although the internet offers opportunities to such advocates, it also offers the possibility for regional, state and non-state actors to interfere with their work, surveil them, and censor their voices.

In partnership with the Collaboration on International ICT Policy for East and Southern Africa (CIPESA), DefendDefenders, and Strathmore University's Centre for Intellectual Property and Information Technology Law, Small Media has sought to map out the state of internet freedom in East Africa, and assess the extent to which ongoing challenges have impacted negatively upon the work of civil society actors in the region.

To measure the state of internet freedom in the region, we have taken the African Declaration of Internet Rights and Freedoms (ADIRF) as our key point of reference. This declaration, drafted and signed by a large array of African civil society organisations in collaboration with international internet freedom organisations, establishes a set of rigorous principles by which governments and other relevant stakeholders must abide in order to guarantee the online rights and freedoms of citizens across Africa.

Although we were not able to map out the state of internet freedom across the entire region in this report, we were able to focus our efforts on some

of the lesser-studied digital landscapes—Burundi, Rwanda, South Sudan, Tanzania and Uganda.

In collaboration with our partners and regional researchers, we devised a three-pronged methodology to comprehensively assess the state of internet freedom in the focus countries, and gauge civil society's ability to protect itself from digital threats. This report is consequently divided into three core segments: a policy and legal analysis; a CSO digital security assessment; and a technical analysis of states' capacities to censor and surveil online content.

Owing to the ongoing civil war in South Sudan, and the incredibly challenging security situation in the country, we were unable to conduct field work to undertake either a CSO digital security assessment, or network measurements and technical analysis. Our analysis of the digital security situation in South Sudan is therefore limited to a policy and legal analysis. Chapter 1 examines the legislative and policy landscape in each of the target countries, and assesses the extent to which government policies align with the principles of the ADIRF. This analysis also takes stock of the ways that regional governments implement these policies in practice, illustrating any instances in which digital freedoms have been violated or threatened.

Chapter 2 explores the results of our CSO digital security assessments based on interviews with local CSOs regarding three key topic areas: the digital threats that CSOs in the region perceive, any training and support networks that already exist, and the tools, practices and knowledge of CSOs to combat the digital threats they face. In total 39 interviews with CSOs from across the region were conducted: 12 in Tanzania, 10 in Uganda, 7 in Rwanda and 10 in Burundi.

Chapter 3 sees us present the results of the network measurements on the extent to which regional governments interfere with online traffic, restrict internet access, and intercept online communications. Measurements employed ICLab's Centinel tool and OONI Probe to gather crucial data about the state of local networks in the focus countries.

Taken together, these three components offer a clear picture of the state of internet freedom in each of the focus countries in this report, and of the challenges CSOs face in navigating this landscape. We hope that this research will prove instructive to regional policy makers to bring their policies into line with the ADIRF, and to the CSOs and digital security providers who will need to work together to protect themselves from the growing threats in the region.

We would like to consider this report to be a starting point for further discussion and research in this field. We highlight a series of challenge areas for regional civil society, and suggest some measures that could be taken to insulate CSOs from the worst of the existing threats. But efforts to advocate for a free and open internet in East Africa will require the continued engagement and participation of civil society, governments, and international organisations. We hope that this report serves as a useful guide to these stakeholders as they work to support internet freedom in the region in the months and years to come.

The African Declaration of Internet Rights and Freedoms

This report takes the 2014 African Declaration of Internet Rights and Freedoms (ADIRF) as its primary frame of reference to assess the state of internet freedom in Burundi, Rwanda, South Sudan, Tanzania and Uganda.

The African Declaration on Internet Rights and Freedoms is a Pan-African initiative to promote human rights standards and principles of openness in internet policy formulation and implementation on the continent. The Declaration is intended to elaborate on the principles which are necessary to uphold human and people's rights on the internet, and to cultivate an environment that can best meet Africa's social and economic development needs and goals.

The Declaration builds on well-established African human rights documents including the African Charter on Human and Peoples' Rights of 1981, the Windhoek Declaration on Promoting an Independent and Pluralistic African Press of 1991, the African Charter on Broadcasting of 2001, the Declaration of Principles on Freedom of Expression in Africa of 2002, and the African Platform on Access to Information Declaration of 2011.

Our mission is for the Declaration to be widely endorsed by all those with a stake in the internet in Africa and to help shape approaches to internet policy-making and governance across the continent.[1]

1 African Declaration on Internet Rights and Freedoms, (2016), 'About', retrieved 02/03/2017, http://africaninternetrights.org/about/

The Principles of the ADIRF

Guiding the ADIRF are a set of principles developed in collaboration between a wide range of African civil society actors, and international organisations working to promote internet freedom and freedom of expression globally. The principles of the Declaration are noted below.

The ADIRF is an incredibly far-ranging and ambitious document, and although we support its objectives we were unable to assess states' compliance with all of the ADIRF's principles within the scope of this research project. As such, we have selected nine principles to form the primary basis for our assessment in this study, though we acknowledge that the other principles should be drawn into any future work attempting to evaluate ADIRF compliance.

1. Openness

The internet should have an open and distributed architecture, and should continue to be based on open standards and application interfaces and guarantee interoperability so as to enable a common exchange of information and knowledge. Opportunities to share ideas and information on the internet are integral to promoting freedom of expression, media pluralism and cultural diversity. Open standards support innovation and competition, and a commitment to network neutrality promotes equal and non-discriminatory access to and exchange of information on the internet.

2. Internet Access and Affordability

Access to the internet should be available and affordable to all persons in Africa without discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. Access to the internet plays a vital role in the full realisation of human development, and facilitates the exercise and enjoyment of a number of human rights and freedoms, including the right to freedom of expression and information, the right to education, the right to assembly and association, the right to full participation in social, cultural and political life and the right to social and economic development.

3. Freedom of Expression

Everyone has the right to hold opinions without interference. Everyone has a right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds through the internet and digital technologies and regardless of frontiers. The exercise of this right should not be subject to any restrictions, except those which are provided by law, pursue a legitimate aim as expressly listed under international human rights law (namely the rights or reputations of others, the protection of national security, or of public order, public health or morals) and are necessary and proportionate in pursuance of a legitimate aim.

4. Right to Information

Everyone has the right to access information on the internet. All information, including scientific and social research, produced with the support of public funds, should be freely available to all, including on the internet.

5. Freedom of Assembly and Association and the Internet

Everyone has the right to use the internet and digital technologies in relation to freedom of assembly and association, including through social networks and platforms. No restrictions on usage of and access to the internet and digital technologies in relation to the right to freedom of assembly and association may be imposed unless the restriction is prescribed by law, pursues a legitimate aim as expressly listed under international human rights law (as specified in Principle 3 of this Declaration) and is necessary and proportionate in pursuance of a legitimate aim.

6. Cultural and Linguistic Diversity

Individuals and communities have the right to use their own language or any language of their choice to create, share and disseminate information and knowledge through the internet. Linguistic and cultural diversity enriches the development of society. Africa's linguistic and cultural diversity, including the presence of all African and minority languages, should be protected, respected and promoted on the internet.

7. Right to Development and Access to Knowledge

Individuals and communities have the right to development, and the internet has a vital role to play in helping to achieve the full realisation of nationally and internationally agreed sustainable development goals. It is a vital tool for giving everyone the means to participate in development processes.

8. Privacy and Personal Data Protection

Everyone has the right to privacy online, including the right to the protection of personal data concerning him or her. Everyone has the right to communicate anonymously on the internet, and to use appropriate technology to ensure secure, private and anonymous communication. The right to privacy on the internet should not be subject to any restrictions, except those that are provided by law, pursue a legitimate aim as expressly listed under international human rights law, (as specified in Article 3 of this Declaration) and are necessary and proportionate in pursuance of a legitimate aim.

9. Security, Stability and Resilience of the Internet

Everyone has the right to benefit from security, stability and resilience of the internet. As a universal global public resource, the internet should be a secure, stable, resilient, reliable and trustworthy network. Different stakeholders should continue to cooperate in order to ensure effectiveness in addressing risks and threats to security and stability of the internet. Unlawful surveillance, monitoring and interception of users' online communications by state or non-state actors fundamentally undermine the security and trustworthiness of the internet.

10. Marginalised Groups and Groups at Risk

The rights of all people, without discrimination of any kind, to use the internet as a vehicle for the exercise and enjoyment of their human rights, and for participation in social and cultural life, should be respected and protected.

11. Right to Due Process

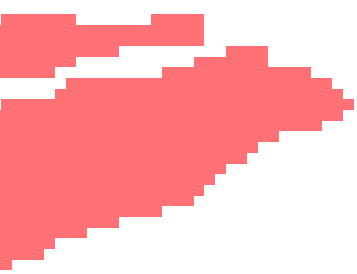
Everyone has the right to due process in relation to any legal claims or violations of the law regarding the internet. Standards of liability, including defences in civil or criminal cases, should take into account the overall public interest in protecting both the expression and the forum in which it is made; for example, the fact that the internet operates as a sphere for public expression and dialogue.

12. Democratic Multistakeholder Internet Governance

Everyone has the right to participate in the governance of the internet. The internet should be governed in such a way as to uphold and expand human rights to the fullest extent possible. The internet governance framework must be open, inclusive, accountable, transparent and collaborative.

13. Gender Equality

To help ensure the elimination of all forms of discrimination on the basis of gender, women and men should have equal access to learn about, define, access, use and shape the internet. Efforts to increase access should therefore recognise and redress existing gender inequalities, including women's underrepresentation in decision-making roles, especially in internet governance.



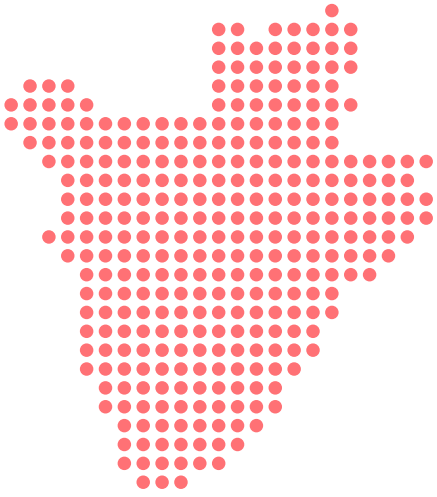
Regional Policy and the African Declaration

In this chapter we will assess the state of internet freedom across East Africa by undertaking an analysis of the levels of compliance between the legislation and policy implementation of regional governments, and the ADIRF. In doing so, this report exposes a number of areas in which governments should be pressed to adapt their existing regulatory and legislative frameworks to ensure that they are more conducive to the protection of citizens' online rights.

The ADIRF offers a clear roadmap for African governments to adhere to in order to enable their citizens to develop and participate in online communities, and to equip them with the necessary tools to engage with wider civil society discourses around development, human rights, and political freedoms. It is our hope that this analysis will help civil society advocates and internet freedom champions to hold regional governments to account, and press them to align their policies with the principles of the ADIRF. In doing so, they will empower civil society, support free expression, and pave the way for greater public participation in digital society across the region.

Burundi

Criticism of the government is not taken lightly in Burundi. Although the country has introduced a number of protections for freedom of speech and the right to privacy, in reality they do not prevent violations taking place. Ambiguously worded laws provide opportunities for governmental bodies to systematically restrict internet freedom in the country. This is evidenced by the temporary blocking of social media networks and the arrests of social media users that have taken place.



1. Openness

The *Autorité de Régulation et de Contrôle des Télécommunications* (ARCT) is the national telecommunications regulatory authority in Burundi. Established under Law No 100/182 of September 30, 1997, ARCT issues operator licenses under a technology neutral regime. There are 11 licensed Internet Service Providers (ISPs) and four mobile phone operators, with the state-owned Onatel also offering fixed line services. Burundi has 30 licensed radio stations and three TV stations, with the public broadcaster National Radio and Television Burundi being the only one with a nation-wide reach. Burundi does not have guidelines on network neutrality.

2. Internet Access and Affordability

Mobile phone penetration stood at 48% as of June 2016, but internet penetration remained low, at 8.2% of the population.[2] The average daily cost of 1GB mobile internet across operators is Burundian Francs (BIF) 1,000 (US$ 0.60). According to the regulator, costs of voice calls on the same network vary from BIF 96 (US$0.06) to BIF 168 (US$0.10) per minute while off-net calls range from 150 BIF (US$0.09) to 210 BIF (US$ 0.12) per minute. Burundi does not have a Universal Service Fund but provisions within the National ICT Policy Plan for 2010-2025 call for ensuring rural connectivity.[3]

BurundiX, the local Internet Exchange Point (IXP), was officially launched in March 21, 2014.[4] The project whose technical infrastructure is hosted at the University of Burundi brings together all the ISPs operating in Burundi and the Government of Burundi through SETIC (*Secrétariat Exécutif des Technologies de l'Information et de la Communication*) and is expected to result in faster and cheaper local internet speeds.

3. Freedom of Expression

Burundi's constitution guarantees freedom of expression, freedom of religion, thought, conscience and opinion under Article 31. The Law No. 1/15 of 9 May 2015 regulating the Burundi Press applies to all forms of communication online and offline, public and private. Article 1 of the law states: "The provisions of this Law shall apply to all modes of communication, audiovisual, cinematographic, written, on the internet and to all media both in the public and private domain". Although the 2015 law's broad definition of a journalist as anyone in the practice of journalism conforms to international standards of the freedom of expression[5], its conditions for practising do not. Article 5 requires that journalists have at least a diploma qualification or at least two years of work experience in a press organisation, work as a journalist as their

---

2 ARCT, (2016), 'Analysis of the ICT Sector in Burundi', retrieved 02/03/2017, http://www.arct.gov.bi/images/statistique/anasetic1.pdf

3 See Politique Nationale De Developpement Des Technologies De L'information Et De La Communication Du Burundi (2010-2025), (2010), retrieved 02/03/2017, http://www.burundiconference.gov.bi/IMG/pdf/Politique_Sectorielle_TIC-3.pdf

4 Internet Society, (2014), 'Internet Exchange Point Launched on 21 March 2014 in Bujumbura, Burundi', retrieved 02/03/2017, http://www.internetsociety.org/news/internet-exchange-point-launched-21-march-2014-bujumbura-burundi

5 CIPESA, (2015), 'East African Court Declares Sections of Burundi's Media Law 'Undemocratic'', retrieved 02/03/2017, http://cipesa.org/2015/05/east-african-court-declares-sections-of-burundis-media-law-undemocratic/

main regular and remunerated activity, and obtain a valid press card from the National Communications Council (CNC). The protection of sources is guaranteed under Article 16. Press organisations must submit annual narrative and financial reports to the CNC (Article 22). Moreover, address details of the director of a newspaper, the publishing house, and website host are required upon first publication (Article 26).

The law gives the CNC powers to issue warnings to media houses or journalists that break the law, with failure to comply with three warnings from the commission leading to possible suspension of the media or withdrawal of accreditation. The director of the publication, the editor and responsible journalist may also be prosecuted. Fines range from BIF 4,000,000 to BIF 8,000,000 (US$ 2,400 to US$ 4,800). The right to reply and to make corrections is provided for (Articles 48-55).

The 2015 law is an amendment of the 2013 law, which had prescribed punishments including high fines, the suspension of media outlets, and the withdrawal of press cards for several broadly worded offenses, such as publishing or broadcasting stories that undermine national unity and public order, or that are related to national defense, security, public safety, unauthorised demonstrations and the economy. The previous law had also limited the protection of journalistic sources, and increased the enforcement powers of the CNC, which is widely considered to be controlled by the president. These articles were removed from the law following rulings on appeals by the Burundi Union of Journalists (BUJ) at the local constitutional court and the East African Court of Justice (EACJ), which found them detrimental to press freedom.

The journalists' union also contested the requirement for online publications and news agencies to disclose to the CNC or the public prosecutor's office information including: the first edition of the publication, the name, nationality and full address and criminal record of the Director of the publication, the full address of the web host, the languages of publication and the constitution of the web publisher. In their judgement, the EACJ judges, however, did not refer to this article and to several others which the petitioners said provided "an unduly onerous and restrictive framework for the regulation of the print and web media."[6]

The EACJ found the provision obligating journalists to reveal their sources in situations where the information related to "state security, public order, defence secrets, and the moral and physical integrity of one or more persons" (Article 20) to be in violation of the EAC Treaty.

Burundi's Penal Code restricts freedom of expression by prohibiting the use of words, gestures and threats against public officers in the course of their duties (Article 378), which are injurious to their character, defamatory and will lessen their dignity or the respect which should be accorded to them.[7]

---

6 CIPESA, (2015), 'East African Court Declares Sections of Burundi's Media Law 'Undemocratic'', retrieved 02/03/2017, http://cipesa.org/2015/05/east-african-court-declares-sections-of-burundis-media-law-undemocratic/

7 The penalty of which is either six months to five years imprisonment or a fine of BIF 10,000 to 50,000 or both.

The ARCT ordered telecom operators to block mobile access to social media applications including Twitter, Facebook, WhatsApp, Viber and Tango beginning on April 27, 2015 in order to stifle opposition protests.[8] Many users were able to access these services, however, using virtual private networks (VPNs) until the blockage was lifted two weeks later on May 13.

In May 2013, the ARCT ordered the publishers Iwacu to suspend comments on their online news site www.iwacu-burundi.org for 30 days for being a "threat to national security".[9] The authority did not specify the particular readers' comments it deemed a threat to national security. Nonetheless, the Iwacu publishers complied and not only shut down the comments section, but the entire website, for a month.

Security agencies and militia affiliated to the ruling party have also been complicit in freedom of expression violations. During the protests against President Pierre Nkurunziza's decision to run for a third term in office, which he then won in a disputed election in July 2015, security forces violently suppressed the protests and the premises of various independent media outlets were raided by security forces and civilian supporters of the embattled president.[10] This forced Radio Publique Africaine, Radio Television Rema, Radio Isanganiro, Radio Bonesha FM, and Radio Television Renaissance to close. This deprived citizens of a key source of information especially since radio is the primary source of information for most Burundians.

Meanwhile, during 2010-2011, Jean Claude Kavumbagu, the editor of the online newspaper Net Press was detained for 10 months on charges of treason and defamation under the 2003 Press Law. The charges were the result of an article that criticised the ability of Burundi's security forces to defend the country against terrorist attacks. Throughout his detention and trial, the Net Press website and article in question remained accessible. Prior to 2010, Kavumbagu had been arrested and imprisoned five times over content published on his online newspaper.[11]

As a result of the harsh media environment in the country, journalists and civil society members working in Burundi and abroad began operating online news outlets, disseminating news via text-message services, Twitter, Facebook, and SoundCloud. Examples include Humura and Inzamba online media.[12]

---

8 Freedman, Myles, (2016), 'Burundi: Access Urges Action on Burundi's Internet Shut Down', *Extensia*, retrieved 02/03/2017, http://extensia-ltd.com/burundi-access-urges-action-on-burundis-internet-shut-down/

9 Reporters Without Borders, (2013), 'Burundi - Media regulator suspends comments on press group's website', retrieved 02/03/2017, www.trust.org/item/20130531164503-qium7/?source%20=%20hppartner

10 Havyarimana, Moses, (2015), 'Gun clashes rage on in Burundi as radio station attacked', *The Nation*, retrieved 02/03/2017, http://www.nation.co.ke/news/africa/Burundi-president-in-secret-location-in-Dar-es-Salaam/1066-2716134-83dj9j/index.html

11 Kavumbagu, Jean-Claude, (2016), 'Jean-Claude Kavumbagu', *PEN*, retrieved 02/03/2017, https://pen.org/advocacy-case/jean-claude-kavumbagu/

12 Anderson, Liam (2016), 'Burundi's Independent Media Aren't Going Down Without a Fight', *Global Voices,* retrieved 02/03/2017, https://globalvoices.org/2016/02/16/burundis-independent-media-arent-going-down-without-a-fight/ and CIPESA, (2016), 'State of Internet Freedom in Burundi Report, 2016', retrieved 02/03/2017, http://cipesa.org/?wpfb_dl=230

However, with the country's low internet penetration, the reach of these services is limited.

Social media users have not been spared either. In August 2016, 56 members of a WhatsApp group were arrested in the capital Bujumbura for allegedly spreading defamatory and abusive statements on the messaging service.[13] The majority of the suspects (46) were released but eight remained in prison over charges of slander and defamation of public officials and institutions.[14]

4. Right to Information

Burundi does not have a freedom of information law and the right is not explicitly defined in the constitution. Journalists face difficulties in obtaining access to official state documents and information. In ordering the blockage of social media in 2015 as detailed above and issuance of a notice against SMS transmissions (see section on privacy and data protection below), the government of Burundi has restricted the sharing of information and ideas over the internet.

5. Freedom of Assembly and Association and the Internet

Freedom of assembly and of association, and the right to found associations or organisations in accordance with the law is provided for under Article 32 of the Constitution. The article does not specifically state that the provisions apply on the internet.

Through arrests of WhatsApp users and the blocking of content on news websites, Burundi is failing to adhere to the freedoms that are set out in the Constitution.

6. Cultural and Linguistic Diversity

// Limited data available.

7. Right to Development and Access to Knowledge

// Limited data available.

8. Privacy and Personal Data Protection

Article 28 of Burundi's constitution provides for the right to respect for private life and personal communications. However, Article 43 of the constitution provides for lawful limits to individuals' privacy in accordance with the law. While there is no solitary data protection law in Burundi, there are data protection and privacy provisions in several legislations:

Law No. 1/10 of April 3, 2013 on the reform of the Code of Criminal Procedure provides conditions under which personal communication can be lawfully accessed. It states that the Public Prosecutor has the right to seize telegrams,

---

13 RFI, (2016), 'Burundi: arrestation des membres d'un groupe de discussion WhatsApp', retrieved 02/03/2017, http://www.rfi.fr/afrique/20160824-burundi-arrestation-groupe-WhatsApp-communication

14 LIGUE-ITEKA, (2016) 'Quarterly bulletin of the Burundian League of Human Rights, July-September 2016', retrieved 02/03/2017, http://www.ligue-iteka.bi/images/Bulletin/Bulletintrimestriel.pdf

letters and objects of any kind, if they appear to be essential to establishing the truth during a criminal investigation. The vague and broad language of "objects of any kind" presents problems for the protection of privacy and also suggests that online communications fall within this scope.

Article 23 of Law No. 1/011 of 1997 on Telecommunications obliges communications service providers and their staff members to protect the privacy of subscribed users (confidentiality of communications exchanges through their networks). Article 40 prescribes penalties as per the penal code for staff of telecom service providers who violate the confidentiality of communications.

Article 248 of the Penal Code prescribes a fine between BIF 50,000 and BIF 200,000 (US$ 30 to US$ 120), and a maximum of six months imprisonment for an individual who unlawfully opens or destroys a letter.

Article 6 of Law No 100/112 of April 5, 2012 (which reorganised the functioning of ARCT) also provides that service providers protect end users. It obliges ARCT to protect and promote communication users' rights.

However, Article 24 of the 1997 Law on Telecommunications provides that a service provider may be required to provide confidential information on demand if that demand is lawful according to the mandate of ARCT.

Since September 2011, Burundi has registered subscribers of mobile phone operators and ISPs, with personal information including the names and addresses of users being collected, purportedly as a means to enhance national security. The spokesperson of the First Vice President reported that operators are now able to contribute to national security by collecting and storing the identities of their subscribers.[15]

Meanwhile, a March 2016 Ministerial Law[16] which is aimed at combating fraud prohibits the possession of two SIM cards from one telecom operator. Authorisation is required from the ARCT for any user requiring two SIM cards from an operator. Article 3 of the Law obliges mobile operators to verify that subscribers use the exact SIM card they registered. Further, Article 3 obliges mobile operators to "take all the necessary measures" to verify if SIM card users are the "real subscribers" and if they detect an anomaly, to block the SIM card. Failure to comply with this article may result in the operator facing a fine of five million Burundi Francs (US$ 2,967).

Earlier on January 7, 2014, ARCT issued a notice warning the public against the transmission of SMS and anonymous calls that could fuel tensions. The notice came at a time opposition leaders were mobilising, including via SMS, for mass protests against proposed constitutional amendments that, among others, would revise presidential term limits to allow Nkurunziza to run for a third term. The communications regulator stated that it would

15 Presidential Office, (2011), 'Le Premier Vice-Président de la République rencontre les opérateurs de la téléphonie mobile', retrieved 02/03/2017, http://www.presidence.bi/spip.php?article1928

16 ARCT (2016), 'Ordonnance No. 540/356', retrieved 02/03/2017, http://www.arct.gov.bi/images/image0008.pdf

work with service providers "on cooperation mechanisms in the traceability" of communications and reminded all operators to fulfil their subscriber registration obligations. The opposition called off the protests for unclear reasons. There were no reported incidents in relation to the regulator's notice.

9. Security, Stability and Resilience of the Internet

Burundi's existing laws are silent on encryption, both in terms of its promotion for confidentiality and security of information and banning the use of encryption software.

10. Marginalised Groups and Groups at Risk

Although existing Burundian legislation does not explicitly limit the free expression of LGBTI people online, the Burundian state has criminalised homosexuality since 2009. Harassment and persecution of the community has been on the rise in recent years, and many LGBTI Burundians have been forced into exile.[17] In such a context, protections for LGBTI Burundians online are non-existent.

11. Right to Due Process

The CNC's decisions with regard to the regulation of the media are enforceable before any appeal to the Administrative Court. The government's orders to block websites and social media pages have not been challenged, either in the media, or in court.

12. Democratic Multistakeholder Internet Governance

// Limited data available.

13. Gender Equality

// Limited data available.

17Kushner, Jacob, (2016), 'Young, Gay, and on the Run in East Africa', *Take Part*, retrieved 07/03/2017, http://www.takepart.com/feature/2016/08/12/lgbt-refugees-east-africa

Rwanda

Rwanda's media ecology remains tightly regulated by the state, with journalists and media organisations required to operate under a strict accreditation system. The laws that define this challenging media landscape—ostensibly introduced to manage the enduring societal tensions underlying the 1994 genocide—have been deployed against online media sources, including blogs and social media users. Extrajudicial attacks have additionally taken place on a number of occasions.

1. Openness

The framework for licensing of operators in Rwanda is technology and service neutral. Rwanda's Utilities Regulatory Authority (RURA) licenses telecommunications and broadcast operators under four categories: Network Infrastructure; Network Services; application services; and content services. There are four telecommunications (fixed and mobile) operators, nine Internet Service Providers, 11 licensed Free to Air television stations, three licensed pay TV stations, 32 radio stations, 54 newspapers and 34 online operators as of September 2016.

2. Internet Access and Affordability

As of December 2016, there were 8.9 million mobile phone subscribers which represents a penetration rate of 78%. Internet users are an estimated 3.6 million.

Rwanda's Universal Service Fund is subsidised by up to a 2% levy on operators' turnover. Managed by RURA, the fund supports ICT literacy and establishment of centres to provide affordable access to rural communities. In October 2015, Rwanda launched its ICT Master Plan – Vision 2020 – which has prioritised improved access especially via mobile. The Rwanda internet Exchange (RINEX) facilitates faster and cheaper local internet traffic. Currently, six of the eleven local ISPs have opted to peer through the RINEX.[18]

3. Freedom of Expression

The Constitution of Rwanda, 2003 (amended 2015) guarantees that all citizens have the right to freedom of expression and freedom of the press (Article 38). The freedoms, however, must not "prejudice public order and good morals, the protection of youth and children, right of every citizen to honour and dignity and the protection of personal and family life."

Law No. 2 of 2013 on Regulating Media (Media Law)[19] provides some safeguards for freedom of the press but contains a lot of provisions which pose a threat to journalists and the independence of the media, including online media. Article 19 of the law provides that every person has the right to receive, disseminate or send information over the internet and the right to create a website through which he/she may disseminate information without needing to be a professional journalist.

The state, however, controls the media by requiring authorisation for media companies to be set up. Journalists are also required to obtain accreditation in order to practice journalism, which appears to be an unfounded restriction on freedom of expression.

Section 166 of the Penal Code Act of Rwanda criminalises speech made in public places, where such speech incites the public against established powers, or incites citizens against each other. Persons convicted under this

18 Rwanda Internet Exchange, (2015), retrieved 02/03/2017, http://rinex.org.rw

19 Official Gazette, (2013), 'Law determining the responsibilities, organisation, and functioning of the Media High Council', retrieved 02/03/2017, http://www.mhc.gov.rw/fileadmin/templates/PdfDocuments/Laws/Official_Gazette_n__10_of_11_March_2013.pdf

section are liable to imprisonment (two to ten years) and a fine of 2000 to 100,000 Rwanda Francs (US$ 2 to US$ 121) or one of these penalties.

Article 8 of the Electronic Messages, Electronic Signatures and Electronic Transactions Law No. 18 of 2010 protects the liability of intermediaries and service providers for the content transmitted through their networks, thereby promoting the internet as a freedom of expression and media platform. They are, however, required to take down content when handed a takedown notice, and there are no avenues for appeal.

Under media laws and laws on promoting genocide, several websites, mostly critical online newspapers and websites of opposition groups, are blocked in Rwanda. In 2010, the government banned the newspapers *Umuseso* and *Umuvugizi*, citing "violation of the media law and inciting public disorder."[20] Online news site *Umusingi* was blocked in 2011. Online news site *Inyereri* is also reported to have been blocked over several years.[21] In late 2014 the government added the BBC website to the list of websites blocked in Rwanda as part of its crackdown on those broadcasting the documentary, *Rwanda, The Untold Story*. The programme reported on allegations that the number of Hutus who died during the 1994 Rwanda genocide was much higher than officially recognised.[22]

In May 2015, various additional independent news outlets and opposition blogs were reported to have been blocked for some time including Veritas Info, The Rwandan, and Leprophete.[23][24] The editors of some were also charged in court over publishing material considered defamatory,[25] endangering national security or genocide denial.[26] Many got sentenced while some fled into exile. In the cases which have been adjudicated publically, the blockage of the websites was ordered by court of the press ombudsman.[27]

But not all blockages or other attacks on critical websites have been issued through transparent, legal, or known processes. For example, John Williams Ntwali, the owner of www.ireme.net and www.ireme.org, one of the few

---

20 Kigaliwire, (2010), 'Umuseso and Umuvugizi newspapers hit with 6 month ban', retrieved 02/03/2017, http://kigaliwire.com/2010/04/14/umuseso-and-umuvugizi-newspapers-hit-with-6-month-ban

21 CIPESA, (2014), 'State of Internet Freedom in Rwanda, 2014', retrieved 02/03/2017, http://www.cipesa.org/?wpfb_dl=179

22 RSF, (2014), 'State of the Media in Rwanda', retrieved 02/03/2017, https://rsf.org/sites/default/files/6_5_2015_ib_-_final_report_on_state_of_the_media_freedom_in_rwanda_00.00.pdf

23 Article 19, (2015), 'Rwanda Journalist Found Guilty on Defamation Charges', retrieved 02/03/2017, https://www.article19.org/resources.php/resource/37871/en/rwanda:-journalist-found-guilty-on-defamation-charges

24 Freedom House, (2015), Freedom on Net Rwanda, retrieved 02/03/2017, https://freedomhouse.org/report/freedom-net/2015/rwanda

25 Article 19, (2015), 'Rwanda Journalist Found Guilty on Defamation Charges', retrieved 02/03/2017, https://www.article19.org/resources.php/resource/37871/en/rwanda:-journalist-found-guilty-on-defamation-charges

26 CPJ, (2012), 'Jailed Rwandan Editors Turn to African Commission', retrieved 02/03/2017, https://cpj.org/blog/2012/12/jailed-rwandan-editors-turn-to-african-commission.php

27 IFEX, (2010), 'Rwanda Independent Website Blocked Prior to Elections', retrieved 02/03/2017, http://www.fesmedia-africa.org/what-is-news/statements-developments/news/article/rwanda-independent-website-blocked-prior-to-elections/

independent and critical websites whose publisher is still living in Rwanda, has had his websites maliciously put down by possible state agents.[28] As recently as August 2016, the local language website of the news media outlet Great Lakes Voice was blocked by authorities, according to the State of Internet Freedom in Africa 2016 report.[29]

Meanwhile, the government is reported to use pseudonymous Twitter accounts to intimidate journalists and to spread propaganda.[30] In March 2014, one such Twitter account, which had taunted foreign journalists over their coverage of the government's possible involvement in the murder of an opposition leader, was found to belong to a staff member at the Office of the President.[31]

4. Right to Information

Access to information is recognised under Article 38 of Rwanda's Constitution. Public access to information in the possession of Rwandan authorities is provided for in the Law Relating to Access to Information of 2013. The law outlines the procedures and modalities for requests, receipts and the copy and use of information. Information requests can be made in "writing, telephone, internet and other means of communication." However, the law has no provisions for response times to information requests. Article 11 states that an information officer takes a decision to release information "according to priorities". But as seen in preceding sections, the blockage of various websites, and prosecution of various online journalists, hinder citizens' access to information.

5. Freedom of Assembly and Association and the Internet

Articles 39 and 40 of the Constitution guarantee the rights to freedom of association and "peaceful and unarmed" assembly in accordance with the law, respectively. It is as yet unclear whether these guarantees extend to online spaces.

As of February 2017, Rwanda has not engaged in the wholesale blocking of access to social networking platforms.

Through blocking access to critical websites and content, the government is failing in its duty to provide for the freedom of assembly and association.

6. Cultural and Linguistic Diversity

// Limited data available.

---

28 Great Lakes Voice, (2015), 'Rwanda News Website Ireme Latest to be Blocked', retrieved 02/03/2017, http://greatlakesvoice.com/rwanda-news-website-ireme-latest-to-be-blocked/

29 CIPESA, (2016), 'State of Internet Freedom in Africa 2016', retrieved 02/03/2017, http://cipesa.org/?wpfb_dl=225

30 CIPESA, (2014), 'State of Internet Freedoms in Rwanda, 2014', retrieved 02/03/2017, http://cipesa.org/?wpfb_dl=179

31 CPJ, (2014), 'Twitter War Shines Light on How Rwanda Intimidates Press', retrieved 02/03/2017, http://www.cpj.org/blog/2014/03/twitter-war-shines-light-on-how-rwanda-intimidates.php

7. Right to Development and Access to Knowledge

// Limited data available.

8. Privacy and Personal Data Protection

The right to privacy of person and communications is guaranteed in Article 23 of Rwanda's constitution: "the privacy of a person, his or her family, home or correspondence shall not be subjected to interference in a manner inconsistent with the law; the person's honour and dignity shall be respected... confidentiality of correspondence and communication shall not be waived except in circumstances and in accordance with procedures determined by the law."

Articles 281, 285, 286 and 287 of the Rwandan Penal Code establish a series of offences to protect the right to privacy and the Law No. 4 of 2013 on Access to Information prohibits publication of information held by a public or private body if it may involve interference in the privacy of an individual when it is not in the public interest (Article 4).

Despite these provisions, national legislation governing surveillance is inadequate, leaving significant gaps in safeguards, oversight and remedies against unlawful interference with the right to privacy. Equally, Article 24 of the Telecommunications Law No. 44 of 2001 provides for the protection of users' personal information and data, but there are claw-back clauses that allow the regulator to obtain such information without elaborating the circumstances and procedures for obtaining such information. This law, for instance, requires operators to only collect and process personal information of individual users, which is "strictly necessary for providing bills to users and for determining interconnection payments."[32] This is in conformity with Article 54 of the Act which states, "every user's voice or data communications carried by means of a telecommunications network or telecommunications service, remains confidential to that user and the user's intended recipient of that voice or data communications."

The law that regulates telecommunications contains a general provision safeguarding the privacy of communications and some safeguards (including the requirement of court's authorisation for the interception of communications). None of these limitations, nor the requirement of a court order, are included in the 2013 law regulating the interception of communications (Law No 60/2013). While not explicitly repealing the telecommunications law No. 44/2001 in the regulation of these matters, the 2013 law repeals "all prior legal provisions". The 2013 law empowers the police, army and intelligence services to listen to and read private communications, both online and offline, in the interests of "national security". There is no requirement to justify the interference with someone's privacy as necessary and proportionate to a legitimate aim.

Government authorities of "the relevant security organs" are authorised to apply for an interception warrant. Warrants are issued by a national prosecutor who is appointed by the Justice Minister (Article 9). In urgent

32 RURA, (2001), 'Telecommunications Law No. 44 of 2001', retrieved 02/03/2017, www.rura.rw/fileadmin/laws/TelecomLaw.pdf

security matters, a warrant may be issued verbally, "but the written warrant shall be completed in a period not exceeding twenty four (24) hours". A warrant shall be valid for three months. In May 2014, the government appointed the Ombudsman and Deputy Ombudsman as a team of inspectors in charge of monitoring that interception of communication is done in accordance with the law.[33]

All communication service providers are required to ensure that their systems are technically capable to enable communications interception upon request. However, the law also provides for backdoor access and the interception of communications using technologies that do not require the facilitation by the relevant communication service provider. This allows Rwandan security agencies to hack and to intercept communications without notifying the provider. The risk of abuse is very high especially in a context where political life and public discourse are already significantly government controlled.

There is no comprehensive personal data protection legislation. There is reported to be a Data Protection Bill, 2013[34] containing provisions that would penalise unauthorised access to computer systems and data, unauthorised modification of computer data, unlawful possession of computer systems, devices and data, and unauthorised disclosure of passwords, among others things. Concerns, however, include broad exceptions to the protection of personal data, on grounds of national sovereignty, national security and public order.

The lack of a comprehensive data protection law in Rwanda is of concern with the increasing government collection of individuals' personal data. Mandatory SIM card registration was introduced in 2013, giving RURA and other authorised persons or institutions open access to the SIM card databases of service providers. Also, the Rwandan National Identification Agency has issued biometric IDs to more than 80 percent of the adult population to be used as proof of identity to access a range of services ranging from banking to social security. Without effective data protection provisions, these and other initiatives, such as the introduction of e-passports, expose Rwandans to the risk of breaches to their privacy by state and non-state actors.

In April 2014, it was reported that Rwandan authorities had intercepted the communications of two suspects in a treason trial. According to reports, private messages sent over the phone, WhatsApp and Skype were presented in court as evidence to show conspiracy to topple the government.[35] Two years later in March 2016, the Military High Court in Rwanda sentenced two soldiers - Col Tom Byabagamba to 21 years in jail and Brig Gen (rtd) Frank Rusagara to 20-years in jail, after they were both found guilty of tarnishing

---

33 Ombudsman, (2014), 'Presidential Order appointing inspectors in charge of monitoring the interception of communication', retrieved 02/03/2017, http://www.ombudsman.gov.rw/IMG/AMATEGEKO-%20WEBSITE/INTERCEPTION%20OF%20COMMUNICATION/Iteka%20rya%20Perezida%20rigena%20itsinda%20ry'abagenzuzi%20b'igenzura%20ry'itumanaho.pdf

34 Privacy International, (2015), 'Universal Periodic Review Stakeholder Report: 23rd Session, Rwanda. The Right to Privacy in Rwanda', retrieved 02/03/2017, https://www.privacyinternational.org/sites/default/files/Rwanda%20UPR_PI_submission.pdf

35 The East African, (2014), 'Phone Evidence Used in Terror, Treason Case', retrieved 02/03/2017, http://www.theeastafrican.co.ke/news/Phone-evidence-used-in-terror/-/2558/2294196/-/klwpvi/-/index.html

the image of the country, among others. For Rusagara, it was stated that on several occasions he circulated material, mainly through his email, most of which was propaganda based on rumours, with an aim of tarnishing the image of the state. During the hearings, the military prosecution displayed messages that the former general shared using his emails.[36]

According to leaked emails from Hacking Team, an Italian surveillance firm, the Rwandan government allegedly attempted to purchase the company's sophisticated spyware, known as Remote Control System (RCS) in 2012.[37]

9. Security, Stability and Resilience of the Internet

In March 2015, Rwanda approved the National Cyber Security Policy aimed at safeguarding public and private infrastructure, personal information of web users, financial/banking information as well as sovereign data from cyber-attacks.[38] The policy was developed in consultation with stakeholders through the Ministry of ICT. Consequently, the Rwanda National Police set up a Cybercrime and Digital Forensics unit, which provides anti-cybercrime trainings with the help of Interpol to equip the police with skills to detect and investigate cybercrime, understand cyber terrorism, principles of evidence collection for cybercrime, electronic money transfer technology, and basic ICT tools in analyzing cybercrime evidence.

Meanwhile, one of the objectives of the 2013 Draft ICT Bill[39] is to put in place strategies to ensure information security and network reliability and integrity in terms of electronic communications.

10. Marginalised Groups and Groups at Risk

Law N° 47/2001 on Prevention, Suppression and Punishment of the Crime of Discrimination and Sectarianism penalises discrimination and sectarianism defined as "any speech, writing, or actions based on ethnicity, region or country of origin, the colour of the skin, physical features, sex, language, religion or ideas aimed at depriving a person or group of persons of their rights as provided by Rwandan law and by International Conventions to which Rwanda is party"; and "any speech, written statement or action that divides people, that is likely to spark conflicts among people, or that causes an uprising which might degenerate into strife among people based on discrimination" respectively.

Further, Law N° 84/2013 on the crime of genocide ideology and other related offences, which repealed the Repression of Genocide Ideology Law 2008, defines the crime as "...any deliberate act, committed in public whether orally,

---

36 The New Times, (2016), Rodrigue Rwirahira, Byabagamba, Rusagara get lengthy jail terms, retrieved 02/03/2017, http://www.newtimes.co.rw/section/article/2016-04-01/198556/

37 WikiLeaks, (2015), 'Hacking Team', retrieved 02/03/2017, https://wikileaks.org/hackingteam/emails/emailid/449906

38 The New Times, (2015), 'Cabinet Approves CyberSecurity Policy', retrieved 02/03/2017, *http://www.newtimes.co.rw/section/article/2015-03-22/187138/*

39 The Rwandan Parliament, (2013), 'Draft Law Governing Information and Communication Technologies', retrieved 02/03/2017, www.parliament.gov.rw/uploads/tx_publications/DRAFT_LAW___GOVERNING_INFORMATION_AND_COMMUNICATION_TECHNOLOGIES.pdf

written or video means or by any other means which may show that a person is characterized by ethnic, religious, nationality or racial-based with the aim to: (1) advocate for the commission of genocide; (2) support the genocide."

11. Right to Due Process

Ambiguities in Rwanda's legislation, including the Media Law, mean that there is a possibility that the right to due process is not being fully enacted in all cases. The blocking of opposition websites, and the websites of organisations such as the BBC, who have aired content that does not necessarily follow the government line, does not comply with the African Declaration's need for the recognition of the internet as a forum for debate and freedom of expression.

12. Democratic Multistakeholder Internet Governance

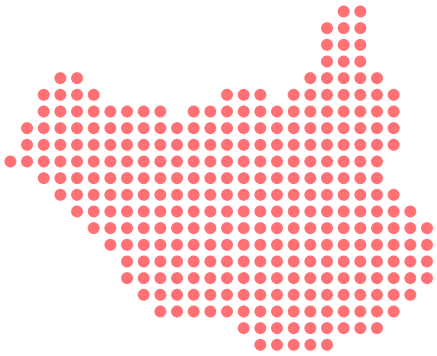
The Rwanda Utilities Regulatory Authority was established under the 2001 law governing telecommunications as an autonomous institution to regulate the provision of public utilities goods and services, including telecommunications. The 2001 law was amended in 2013 and RURA's mandate was extended to include "telecommunications, information technology, broadcasting and converging electronic technologies including the internet and any other information and communication technology." The authority regularly consults the public and stakeholders in its decisions. Recent consultations have been on the regulations governing postal and courier services and telecom network security.

13. Gender Equality

Women and youth empowerment is among the pillars of Vision 2020, with a focus on ICT education, skills and capacity building, and increased participation in ICT related business.

South Sudan

South Sudan is a young country, and legislative frameworks around internet freedom are still emerging. The country faces numerous obstacles to internet access, including a poor ICT infrastructure, expensive internet access and low digital literacy rates. In addition to this, recent legislation has provided authorities with sweeping powers to intercept communications and carry out arrests without proper judicial oversight. With an intense civil conflict ongoing, there is currently little attention being paid the development of the digital landscape.



1. Openness

The Ministry of Telecommunications and Postal Services (MoTPS) and the Ministry of Information and Broadcasting (MoIB) govern the ICT sector. The MoTPS oversees the formation and implementation of the ICT sector,[40] whilst the Ministry of Telecommunications in particular oversees the ICT sector. The two ministries share responsibilities in the licensing of new media operators - the MoIB gives approvals, assesses and issues licenses for establishments while the MoTPS controls the frequency allocations.

The Media Authority Act 2013 recognises the internet and new media as modes of communication. Under Article 14 (b), the Act states that registration requirements related to the internet and new media should not hinder competition nor be used as a means of restricting market entry. There are five telecommunication operators in South Sudan: MTN, Zain, Sudatel, Vivacell and Gemtel.[41]

2. Internet Access and Affordability

According to ITU estimates for 2015, South Sudan's internet penetration rate stands at 17.9%, with mobile penetration at 23.9%.[42] Key challenges in the ICT sector include weaknesses in government regulation, insufficient ICT infrastructure and expertise, expensive internet access, and lack of awareness of the potential of ICT, which in itself corresponds with low digital literacy rates.[43] Nonetheless, there is a significant amount of activity within the country's ICT sector to expand broadband connectivity and mobile services. As South Sudan does not currently have an ICT policy framework in place, ongoing efforts to boost infrastructure capacity have seen the country coordinate operational efforts in partnership with its East African counterparts.

In January 2015, South Sudan and Kenya signed on to a joint project to connect the two countries by fibre optic cables.[44] With funding from the World Bank, the project was commissioned in September of the same year.[45] Further, South Sudan joined the One Network Area scheme, which removed international roaming charges for calls between Uganda, Kenya, Rwanda and South Sudan.[46]

---

40 GOSS, (2008), 'Telecommunications and Postal Services Sector Policy, Framework and Work Plan 2008'.

41 Budde, (2016), 'South Sudan - Telecoms, Mobile and Broadband - Statistics and Analyses', retrieved 02/03/2017, https://www.budde.com.au/Research/South-Sudan-Telecoms-Mobile-and-Broadband-Statistics-and-Analyses

42 ITU, (2015), 'South Sudan Profile 2015', retrieved 02/03/2017, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

43 Fortune of Africa, (2016), 'ICT and Telecommunication Sector of South Sudan', retrieved 02/03/2017, http://fortuneofafrica.com/southsudan/ict-and-telecommunication-sector-of-south-sudan/

44 Business Daily Africa, (2015), 'Kenya, South Sudan in plan to lay fibre optics to Juba', retrieved 02/03/2017, http://www.businessdailyafrica.com/Corporate-News/Kenya--South-Sudan-in-plan-to-lay-fibre-optics-to-Juba/-/539550/2600108/-/bpwc67/-/index.html

45 All Africa, (2015), 'Sudan: World Bank Releases Sh54 Billion for S. Sudan Fibre Optic Link', retrieved 02/03/2017, http://allafrica.com/stories/201509091537.html

46 The East African, (2014), 'EA to adopt One Network Area, call rates to drop', retrieved 02/03/2017, http://www.theeastafrican.co.ke/news/-/2558/2554690/-/50hk8dz/-/index.html

3. Freedom of Expression

South Sudan is not party to some key international and regional human rights instruments, such as the International Covenant on Civil and Political Rights (ICCPR), the International Covenant on Economic Social and Cultural Rights (ICESCR), and the African Charter on Human and Peoples' Rights (ACHPR), which raises concerns about the young nation becoming a functioning democratic state.[47]

However, freedom of expression and media is provided for under Article 24 of the 2011 Constitution. The Article states:

> (1) Every citizen shall have the right to the freedom of expression, reception and dissemination of information, publication, and access to the press without prejudice to public order, safety or morals as prescribed by law.
>
> (2) All levels of government shall guarantee the freedom of the press and other media as shall be regulated by law in a democratic society.
>
> (3) All media shall abide by professional ethics.

Article 13 (a) of the Media Authority Act 2013 states that all media should be protected as essential to democracy. The law also protects the media from censorship by any official or non-official authority under Article 13 (b). There are no registration requirements for practising journalism (Article 13 (h)). Unlawful arrest, detention, harassment, intimidation and the torture of journalists, including photojournalists, is prohibited under Article 13 (p).

The 2013 Act criminalises defamation, hate speech and incitement of violence. Complaints are made to the Press and Broadcast Council which is tasked with the investigation and resolution of matters through mediation and negotiation. Sanctions for defamation include a requirement for the false information to be corrected, and compensation. Regarding hate speech and incitement, possible sanctions include publication of a correction or apology, compensation, a fine, warning, suspension or the termination of a broadcast license, and the seizure of equipment, among others. Fines and compensation amounts are not specified. For hate speech and incitement cases deemed "serious", and where "malicious intent or recklessness is shown", a prison term of up to five years may be imposed.

Although the Broadcasting Corporation Act 2013 seeks to promote a free press through setting up an oversight body free from government interference, the board, chairperson and vice chairperson are appointed by the president upon approval of the National Legislative Assembly (NLA) through a majority vote (Article 10). For the regulation, development and promotion of a professional media sector, the 2013 Media Act establishes the independent Media Authority. However, similar to the Broadcasting Corporation Act, members of the Board of the Media Authority are appointed by the president

47 See: OHCHR, 'Status of Ratification of 18 International Human Rights Treaties', retrieved 02/03/2017, http://indicators.ohchr.org and 'ACHPR Ratification', retrieved 02/03/2017, http://www.achpr.org/instruments/achpr/ratification/

upon approval of the NLA through a majority vote (Article 9).

No statistics are available on social media usage in the country. Nonetheless, platforms such as Twitter and Facebook have become increasingly popular for information sourcing and sharing. However, the same platforms have been criticized for fueling ethnic tension by spreading false news.[48]

Liability of service providers is limited under Article 14(g) of the Media Authority Act 2013 which states that "internet service providers shall be regarded as providing carriage for information and that function shall incur no legal liability imposed by the content that is carried." Furthermore, under Article 14 (i), internet service providers are "not liable for any aspect of the content which they transmit in their function of providing data carriage."

Regarding content filtering, Article 14 (k) of the media law restricts it to pornographic content upon user request. It states that "to the extent that filtering of pornographic content or material is needed, internet service providers shall provide upon request by the end user, filtering software for terminals, or equivalent filtering services applied by the service provider before reaching end user terminals".

4. Right to Information

The right of access to information is provided for under Article 32 of the Constitution which states: "Every citizen has the right of access to official information and records, including electronic records in the possession of any level of government or any organ or agency thereof, except where the release of such information is likely to prejudice public security or the right to privacy of any other person."

The Right to Access Information Act 2013 gives effect to citizens' constitutional right to access information and promotes disclosure in the interest of the public. Under Article 22 of the Act, information that "may harm protected interests" is exempt from disclosure. The burden of proof of potential harm lies with the relevant public or private agency. The Article further states that information is not exempt from access "merely on the basis of its classification status."

Requests can be made to public and private bodies in writing. Where an individual is unable to make a request in writing, an oral request can be submitted. Under this law, requests for information should be responded to within seven working days with provision for an extension of up to 20 days. Article 10 (2) provides for expedited responses to information requests for securing the life or liberty of a person within 48 hours. Failure to respond is deemed a rejection. However, the Act does not provide recourse procedure for denial of information.

The Act imposes fees for reproduction, retrieval or transcribing costs of information requests. Requests for personal information about the requester

48 Till Waescher, (2016), 'Access to Information and Freedom of Expression are a Myth in South Sudan - An Interview with Philips Anyang Ngong', retrieved 02/03/2017, http://www.global.asc.upenn.edu/access-to-information-and-freedom-of-expression-are-a-myth-in-south-sudan/

or those made in the interest of the public are exempt from fees.[49] Pursuant to the Act, all public bodies are required to appoint an information officer to serve as a central contact and promote best practices in relation to record maintenance.

5. Freedom of Assembly and Association and the Internet

Articles 25 and 26 of the Constitution guarantee the rights to freedom of association and assembly, and the right to participate, respectively. It is unclear to what extent these rights are guaranteed for online activities.

However, Freedom House points out that these rights are not adhered to by the government.[50] Protests are violently put down and pro-opposition journalists have been labelled "anti-government agitators" by state officials.[51]

6. Cultural and Linguistic Diversity

// Limited data available.

7. Right to Development and Access to Knowledge

// Limited data available.

8. Privacy and Personal Data Protection

Article 22 of South Sudan's constitution guarantees citizens the right to privacy of home, family and correspondence. "Unreasonable" disclosure of personal information is prohibited under Article 25 of the Right to Information Act. However, under the same article, a court may order the disclosure of personal information if it determines that it is in the interest of the public. The country has no data protection law.

In October 2014, the South Sudan government passed the National Security Service (NSS) law, which gives security agencies unfettered authority to arrest and detain suspects, monitor communications, conduct searches, and seize property without clear judicial oversight. Article 13 (11) of the Act gives the NSS the powers to "monitor frequencies, wireless systems, publications, broadcasting stations and postal services in respect to security interests so as to prevent misuse by users." Further, under Article 13 (12), the authority has the power to "request any information, statement, document, or any relevant material from any suspect and potential witness for perusal or examination, keep or take necessary or appropriate measures in respect of such information, statement, document or relevant material". Under Article 32, the NSS also has the power to "gather and retain information related to any person, persons or institutions as is necessary for carrying out its duties and functions."

---

49 See Article 12

50 Freedom House, 'South Sudan', retrieved 08/02/2017, https://freedomhouse.org/report/freedom-world/2016/south-sudan

51 Foreign and Commonwealth Office, 'South Sudan - Country of Concern', retrieved 08/02/2017, https://www.gov.uk/government/publications/south-sudan-country-of-concern--2/south-sudan-country-of-concern

The operations of the security service are overseen by the security minister who, under Article 14 (6), is mandated to "approve the functional directives" issued by the directors of the NSS "in relation to physical security, communication security, protection of classified information and any other matter necessary for the Service".

In the second half of 2012, South Sudan was the only African country to have made a user information request to Twitter. The information request was rejected.[52]

SIM Card registration is in force in the country. Requirements for subscriber registration include a valid identity document, such as a national ID, passport or voter's card.[53]

9. Security, Stability and Resilience of the Internet

As reported in the ITU CyberWellness profile, South Sudan does not have any officially approved national or sector specific cyber-security framework for implementing internationally recognised cyber security standards.[54]

10. Marginalised Groups and Groups at Risk

// Limited data available

11. Right to Due Process

As mentioned above, in October 2014, the South Sudan government passed the National Security Service (NSS) law, which gives security agencies unfettered authority to arrest and detain suspects, monitor communications, conduct searches, and seize property without clear judicial oversight. By removing proper judicial oversight, and giving overarching powers to security services, due process is placed at risk.

12. Democratic Multistakeholder Internet Governance

// Limited data available

13. Gender Equality

In March 2015, the first South Sudan Information Communication Technology for Development (ICT4D) conference was held in the country's capital Juba, resulting in key recommendations to promote and facilitate the use of ICT in all sectors. Among them were gender mainstreaming in the ICT sector, establishment of a fund to support research and innovation, exchange

---

52 Twitter, 'Twitter Transparency Report', retrieved 02/03/2017, https://transparency.twitter.com/en/countries/ss.html

53 See: NCA-SS, (2016), 'South Sudan Extends Simcard Registration Deadline', retrieved 02/03/2017, http://nca-ss.org/index.php/2016/06/09/welcome-to-national-communication-authority-south-sudan-3/ and MTN South Sudan, 'MTN Simcard Registration', retrieved 02/03/2017, http://www.mtn-ssd.com/simRegistrationLanding.html

54 ITU, (2015), 'CyberWellness Profile Republic of South Sudan', retrieved 02/03/2017, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/South_Sudan.pdf

programmes and the establishment of ICT training centres for the youth.[55]

55 UNESCO, (2015), 'South Sudan Accelerates ICT in all Sectors' retrieved 02/03/2017, http://www.unesco.org/new/en/communication-and-information/resources/news-and-in-focus-articles/in-focus-articles/2015/south-sudan-accelerates-icts-in-all-sectors

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.

1. Openness

Tanzania's Communications Regulatory Authority (TCRA) licences operators under four main categories – network facility services, network services, application services and content services and corresponding market segments: International, National, Regional, District and Community. There are seven telecoms operators in the country - Airtel, Zantel, Halotel, Vodacom, Tigo, TTCL and Smart. In addition to this, there are 28 internet Service Providers registered with the Tanzania Internet Service Providers Association (TISPA).[56] As of April 2016, Tanzania had a total of 123 licensed radio stations, 24 televisions stations and 881 print media outlets – some of which maintain an online presence. The country does not have guidelines on network neutrality.

2. Internet Access and Affordability

According to the Tanzania Communications Regulatory Authority (TCRA) Quarterly Statistics reports of December 2016, there were 40.1 million mobile and fixed telephone subscribers, representing a penetration rate of 80%.[57] For the same period, the regulator reported a total of 19.8 million internet users, translating into a 40% penetration.[58] The average monthly cost of 1GB mobile internet is US$ 4.

The Universal Communications Service Access Fund, established in 2006, is aimed at ensuring availability of communication services in rural and urban underserved areas.[59] As of August 2016, the fund had provided over US$ 36 million to operators to aid infrastructure set-up in rural areas. Internet connectivity has been extended to schools and hospitals in at least 10 regions across the country.[60]

Tanzania's National ICT Policy of May 2016 has broadband access and infrastructure development among its objectives. The policy states that "it intends to put in place measures and mechanisms to accelerate broadband penetration and access" by ensuring a conducive environment of collaboration between the public and private sector in exploring various means of financing access to broadband services, as well as ensuring the availability and accessibility of reliable and affordable broadband services country-wide.[61]

TISPA operates the Tanzania Internet eXchange (TIX) whose aim is to provide a local facility for the exchange of internet traffic in the country. Currently,

---

56 TISPA, (2017), 'Tanzania Internet Service Providers Association (TISPA), Members as at February 2017', retrieved 02/03/2017, http://tispa.or.tz/?page_id=24

57 TCRA, (2016), more at http://www.tcra.go.tz/images/documents/telecommunication/CommStatMarch16.pdf as accessed on 20th July 2016

58 *Ibid*

59 See section 4(1) and 6(a) of the Universal Communications Service Access Act, 2006

60 USCAF, (2016), 'Universal Communications Services Access Fund, Rural Telecommunication Project August 2016', retrieved 02/03/2017, http://www.ucsaf.go.tz/files/publications/attachments/7a3147aad8bedd6e5a0aeec341f253f4.pdf

61 Ministry of Works, Transport and Communication, (2016), 'National ICT Policy 2016', retrieved 02/03/2017, https://tanzict.files.wordpress.com/2016/05/national-ict-policy-proofed-final-nic-review-2.pdf

there are 34 internet service providers connected to it.[62]

3. Freedom of Expression

Article 18 of the Tanzanian Constitution of 1977 guarantees the right to freedom of opinion and expression and the rights to seek, receive and impart information. It states: "every person - (a) has a right to freedom of opinion and expression of his ideas; (b) has a right to seek, receive and, or disseminate information regardless of national boundaries; (c) has the freedom to communicate and protection from interference with his communication; (d) has a right to be informed at all times of various important events of life and activities of the people and also of issues of importance to the society."

For 40 years, Tanzania's media landscape was governed by the Newspaper Act 1976. The 1976 Act was recently repealed by the Media Services Act, 2016 which was enacted in November 2016 and came into effect a month later. However, the new Act maintains a lot of the provisions contained in the previous law. Article 7 sets out the obligations of media houses while Article 8 provides for licensing. The Act requires that all journalists be accredited (Article 18-20) in order to be able to practice journalism and grants the Minister of Information, Culture and Sports the power to prohibit or sanction the publication of any content that jeopardises national security or public safety (Section 59). The same Act gives the Minister powers to prohibit importation of a publication if he or she is of the opinion that its importation would be contrary to the public interest.

Under Article 47 of the 2016 Act, it is an offense to publish information or content which is "intentionally or recklessly falsified" or malicious or fraudulent, and threatens national defense or economic interests, public order and safety, morality or public health. Publication of defamatory content is an offence under the Act (Part V), as is the publication of seditious content (Article 49-50).

Any person who operates unlicensed media, practices journalism without accreditation, disseminates false information or prints, publishes, sells, distributes or reproduces seditious content is liable to a fine of between Tanzania Shillings (TZShs) 5 - 20 million (US$ 2,200 – 8,800) or imprisonment for a period of three to five years, or both (Article 47). Other offenses in the Act include the publication of "any false statement, rumour, or report which is likely to cause fear and alarm to the public or to disturb public peace".

The Media Council of Tanzania (MCT), Legal and Human Right Centre (LHRC), and Tanzania Human Rights Defenders Coalition (THRDC) lodged a petition at the East African Court of Justice (EACJ) on January 11, 2017 to challenge the Media Services Act and suggested the amendment of several provisions.[63]

---

62 Tanzania Internet Exchange, retrieved 02/03/2017, https://www.tix.or.tz

63 African Centre For Media Excellence, (2017), 'Tanzania Media Services Act, 2016 challenged at the East African Court of Justice', retrieved 02/03/2017, https://acme-ug.org/2017/01/13/tanzania-media-services-act-2016-challenged-at-the-east-african-court-of-justice/

In June 2015, Tanzanian authorities published guidelines for blogs and other online content providers in advance of the elections. Under the rules, online media are required to register with the TCRA, take steps to ensure balanced election coverage, edit controversial user comments and online discussions, and give the right to reply to aggrieved parties and candidates.[64]

The National Security Act of 1970 makes it a punishable offence to in any way investigate, obtain, possess, comment on, pass on or publish any document or information which the government considers to be classified. It is also an offense to "communicate classified matter to an unauthorized person, or to approach, inspect or enter a protected place for any purpose prejudicial to the safety or interests of the United Republic of Tanzania." There is no clear stipulation, according to the existing Civil Service Standing Orders, as to what constitutes a classified document and as a result, even a letter of staff transfer from one department to another can be considered to be classified information.

The Electronic and Postal Communications Act of 2010 (EPOCA) establishes several offences which criminalise the freedom of expression and create a harsh environment for it in general. This includes prohibitions against the transmission of obscene communications, which are not defined, and prohibitions against the use of a cyber network without authorisation. Section 124(3) states: "Any person who secures unauthorised access to a computer or intentionally causes or knowingly causes loss or damage to the public or any person, destroy or delete or alter any information in the computer resources or diminish its value or utility or affect it injuriously by any means, commits an offence" and on conviction is liable for a fine not less than TZShs 500,000 (US$ 220) or imprisonment of up to three months or to both. Section 132 contains sanctions against "false information". It states: "Any person who furnishes information or makes a statement knowing that such information or statement is false, incorrect or misleading or not believing it to be true, commits an offence" and is liable upon conviction to a fine of TZShs three million (US$ 1,300) or a year in prison, or both.

Under sections 37 (4) and (5) of the Statistics Act, 2015 it is an offence for a "radio station, television station, newspaper or magazine, website or any other media" to publish "false statistical information" or for an "agency or person" to publish "official statistical information which may result in the distortion of facts." Additionally, the Statistics Act imposes harsh penalties on those found guilty of publishing misleading and inaccurate statistics or statistics not approved by the National Statistics Bureau. The punishment is a one-year jail term and a fine of TZShs 10 million (US$ 4,586).

Meanwhile, the Cybercrime Act, 2015 which is aimed at "criminalizing offences related to computer systems and Information Communication Technologies" seeks to address child pornography (Section 13), cyberbullying (Section 23), online impersonation (Section 15), electronic production of racist and xenophobic content (Section 17), unsolicited messages (otherwise known as spam) (Section 20), illegal interception of communications (Section

64 CIPESA, (2015), 'Tough New Election Reporting Rules for Tanzania's Bloggers', retrieved 02/03/2017, http://cipesa.org/2015/08/tough-new-election-reporting-rules-for-tanzani-as-bloggers/

6), and publication of false information (Section 16).

Section 16 of the Act states: "Any person who publishes information, data or facts presented in a picture, text, symbol or any other form in a computer system where such information, data or fact is false, deceptive, misleading or inaccurate commits an offence, and shall on conviction be liable to a fine not less than three million shillings (US$ 1,300) or to imprisonment for a term not less than six months, or to both."

The Cybercrime Act has been criticised for being stringent on press freedom and freedom of expression, with stiff penalties for vague offences such as sending spam, which attracts a penalty of at least TZShs 3,000,000 (US$ 1,300) or three times the value of undue advantage received, whichever is greater, imprisonment for at least one year, or both. The Act also provides for restrictions against data espionage (Section 8), for instance, which may also limit information necessary for investigative journalism, research or other legitimate use.
Within months of its enactment, the Cyber Crimes Act was used against 10 social media users.[65] According to the State of Internet Freedom in Tanzania 2016 report several cases have been filed by the government against persons who, in various ways, are alleged to have broken the Cybercrimes Act.[66]

During the tallying of results for the 2015 elections, popular online discussions forum Jamii forums unexpectedly went offline and was inaccessible for a couple of hours before it was restored by its administrators. But it is not clear if the government had a hand in the site's take down, and if it did, how. Back in February 2008, the forum's founders were detained and interrogated for 24 hours, in what observers said was a politically motivated attempt to shut down the site. Although they were released after one day, police confiscated three computers used to host their website, shutting down the site for five days while the equipment remained under police custody.[67] Furthermore, in 2011, it was reported that Jamii Forums was cloned by the Tanzania government to disrupt conversations of members associated with the opposition.[68] More recently in December 2016, one of the site founders was arrested, detained for five days and charged under the cybercrime law with the obstruction of investigations for declining to reveal to police the identities of individuals who posted content to the forum, and "operating a domain not registered in Tanzania".[69]

---

65 Reuters, (2016), 'Tanzanian lecturer charged with insulting president on WhatsApp', retrieved 02/03/2017, http://www.reuters.com/article/us-tanzania-president-idUSKCN11T14C?il=0

66 See: CIPESA, (2016), 'State of Internet Freedom in Tanzania 2016', retrieved 02/03/2017, http://cipesa.org/?wpfb_dl=229

67 Balancing Act, (2009) 'Tanzanian Government detains two website editors', retrieved 02/03/2017, http://www.balancingact-africa.com/news/en/issue-no-395/internet/tanzanian-government/en#sthash.AHUhqz7O.dpuf

68 Interview with Jamii Media co-founder Maxence Melo, (2016)

69 CIPESA, (2016), 'UPDATE: Maxence Melo Charged with Obstruction of Investigations and Operating a Domain Not Registered in Tanzania', retrieved 02/03/2017, http://cipesa.org/2016/12/update-maxence-melo-charged-with-obstruction-of-investigations-and-operating-a-domain-not-registered-in-tanzania/

In September 2015, human rights activists filed a case at the High Court, protesting some sections of the Cybercrime Act. The Tanzania Human Rights Defenders Coalition (THRDC), Legal and Human Rights Centre (LHRC) and other organisations sought the amendment of several provisions that infringe freedom of expression, privacy and the right to information. In December 2016, the High Court declared only Section 50 of the law unconstitutional. This section relates to the Director of Public Prosecutions being able to punish suspects who confess before the start of court procedures. The activists have mentioned that they would appeal against the decision.[70]

4. Right to Information

Tanzania's Access to Information Act was passed in September 2016, ten years after it was first drafted. The Act provides for public access to information in the possession of Tanzanian authorities as well as private entities which utilise public funds, and are in possession of information of public interest. Exemptions apply to information that may "undermine the defense, national security and international relations" of Tanzania, impede due process or endanger the life of a person, undermine lawful investigations, facilitate the commission of an offense or infringe commercial interests such as intellectual property. Other exemptions include information that may cause "harm" to the economy, judicial considerations, legal proceedings and cabinet records.

Information requests can be made in writing or orally on grounds of disability or illiteracy. The Act stipulates a response time to requests of 30 days. Article 19 of the Act provides for the review of the decisions of information holders, as well as appeals.

5. Freedom of Assembly and Association and the Internet

Article 20 of the Constitution guarantees the freedom of association, stating that "Every person has a freedom, to freely and peaceably assemble, associate and cooperate with other persons, and for that purpose, express views publicly and to form and join with associations or organizations formed for purposes of preserving or furthering his beliefs or interests or any other interests."

Further, Article 21 provides for the freedom to participate in public affairs including the right to take part in matters pertaining to the governance of the country, either directly or through representatives freely elected by the people, in conformity with the procedures laid down by, or in accordance with the law and the freedom to participate fully in the process leading to the decision on matters affecting him/her, his/her well-being or the nation.

However, the arrest of one of Jamii Forum's founders, alongside those of social media users under the Cybercrimes Act suggest that in practice, the Tanzanian government is denying freedom of assembly and association on the internet.

---

70 The Citizen, (2017), 'Activists to Challenge Ruling on Cybercrime Law', retrieved 02/02/2017, http://www.thecitizen.co.tz/News/Activists-to-challenge-ruling-on-cybercrime-law/1840340-3505144-dfsp99/index.html

6. Cultural and Linguistic Diversity

// Limited data available.

7. Right to Development and Access to Knowledge

// Limited data available.

8. Privacy and Personal Data Protection

Currently, Tanzania does not have a data protection and privacy law. Nevertheless, personal data and privacy are still safeguarded by provisions of Article 16 of the Constitution, which provides for a right to privacy. Among other things, the provisions prohibit unnecessary and unreasonable interference with personal communication. Furthermore, regulation 6(2)(e) of the Electronic and Postal Communication (Consumer Protection) Regulations, 2011 protects customer data from unwanted disclosure. Citizens' privacy is also protected under Article 6 of the Right to Information Act 2016, which exempts the disclosure of information that may invade the privacy of an individual.

The Tanzania Communications Regulatory Authority Act of 2003 allows the authority to obtain information, documents and evidence related to communications in the performance of its functions (Section 17). This provision may be misused by state agencies to compel ISPs to release user information to the government.

Sections 30 and 31 of the Prevention of Terrorism Act (2002) provide for intelligence gathering and the lawful interception of communications. Section 30 allows the Minister to require communication service providers to retain communications data for the purposes of the prevention or detection of offences of terrorism or for the purposes of prosecution of offenders under the Act. Section 31 gives a police officer powers to intercept communications for purposes of obtaining evidence of commission of an offence of terrorism upon issuance of a court order. Similarly, police officers may be authorised under the law to enter any premises and to install any device for the interception and retention of communications. Moreover, section 31(4) of the same Act allows the admissibility as evidence of any communications intercepted, including from outside of the country, in proceedings for any offence under the Act.

Meanwhile, EPOCA allows the government to intercept the communications of an individual by making an application to the public prosecutor for authorisation to intercept or to listen to any communication transmitted or received by any communications. The public prosecutor must consider whether any communications are likely to contain any information relevant to an investigation before authorising such access.

The 2015 Cybercrime Law gives police wide-ranging ability to search the homes of suspected violators of the law, seize their electronic hardware, and demand their data from online service providers (Part IV). Fears of abuse of these powers were found to be legitimate during the 2015 elections when police searched and seized computers, cell phones and other electronic gadgets of members of an opposition party and a human rights organisation

who were monitoring the election.[71]

Meanwhile, the Tanzania Intelligence and Security Service Act of 1996 is also relevant to the interception of communications because of the powers the Act gives to security agencies to collect intelligence and investigate crimes. Section 18 outlines the powers to investigate and conduct interception of communications which permit the Tanzanian intelligence service to enter into arrangements with various other actors including any person, local government or other authority, any police force or other policing organisations, as well as foreign governments or international organisations of states with the sole authorisation of the Minister responsible, as well as the Minister of Foreign Affairs in the case of engagement with foreign governments and organisations. Exercising this power, the Act can facilitate interception of any communication on the grounds of national security.

Mandatory SIM card registration has been in effect in Tanzania since January 2009. In a public notice, TCRA required mobile service providers to maintain databases of information on their subscribers including: information on the name, phone number, date of birth, gender, address, alternative phone numbers and ID card numbers such as passports, driving licences, student cards, voter registration cards or letters from a local government official. In May 2013, it was announced that all unregistered SIM cards would be deactivated on July 10.[72] Last July, the regulator imposed fines on six telecom companies for "irregularities" in subscriber registration.[73]

There is speculation amongst citizens that the government conducts surveillance on communication over social media platforms such as WhatsApp, especially of individuals suspected of spreading false or defamatory statements against the government or the president. In a recent incident, a message allegedly from TCRA that went viral demanded that the recipient surrenders to a police station on allegations that their number was used to spread false and defamatory statements against the president.[74] In another case, opposition Member of Parliament Godbless Lema was arrested and reprimanded by the police on allegations of publishing online statements which were construed as incitement.[75]

Meanwhile, emails released by WikiLeaks from the Italian surveillance malware vendor Hacking Team, revealed an exchange between

---

71 Protectionline, (2015), 'Arrest of 38 Human Rights Defenders at TACCEO Election Observation Centre', retrieved 02/03/2017, http://protectionline.org/2015/11/04/tanzania-arrest-38-human-rights-defenders-tacceo-election-observationcenter/

72 TCRA, (2013), 'Public Notice, SIM Card Registration', retrieved 02/03/2017, https://www.tcra.go.tz/images/Press%20Release/simCardRegPresRelease2013.pdf

73 The East African, (2016), 'Tanzania fines six telcos over sim registration', retrieved 02/03/2017, http://www.theeastafrican.co.ke/business/Tanzania-fines-six-telcos-over-sim-registration/-/2560/3287896/-/11v5r86z/-/index.html

74 This message was shared on various social media platforms, including Whatsapp, Instagram and Facebook.

75 Tanzania Today, 'Lema Arrested by Police', retrieved 02/03/2017, http://www.tanzaniatoday.co.tz/news/lema-akamatwa-na-polisi

representatives from the Tanzanian President's Office and Hacking Team.[76]

An email from the government representative expressed interest in visiting Hacking Team's office with a view of purchasing its Galileo surveillance system.[77] This surveillance technology has the ability to bypass encryption, take control of a user's device and monitor all activities conducted on the device.

According to the 2015 Vodafone Law Enforcement Disclosure Report, in 2014 Tanzania's government made 933 requests for local subscribers' data.[78]

9. Security, Stability and Resilience of the Internet

// Limited data available.

10. Marginalised Groups and Groups at Risk

Tanzania has criminalised homosexuality, and although the prosecution of same sex conduct has not occurred in a number of years, there is still a strong threat to LGBT individuals and groups in the country. Although there is no specific legislation preventing full use of the internet by marginalised groups, this pre-existing legislation means that in practice, there are limitations.

11. Right to Due Process

As noted above, a number of items of Tanzanian legislation contain vaguely worded articles that empower the government to make arbitrary arrests. The Electronic and Postal Communications Act of 2010 (EPOCA)'s language around "obscene communications" and "false information" are particularly clear examples of this ambiguity.

12. Democratic Multistakeholder Internet Governance

Among the regulatory decisions influenced by public consultations is the issuance of licences (pursuant to Article 8 of EPOCA). Recent stakeholder consultation exercises have included a broadcasting services content code[79], review of ICT policy (2003) and a review of the 2003 information and broadcasting policy.

13. Gender Equality

// Limited data available.

---

76 Wikileaks, (2015), 'Hacking Team', retrieved 02/03/2017, https://wikileaks.org/hackingteam/emails/emailid/11776

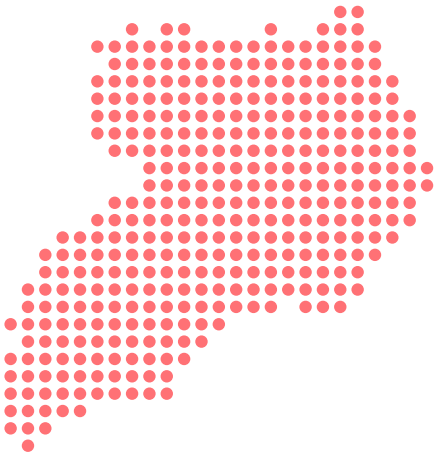
77 Galileo is a remote control system which allows the user to take control of a target's equipment and to monitor them, even if they are using encryption. Hacking Team sells it as a tool to "bypass encryption, collect relevant data out of any device, and keep monitoring your targets wherever they are, even outside your monitoring domain." For more information: Hacking Team, 'Galileo', retrieved 02/03/2017, https://www.hackingteam.it/images/stories/galileo.pdf

78 Vodafone, (2015), 'Country-by-country disclosure of law enforcement assistance demands, 2015', retrieved 02/03/2017, http://www.vodafone.com/content/index/about/sustainability/law_enforcement/country_by_country.html

79 TCRA, (2014), 'The Broadcasting Services Code, 2014', retrieved 02/03/2017, http://www.tcra.go.tz/images/headlines/CodePoliticalPartyElectionsBroadcasting2014.pdf

Uganda

When compared to the other countries in this report, Uganda's digital landscape is generally better developed. Internet access is relatively affordable, and there are government schemes in place that aim to support increased public access to the internet. However, there are also number of laws in place that seek to curtail internet freedom, particularly with regard to freedom of expression. As in other countries in the region, minority communities such as the LGBTI community face particularly high levels of threat online.



1. Openness

Uganda's telecommunications licensing framework is technology neutral, operating under a multi-service authorisation regime - meaning that the regulator does not discriminate between the types of technology through which licensed providers choose to provide public communication services.[80]

Uganda has five major mobile network operators – MTN, Airtel, Africell, Vodafone, and Uganda Telecom. Smaller service providers include Smart Telecom, Smile Telecom, and K2 Telecom. These operators, alongside others, bring the total number of licensed communications providers in Uganda to 47. As of September 2016, Uganda's broadcasting sector had 34 television stations and 292 radio stations in operation.

2. Internet Access and Affordability

Mobile and fixed telephone subscriptions in Uganda stood at 22.3 million (implying a penetration rate of 61%) as of September 2016. In the same period, internet penetration was reported as 45% or at approximately 16.7 million internet users.[81] Currently, the average cost for a daily 10MB mobile Internet bundle is as low as 300 Uganda Shillings (UGX) (about US$ 0.10), while a monthly 1GB bundle costs between Uganda Shillings (UGX) 25,000 – 40,000 (US$ 7-11), depending on the provider.

The Uganda Communications Act 2013 established the Uganda Communications Commission (UCC) whose roles include to develop a modern communications sector that comprises telecommunications, broadcasting, radio communications, postal communications, data communications and infrastructure.

The Rural Communications Development Fund (RCDF) implemented by the UCC and funded by a 2% levy on licensed telecommunications operators' revenue, was established in 2003. It has since seen the establishment of numerous internet points of presence (POPs), internet cafes and ICT training centres, public payphones, district web portals, Multi-Purpose Community Tele-centres (MCT), among others.[82]

The Uganda Internet Exchange Point (UIXP) provides high-speed Internet traffic (IP traffic) exchange facilities for Uganda and external entities. It aims to reduce operational costs for ISPs, spur competition among ISPs to encourage a drop in prices for consumers, improve reliability and performance, and to create new local internet bandwidth in the local market. Currently, 24 ISPs are connected to the UIXP.[83]

---

80 UCC, 'UCC Licensing Regime', retrieved 02/03/2017, http://www.ucc.co.ug/data/smenu/88/Licensing-Overview.html and UCC, 'UCC license application guidelines', retrieved 02/03/2017, http://ucc.co.ug/files/downloads/Licence-Application-Guidelines.pdf

81 UCC, (2016), 'Post, Broadcasting and Telecommunications Market and Industry Report', retrieved 02/03/2017, http://www.ucc.co.ug/files/downloads/Market_&_Industry_Report_for_Q3_July-September_2016.pdf

82 UCC, Rural Communications Development Fund, retrieved 02/03/2017, http://www.ucc.co.ug/data/smenu/71/Rural-Communications-Development-Fund---RCDF.html

83 Uganda Internet Exchange Point, Connect Networks, retrieved 02/03/2017, https://www.uixp.co.ug/networks

3. Freedom of Expression

Article 29 (1)(a) of Uganda's constitution states that, "every person shall have the right to freedom of expression and speech which includes freedom of the press and other media."

The Penal Code establishes and defines offences related to sedition, promotion of sectarianism, criminal libel/defamation, and terrorism. Sections 34 to 36 of the Penal Code Act provide for the prohibition of the importation of publications; and give the Minister discretionary powers on the types of publications to be imported or banned in accordance with the public interest. Where periodical publications are concerned, the order may relate to all or any of the past or future issues.

Section 39 defines a seditious intention as, among other things, "to bring into hatred or contempt or to excite disaffection against the person of the President, the Government as by law established or the Constitution; (b) to excite any person to attempt to procure the alteration, otherwise than by lawful means, of any matter in state as by law established; (c) to bring into hatred or contempt or to excite disaffection against the administration of justice; (d) to subvert or promote the subversion of the Government or the administration of justice." Section 40 provides for a sentence of up to five years imprisonment.

Sectarianism is also punishable under the Penal Code for any person who prints, publishes, makes or utters any statement or carries out any act which is likely to (a) degrade, revile or expose to hatred or contempt; (b) create alienation or despondency of; (c) raise discontent or disaffection among; or (d) promote, in any other way, feelings of ill will or hostility among or against any group or body of persons on account of religion, tribe or ethnic or regional origin (Section 41). It attracts a prison sentence of up to five years.

In 2004, Uganda's constitutional court struck down the offence of the publication of false news, which it deemed incompatible with the right to freedom of expression. In 2010, the constitutional court nullified the law on criminal sedition which had been commonly used to prosecute journalists.[84]

The Computer Misuse Act 2011 broadly defines a computer, to include all types of electronic or electromagnetic systems capable of storing or transmitting data. This broad definition means that any person using an electronic or electromagnetic system has a duty to act within the confines of the Act, failure of which is one of the several offences under the Act. The broad nature of this Act was tested in Nyakahuma vs. Uganda where, in a high court referral to determine whether posting materials on the internet amounted to publication within the meaning of the Penal Code, the judge ruled that the broad nature of the Computer Misuse Act captured all forms of posts made in cyberspace irrespective of the tool used to post.[85]

---

84 IFEX News, (2010), Constitutional Court nullifies law on sedition, retrieved 02/03/2017, https://www.ifex.org/uganda/2010/08/25/sedition_law_null/

85 Uganda Legal Information Institute, 'High Court criminal reference No 1/2013', retrieved 02/03/2017, http://www.ulii.org/ug/judgment/high-court-criminaldivision/2013/30-0

Section 25 of the Act calls for the punishment of "offensive communication" where "any person who willfully and repeatedly uses electronic communication to disturb or attempt to disturb the peace, quiet or right of privacy of any person with no purpose of legitimate communication whether or not a conversation ensues commits a misdemeanour and is liable on conviction to a fine not exceeding UGX 480,000 (about US$ 140) or imprisonment not exceeding one year, or both".

In February 2015, Robert Shaka was arrested on suspicion of using the Facebook alias Tom Voltaire Okwalinga (TVO), to post corruption and incompetence-related criticisms of the president and other senior public officers. In June 2015, he was again arrested and accused of sectarianism and computer misuse under Section 25 of the Computer Misuse Act for allegedly making Facebook posts as TVO that caused or promoted hatred toward the president, his wife, and the Inspector General of Police.[86] In January 2016, former intelligence officer, now political analyst, Charles Rwomushana, was arrested and detained by police after he posted on Facebook a picture purporting to be the dead body of a bodyguard to an opposition presidential candidate who had gone missing.[87] In another incident in February 2016, police arrested two youths for allegedly inciting violence and posting a picture of a dead president.[88]

Under the Anti-Pornography Act 2014, a police officer can order a media house to stop a likely production if he/she deems the matter to be pornographic. Internet Service Providers (ISPs) may also be held liable for "not using, or enforcing the means or procedure recommended by the [government-appointed] Committee to control pornography", for permitting to be downloaded or uploaded through its service, any content of pornographic nature, and are liable on conviction to a fine of up to UGX 10 million (US$ 4,000), or imprisonment of not more than five years, or both (Section 17).

Sections 29 and 30 of the Electronic Transactions Act 2011 delineate the liability of service providers for provision of access to infringing material if the service provider is "not directly involved in the making, publication, dissemination or distribution of the material or a statement made in the material; or the infringement of any rights subsisting in or in relation to the material." Furthermore, the ISP does not bear liability if it "does not have actual knowledge that the data message or an activity relating to the data message is infringing the rights of the user; is not aware of the facts or circumstances from which the infringing activity or the infringing nature of the data message is apparent; does not receive a financial benefit directly attributable to the infringing activity; or removes or disables access to the reference or link to the data message or activity within a reasonable time

86 All Africa, 'Uganda: Who's Tom Voltaire Okwalinga - TVO?', retrieved 02/03/2017, http://allafrica.com/stories/201506100865.html

87 NTV, 'Charles Rwomushana arrested over Aine pictures', retrieved 02/03/2017, http://www.ntv.co.ug/news/crime/09/jan/2016/charlesrwomushana-arrested-over-aine-pictures-10675#sthash.QtAu1aDn.dpbs

88 Daily Monitor, 'Two arrested over 'dead' Museveni picture', retrieved 02/03/2017, http://www.monitor.co.ug/News/National/Two-arrested-over--dead--Museveni-picture/688334-3106714-11plidxz/index.html

after being informed that the data message or the activity relating to the data message infringes the rights of the user."

Section 86 subsection 1 (a) of the 2013 Communications Act gives power to the commission to "direct any operator to operate a network in a specified manner in order to alleviate the state of emergency." The regulator has on a number of occasions used these powers to issue directives to service providers to temporarily block access to certain services. In 2011, UCC directed all service providers to temporarily block access to certain services including Facebook and Twitter in fear of these social media networks being used to intensify opposition protests.[89] On Election Day in February 2016, social media platforms Facebook, Twitter and WhatsApp, as well as the popular mobile money services, were shut down on UCC's orders. Ugandans resorted to using VPNs to share information about the elections.[90] Another shutdown was ordered in May 2016, on the presidential inauguration day.[91]

4. Right to Information

The Access to Information Act, 2005 provides for the right of access to information pursuant to Article 41 of the Constitution, which states that "every citizen has a right of access to information in the possession of the state or any other organ of the state except where the release of the information is likely to interfere with the security of the state or the right to the privacy of any other person". The Act applies to information and records of government ministries, departments, local governments, statutory corporations and bodies, commissions and other government organs and agencies. However, cabinet records and those of its committees, as well as records of court proceedings before the conclusion of the case, are exempted.

Grounds for non-disclosure of information under the Act include the protection of commercial information of third parties (Section 27), the protection of certain confidential information (Section 28), the protection of safety of persons and property (Section 29), the protection of law enforcement and legal proceedings (Section 30), the protection of records privileged from production in legal proceedings and for defence, security and international relations (Section 31).

In spite of having the access to information law in place, obtaining information from government agencies is inhibited by Article 4 of the Official Secrecy Act of 1964, which prohibits public servants from disclosing information that comes to them by virtue of the offices they hold. Breach of the Act could earn a civil servant up to 14 years in prison.

---

89 CIPESA, (2014), 'State of Internet Freedom in Uganda 2014', retrieved 02/03/2017, http://cipesa.org/?wpfb_dl=181

90 Open Net Africa, 'Ugandans Turn to Proxies, VPN in Face of Social Media Shutdown', retrieved 02/03/2017, http://www.opennetafrica.org/ugandans-turnto-proxies-vpn-in-face-of-social-media-shutdown

91 CIPESA, (2016), 'Uganda Again Blocks Social Media to Stifle Anti-Museveni Protests', retrieved 02/03/2017, http://cipesa.org/2016/05/uganda-againblocks-social-media-to-stifle-anti-museveni-protests

5. Freedom of Assembly and Association and the Internet

Article 29 of the Constitution also guarantees the protection of freedom of conscience, expression, movement, religion, assembly and association; Article 38 guarantees civic rights and activities.

However, the arrests of those seen as opposition activists, such as Robert Shaka, suggests that in practice Uganda does not fully comply with the legislation it has set out.

6. Cultural and Linguistic Diversity

// Limited data available.

7. Right to Development and Access to Knowledge

// Limited data available.

8. Privacy and Personal Data Protection

The Access to Information Act 2005 provides for privacy and data protection by prohibiting "the unreasonable disclosure of personal information about a person, including a deceased individual" (Section 26). Meanwhile, the Electronics Signatures Act 2011 prohibits access to any electronic record, book, register, correspondence, information, document, other material or grant access to any other person (Section 81) except for the purpose of the Act and law enforcement.

Likewise, the Computer Misuse Act 2011 prohibits a person who has access to any electronic data, record, book, register, correspondence, information, document or any other material from disclosing to any other person or use it for any other purpose other than that for which he or she obtained access (Section 18 (1) except for the purposes of the Act and for law enforcement purposes. However, Section 28 subsection 5 (c) gives powers to an authorised officer executing a search warrant to "compel a service provider, within its existing technical capability - (i) to collect or record through the application of technical means; or (ii) to co-operate and assist the competent authorities in the collection or recording of traffic data in real time, associated with specified communication transmitted by means of a computer system."

Sections 79 and 80 of the Communications Commission Act 2013 criminalise infringing privacy and provide for the punishment of unlawful interception and disclosure of communication by a service provider. Section 28(2)(b) of the same Act prohibits any broadcasting which infringes upon the privacy of any individual.

Pursuant to the Anti-Terrorism Act 2002, the Interception of Communications Act 2010 legalises state interceptions and the monitoring of communication in telecommunications, postal or any other related system as a means of detecting and combating terrorism. Section 3 of the Act authorises the Minister of security to establish a Monitoring Centre and gives him responsibility over the administration and functioning of the Centre.

Section 5(1) provides the grounds under which an interception warrant may be issued by a designated judge to an authorised person. These include the "gathering of information" concerning an actual or potential threat to national security, public safety or to any national economic interest.

Telecommunications service providers are required by the Act to "install hardware and software facilities and devices to enable interception of communications at all times or when so required, as the case may be." Non-compliance by service providers is punishable by a fine not exceeding UGX 2.24 million (US$ 896) or imprisonment for a period not exceeding five years, or both. Non-compliance could also lead to cancellation of an operator's license.

In 2015, amendments were made to the Terrorism Act to align the law to international requirements by providing for aspects of terror financing and money laundering. The coming into force of the amendment means that the police now possess the power to conduct surveillance on online transactions with the aim of establishing if they are funding terror activities.

The Data Protection and Privacy Bill 2015 seeks to provide for the privacy of individuals and of personal data by regulating the collection and processing of personal information. It articulates the rights of persons whose data is collected including the right to prevent processing of personal data whether for direct marketing or not, rights in relation to automated decision taking and rectification, blocking, erasure and destruction of personal data. It provides measures for the security of data, redress and offences.

In July 2014, Uganda's president praised the Chinese telecommunications technology company, Huawei, for donating a multi-tracking system worth UGX 1.8bn (US$ 750,000) to the Uganda government.[92] In February 2015, the Ugandan Parliament reportedly bought UGX 28bn (over US$ 9.8 million) worth of CCTV cameras and other security measures from another Chinese technology company, ZTE.[93]

Since March 2012 mandatory SIM card registration has been enforced, pursuant to the Regulation of Interception of Communications Act (2010).[94] Although a human rights group filed a suit against the mandatory registration on the grounds that it violated constitutional guarantees on privacy, the court dismissed the challenge.[95] Meanwhile, in 2014, Uganda's directorate of Citizenship and Immigration Control announced that it would start issuing

---

92 ChimpReports, (2014), 'Huawei Donates shs1.8bn Security Equipment to Uganda', retrieved 02/03/2017, http://www.chimpreports.com/huawei-donates-shs1-8bn-security-equipment-to-uganda/

93 Privacy International, (2016), 'State of Privacy Uganda', retrieved 02/03/2017, https://www.privacyinternational.org/node/965

94 UCC, SIM Card Registration, retrieved 02/03/2017, http://www.ucc.co.ug/data/smenu/23/SIM-Card-Registration.html

95 IFEX News, (2013), 'Ugandan court declines to hear SIM card registration case', retrieved 02/03/2017, http://www.ifex.org/uganda/2013/12/19/case_closes/

biometric passports.[96] Uganda has also initiated biometric banking[97] and biometric voter registration.[98]

Anonymous communication has gained prominence in a recent case filed against Facebook in an Irish Court. In May 2016, Fred Muwema, a prominent lawyer, requested Facebook to reveal the true identity and page of TVO, so he could sue him for defamation. Muwema's request followed TVO's publication on his Facebook page that the lawyer had stage-managed an attack on his law firm and been bribed not to represent former presidential candidate Amama Mbabazi, who was petitioning the election results. Following Facebook's refusal to reveal the name and to delete TVOs page, Muwema sued Facebook in Ireland for court to grant the same orders.[99] In denying Muwema's requests, Facebook argued that the Ugandan government had previously sought the identity of TVO and that revealing it would result in increased violation to TVO and other human rights defenders using their platform in Uganda.[100] The Irish High Court ruled in favour of Facebook to protect the identity of TVO but ordered for defamatory content to be taken down.[101]

In 2015, Privacy International released a report detailing how a UK firm, Gamma International, had allegedly sold spyware to the government of Uganda to help authorities conduct surveillance on the media and political activists. The report alleges that government installed the spyware in public places such as hotels to surveil on citizens.[102] Although the government of Uganda denied the existence of spyware, there is a growing fear that the government is illegally tapping into communications.

In July 2015, reports emerged that the Uganda Police and the Office of the Presidency were in advanced stages of acquiring hi-tech surveillance software from Israel and Italy to begin large-scale spying in Uganda.[103] Information released by Wikileaks shows email exchanges between the Italian surveillance malware vendor Hacking Team and its local vendor Zakiruddin Chowdhury, who seemed to have strong contacts with senior Uganda government

---

96 Biometric Update, 'Biometric identification news from Uganda, Kenya and Nigeria', retrieved 02/03/2017, http://www.biometricupdate.com/201411/biometric-identification-news-from-uganda-kenya-and-nigeria

97 The East African, (2014), 'Ugandan banks to adopt biometric identification', retrieved 02/03/2017, http://www.theeastafrican.co.ke/news/Ugandan-banks-to-adopt-biometric-identification/2558-2235862-7cca1sz/index.html

98 VOA News, (2016), 'Uganda to Use Biometric Verification Machines for Elections', retrieved 02/03/2017, http://www.voanews.com/a/uganda-biometric-verification-machines-elections/3147994.html

99 See: Fred Muwema Vs Facebook Ireland Ltd. No. (2016) 4637P

100 Facebook, (2016), 'Government requests (Uganda)', retrieved 02/03/2017, https://govtrequests.facebook.com/country/Uganda/2016-H1/#

101 PC Tech, (2015), 'Court Allows Facebook to Protect TVO's Identity, Orders Deletion of Defamatory Content Against Muwema', retrieved 02/03/2017, https://pctechmag.com/2017/02/court-allows-facebook-to-protect-tvos-identity-orders-deletion-of-defamatory-content-against-muwema/

102 Privacy International, (2015), 'For God and My President: State Surveillance In Uganda', retrieved 02/03/2017, https://privacyinternational.org/sites/default/files/Uganda_Report.pdf

103 Defender's Protection Initiative, 'Police in Shs 5bn spy deal', retrieved 02/03/2017,, http://defendersprotection.org/?p=458

officials.[104]

9. Security, Stability and Resilience of the Internet

In 2013, UCC set up a Computer Emergency Response Team (CERT), whose mandate is to secure communication services in the country. In 2014, a Cyber Crimes Unit was set up within the Police Force.[105]

10. Marginalised Groups and Groups at Risk

In early 2014, president Museveni assented to the Anti-Homosexuality Act 2014, which prohibited any form of sexual relations between persons of the same sex. Section 13 of the law – which was later annulled – outlawed the promotion of homosexuality, including by the use of "electronic devices which include internet, films, and mobile phones for purposes of homosexuality or promoting homosexuality." The penalty was UGX100 Million (US$ 40,000) or minimum five years and maximum seven year jail sentence. Where the offender is a corporate body, association or NGO, on conviction its certificate of registration would be cancelled and its directors and promoters could be punished with seven years imprisonment. Activists argued that this clause could be used to crack down on organisational websites that worked with sexual minorities in Uganda, as well as gay and lesbian websites. Furthermore, they argued that the clause limited the ability of adult consenting LGBTI people to use mobile phones freely as, by implication, "it criminalises even flirting or making dates."[106]

Although the law was subsequently nullified by court, members of the local LGBTI community have reported ongoing malicious attacks on their email and social media accounts, theft of devices and blackmail, among others.[107]

11. Right to Due Process

Legitimate restrictions to human rights are provided for in Article 43 of the Constitution, and rights to redress may be found in Articles 42 and 50 which provide for the right to be treated justly and fairly and to apply to a court of law and for the courts to enforce human rights respectively. Accountability through the establishment of a Human Rights Commission, which reports to Parliament, is provided for in Articles 51 to 53.

12. Democratic Multistakeholder Internet Governance

Stakeholder input is often sought and incorporated into ICT related policies and regulations. In the past, this has included for the Cyber laws of 2011

---

104 Wikileaks, (2015), 'The Hacking Team - Re: R: I: Uganda Police', retrieved 02/03/2017, https://wikileaks.org/hackingteam/emails/emailid/11829

105 Uganda Police Force, 'Uganda Police Cyber Barometer', retrieved 02/03/2017, http://www.upf.go.ug/cyber-barometer/

106 GenderIT, (2014), 'Uganda's Anti-Homosexuality Bill – a great blow to internet freedom', retrieved 02/03/2017, http://www.genderit.org/feminist-talk/uganda-s-anti-homosexuality-bill-great-blow-internet-freedom

107 The Guardian, (2015), 'Gay Ugandans face new threat from anti-homosexuality law', retrieved 02/03/2017, http://www.theguardian.com/world/2015/jan/06/-sp-gay-ugandans-face-new-threat-from-anti-homosexuality-law

(Computer Misuse Act, E-transactions Act and E-Signatures Act). Also in November 2015, the Ministry of ICT called for public comments on the National Broadband Strategy.[108] In June 2016, the National IT Authority hosted a consultative meeting to get stakeholder input into the draft sector certification regulations.[109] While in December 2015, wide public consultations were undertaken on the Draft Data Protection and Privacy bill, 2015, now tabled before Parliament.[110]

However, some policies do not get enough stakeholder scrutiny. On February 26, 2016, the Minister of Information and Communications Technology gazetted the Communications (Amendment) Bill, 2016 that seeks to amend section 93(1) of the Communications Act, 2013 to enable the minister to make statutory instruments without seeking parliamentary approval.[111] The current law requires the minister to lay regulations before parliament for approval, hence the amendment would be an attempt at ousting parliamentary oversight powers.[112] The Amendment not only removes the requirement for parliamentary approval for regulations made by the minister under the Act, but also the requirement to inform parliament of the new legislation made through laying the regulations before parliament. The proposed amendment to the 2013 UCC Act, without public consideration, has been criticised as having a political motive as they give unprecedented powers to the minister to control and manage the industry, without clear checks and balances.[113]

13. Gender Equality

The ICT Policy Framework, 2003 details gender mainstreaming strategies:

a. Take into account gender information needs and interests of both men and women in all information and communication programmes.

b. Develop mechanisms of increasing women's access to information (especially in rural areas), so as to reduce the gender information gap.

c. Use non-discriminative gender sensitive language in information and communication programmes.

---

108 Ministry of ICT & National Guidance, (2015), 'Request for comments: National Broadband Strategy', retrieved 02/03/2017, http://www.ict.go.ug/media/request-comments-national-broadband-strategy

109 NITA-U, 'NITA -U Consultative Workshop for the Draft Certification Regulations', retrieved 02/03/2017, http://www.nita.go.ug/media/nita-u-consultative-workshop-draft-certification-regulations

110 See: CIPESA, (2014), 'CIPESA's Comments on the Draft Data Protection and Privacy Bill, 2014', retrieved 02/03/2017, http://cipesa.org/?wpfb_dl=184

111 Ugandan Parliament, 'Govt seeks to ammend UCC Act', retrieved 02/03/2017, http://www.parliament.go.ug/index.php/about-parliament/parliamentary-news/788-govt-seeks-to-amend-ucc-act

112 HRNJ, (2016), 'Analysis of the Uganda Communications (Amendment) Bill 2016', retrieved 02/03/2017, https://hrnjuganda.org/?page_id=2639

113 All Africa, 'Parliament should disregard UCC Bill of 2016', retrieved 02/03/2017, http://allafrica.com/stories/201603250624.html

d. Ensure equal participation in all aspects of ICT development
There have also been programmes by the regulator aimed at the recognition of women in technology.[114]

114 UCC, (2016), 'International Girls in ICT Day', retrieved 02/03/2017, http://ucc.co.ug/data/dnews/54/.html and UCC, (2016), 'UCC celebrates gender empowerment', retrieved 02/03/2017, http://ucc.co.ug/data/dnews/87/UCC-celebrates-gender-empowerment.html

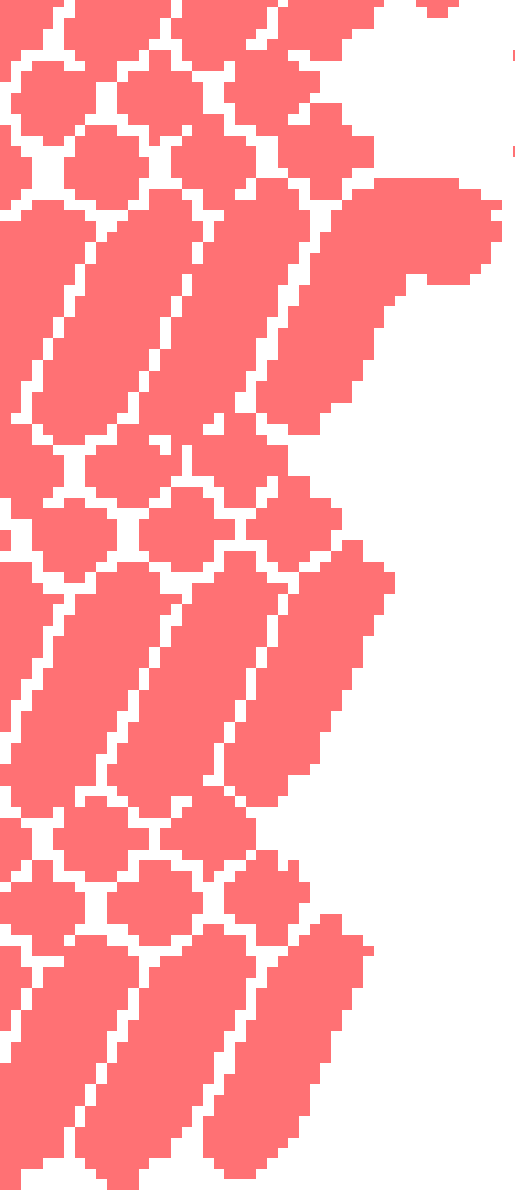
State Compliance with the African Declaration

FULL COMPLIANCE ●
PARTIAL COMPLIANCE ◎
NON-COMPLIANCE ○
NO DATA X

#	Principle	Burundi	Rwanda	South Sudan	Tanzania	Uganda
1	Openness	◎	◎	◎	◎	◎
2	Internet Access and Affordability	◎	◎	◎	●	●
3	Freedom of Expression	○	○	◎	○	○
4	Right to Information	○	◎	◎	◎	◎
5	Freedom of Assembly and Association and the Internet	○	○	○	○	○
6	Cultural and Linguistic Diversity	x	x	x	x	x
7	Right to Development and Access to Knowledge	x	x	x	x	x
8	Privacy and Personal Data Protection	◎	○	○	○	○
9	Security, Stability and Resilience of the Internet	◎	◎	○	x	◎
10	Marginalised Groups and Groups at Risk	x	◎	x	○	○
11	Right to Due Process	○	◎	x	◎	●
12	Democratic Multistakeholder Internet Governance	x	◎	x	◎	◎
13	Gender Equality	x	◎	◎	x	◎

Conclusion

All of the states assessed in our analysis have demonstrated only partial or non-existent-compliance with the majority of the principles of the ADIRF. Internet freedom advocates should work to raise the profile of the ADIRF, and encourage a wider coalition of civil society organisations to formally endorse the declaration and press their governments to do the same.



Chapter 2

Civil Society Digital Resilience

In the previous chapter of the report, we mapped the state of internet freedom across the East Africa region, and identified a number of areas in which government policies have paved the way for abuses of digital rights as set out in the African Declaration on Internet Rights and Freedoms.

In this segment of the report, we will demonstrate how these policies and practices are having a negative impact upon the ability of civil society organisations (CSOs) to operate freely and openly, thereby limiting their capacity to engage in advocacy, to hold politicians and private organisations to account, and to support their target communities.

To this end, we undertook a series of 39 interviews with CSOs drawn from Uganda, Tanzania, Rwanda, and Burundi in order to map out their digital capacities, their perception of digital threats, and their capacity to defend themselves from these threats. We also took stock of the digital security support networks that exist, and assessed the extent to which their training initiatives resulted in the dissemination of digital security knowledge and practices within an organisation's staff and across their organisational networks.

In each of the country assessments that follow, we have anonymised the names of participating organisations and interviewees. Organisation names were assigned a code based on their country of operations and a numerical value.

Note that due to the ongoing political unrest and challenging security environment in South Sudan, we were unable to undertake fieldwork to obtain on-the-ground information about the digital security challenges faced by local CSOs.

Assessing Civil Society Capacities

Our Ratings

THREAT PERCEPTION RATING

The threat perception rating is a score attributed to each country to give an impression of the extent to which local CSOs perceive threats from state and non-state actors. An explanation of our methodology is available in Annex I.

STATE THREAT PERCEPTION RATING

This score indicates the extent to which CSOs in a country are concerned about digital threats originating from state actors.

NON-STATE THREAT PERCEPTION RATING

This score indicates the extent to which CSOs in a country are concerned about digital threats originating from non-state actors, such as cybercriminals and other malicious hackers.

DIGITAL RESILIENCE RATING

This score indicates the general ability of CSOs to protect themselves against digital security threats. For more information about our methodology, and for comprehensive details of CSOs' capacities, see Annexes I and II.

GREATEST PERCEIVED THREAT

The 'Greatest Perceived Threat' is the threat that scored the highest threat perception rating in each country.

Threat Perception Ratings

Countries were attributed Threat Perception and Digital Resilience scores according to our coding methodology (available in Annex III). We attributed ratings based on these scores.

Rating	**Very Low**	**Low**	**Moderate**	**High**	**Extreme**
Score	0-19	20-39	40-59	60-79	80-100

Digital Resilience Ratings

Rating	**Very Limited**	**Limited**	**Sufficient**	**Good**	**Excellent**
Score	0-19	20-39	40-59	60-79	80-100

Burundi

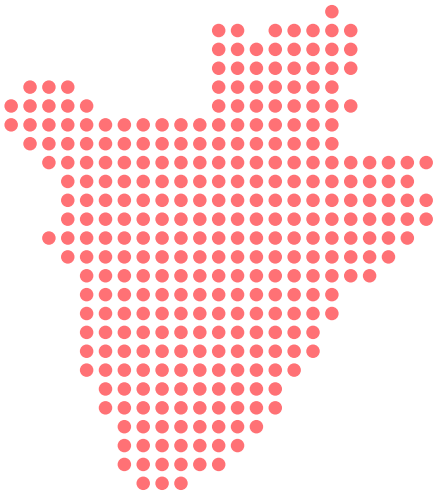
THREAT PERCEPTION RATING
33 // Low

STATE ACTORS
48 // Moderate

NON-STATE ACTORS
18 // Very Low

DIGITAL RESILIENCE
35 // Limited

GREATEST PERCEIVED THREAT
State-Directed Hacking



Burundian CSOs have faced increasing threats to their online activities. Confronted with a developing ICT landscape – as noted in Chapter 1, initiatives are in place to improve internet access and affordability – the Burundian government has begun to invest greater resources into information control measures and regulations.

Communications laws are particularly stringent, with ambiguous registration requirements for journalists. Even social media posts are theoretically regulated by the country's National Communication Council (CNC), and the Penal Code prohibits criticism of public officers. What makes this prospect more concerning is the lack of awareness that CSOs in this country have of the digital security landscape, and the means to combat internet freedom crackdowns.

Assets and Development

Of all the organisations interviewed, CSOs in Burundi are amongst the least digitally well-equipped. It is apparent that employees often use personal computers, or that there is only one computer for the whole organisation. In addition to this, funding limitations have seen some CSOs struggle to get their websites hosted securely.

Threats Identified

The most prominent threats that Burundian CSOs felt they faced were hacking, phishing and surveillance. Of these, surveillance and hacking were seen as stemming primarily from state actors. A number of CSOs actively pointed out that they were "in the sights of power",[115] due to engaging with work that sought to take a critical standpoint against the Burundian government. Interestingly, although state-actors were seen as the biggest threat, and there is a clear and systematic crackdown on freedom of expression by the state, only one organisation conveyed censorship as being an issue for them.

Hacking

State Threat Profile: **High**
Non-State Threat Profile: **Low**

Hacking was identified as the most significant threat perceived by CSOs in Burundi. Organisation 'B4', which focuses on increasing the participation of

115 B3, personal interview, 06/01/2017

civil society in politics, made it clear that hacking posed a growing threat to the protection of their information:

> *"The most important thing is information protection ... we fear the hacking of our e-mails, and illegal intrusions in[to] our computers which store our data."*[116]

'B3', a radio station, saw hacking as one of their major threats:

> *"We have received computer attacks and our site has been hacked several times. We have always faced hackers who prevent us from producing our information in the broadcast, but also in the production by [the use of] computer viruses that attack our computers."*[117]

There was also a clear belief from most CSOs that this threat came almost entirely from state actors:

> *"Our party is targeted by the government ... The security threat comes from the state, because it has driven all political parties to opposition ... The Burundian state instills terror in an attempt to frighten everybody."*[118]

> "*[The threats come from] external people who consider us today as the enemies of power."*[119]

Given the context of Burundi, and the moves by the government to increase their control over the country's digital landscape, it comes as no surprise that state threats were seen as more significant. Hacking poses a significant threat to CSOs ability to continue their work.

Surveillance

State Threat Profile: **High**
Non-State Threat Profile: **Very Low**

Burundian CSOs also identified state surveillance as a significant threat. 'B6', an organisation that works to protect the environment, described their relationship with the state:

> *"The attitude of the Burundian state towards our organisation... The relations are not good to the extent that the state does not digest our denunciation activities. We fear these state actors because they can come to see what we do ... in our organisation."*[120]

Another organisation, 'B7', which works for prisoners that are the victims of human rights violations, put the threat of surveillance into context:

---

116 B4, personal interview, 14/12/2016

117 B3, personal interview, 06/01/2017

118 B8, personal interview, 30/01/2017

119 B3, personal interview, 06/01/2017

120 B6, personal interview, 30/01/2017

> *"[The threat comes from] a state actor, because we denounce what is wrong with the country ... Imagine if you leave the house to go to the office and there is someone who knows that you are aware of them doing wrong. You understand, this makes you very uncomfortable."*[121]

'B4' explained how the relationship between the state and civil society had deteriorated, and that this was the reason that CSOs felt so threatened by state actions:

> *"These last days you know, the relationship between civil society and the government, it happens to be cold, some were targeted, and our organisation has also faced an investigation. Our bank accounts had been blocked, they had suspended them, so with all that, we thought, if things are like that, we are being monitored."*[122]

Overall, it is clear that CSOs face very real surveillance threats, primarily from the Burundian state itself. Those that saw surveillance as a threat were mostly organisations that seek to monitor state actions, and hold the government to account.

Censorship

State Threat Profile: **Low**
Non-State Threat Profile: **Very Low**

Two CSOs we interviewed were concerned by the threat of censorship from the state. 'B6' feared the overarching power of the government in its ability to keep an eye on, and thus influence, what they published:

> *"We fear these state actors because they can come here to see what we do, what we publish, what we write in our organisation."*[123]

'B9', an LGBTI organisation, have to remain highly vigilant when carrying out their work, and have come under threat of direct censorship:

> *"We were conducting a training workshop ... [and] two police officers entered the training room and checked the content of the PowerPoint slides we were using."*[124]

The threat posed to LGBTI organisations in the country is highlighted by the fact that this incident came about due to a business, whose services 'B9' declined, contacting the authorities in revenge, claiming that the organisation was preaching homosexuality.

---

121 B7, personal interview, 30/01/2017

122 B4, personal interview, 14/12/2016

123 B6, personal interview, 30/01/2017

124 B9, personal interview, 11/02/2017

Phishing

State Threat Profile: **Moderate**
Non-State Threat Profile: **Low**

Half of the CSOs interviewed saw phishing as a digital security threat. 'B10', a women's organisation, have had their emails compromised a number of times:

> *"The risks are real, the proof is the fact that some e-mail boxes have been hacked more than one time, and used by other people, criminals that we don't know."*[125]

Another organisation, 'B2', which focuses on poverty alleviation and the environment, explained that because they are not always sure if emails are legitimate or not, they are always at risk from malicious attacks:

> *"Sometimes [a suspicious email] goes through the filter and you find an e-mail talking about, or asking about our information. If you are aware enough, you realise that this could be a trick, but of course, some people can be attacked, because we never know for sure [if they are real emails]."*[126]

In March 2015, a wave of 'spearphishing' attempts (targeted phishing attacks) were launched against an array of Burundian CSOs. One such spearphishing attempt targeted an organisation working around human rights and anti-corruption initiatives. The email – ostensibly from a digital security expert – provided bogus warnings about the security of Google Mail, and attempted to direct its target to a phony 'secure' email service. The message read:

> ***Hello again,***
>
> ***It seems to me that most [people] have not received my mail. My name is Ntwari, engineer in Computer Security in Lyon in France. A friend of ---------- contacted me recently to ask for support following recent cyber attacks against members of civil society, and I would like to help you to secure your communications. So follow this link or type it directly http://----------.com. This concerns Gmail users, I will soon send you something similar for Yahoo users and other services.***
>
> ***Good courage in your struggle and have an excellent day.***

As noted, this spearphishing attempt was one amongst a wave of such attempts in early 2015.

Those CSOs reporting that they perceived phishing as a significant threat tended to lack training in digital security measures. A number of these organisations made it clear that they would be very receptive to digital security training initiatives to help them recognise phishing attempts.

---

125 B10, personal interview, 15/02/2017

126 B2, personal interview, 09/12/2016

Training and Support

Of the ten organisations interviewed in Burundi, only four had actively received digital security training. Of these four, two had then continued to pass the knowledge they had learned onto new recruits to their organisation. It is clear that among a number of organisations, there is a distinct lack of security knowledge. The employee interviewed for 'B4', who had attended a short digital security awareness workshop, explained the lack of knowledge their organisation had:

> *"I was astonished ... I didn't know, I was really below the normal level of knowledge of someone who needs to be protecting data."*[127]

Again, with only four CSOs actively engaged with other organisations that could provide training and support for digital issues, it is clear that there is not a strong network for these organisations to fall back on.

Digital Resilience

For our methodology, see Annex I

DOES YOUR ORGANISATION USE...	BURUNDI	
	SCORING	RATING
...TWO-FACTOR AUTHENTICATION	44.44%	SUFFICIENT
...EMAIL ENCRYPTION	11.11%	VERY LIMITED
...DATA ENCRYPTION	22.22%	LIMITED
...PASSWORD MANAGEMENT TOOLS	33.33%	LIMITED
...CLOUD STORAGE SERVICES	22.22%	LIMITED
..ANTI-VIRUS SOFTWARE	100%	EXCELLENT
...FIREWALL SOFTWARE	33.33%	LIMITED
...FIREWALL HARDWARE	11.11%	VERY LIMITED
RATING	**34.72%**	**LIMITED**

127 B4, personal interview, 14/12/2016

Unsurprisingly considering a lack of support networks and digital security training, only one CSO that was interviewed had an information security policy. However, a number of the organisations demonstrated a very basic level of security, with the vast majority utilising anti-virus, and some also took steps to encrypt either their emails or data.

Overall, there is a clear lack of knowledge regarding digital security tools and practices in Burundian CSOs. 'B1', an organisation that focus on youth engagement, was concerned about its level of knowledge:

> *"Our members and staff don't have [digital security] skills ... so at anytime we can get a lot of problems."*[128]

Confirming this lack of knowledge, the organisation 'B6' expressed issues with its member's digital capabilities and how this impacts their ability to keep data secure:

> *"The danger is there because we do not have enough staff [that know] how to use the internet, [and] in particular ... the security of data."*[129]

Overview

The digital security capacities of Burundi are fairly hollow. There are serious flaws in terms of the lack of security practices in place, and CSOs demonstrate low levels of digital security awareness. This can be attributed to the lack of training and support opportunities available to CSOs in the country. With the Burundian government implementing numerous measures to limit internet freedom, it is crucial that Burundian CSOs are granted access to additional training and support to help them carry out their work safely and effectively.

128 B1, personal interview, 13/12/2016

129 B6, personal interview, 30/01/2017

Rwanda

THREAT PERCEPTION RATING
30 // Low[130]

STATE ACTORS
20 // Low

NON-STATE ACTORS
40 // Moderate

DIGITAL RESILIENCE RATING
37 // Limited

GREATEST PERCEIVED THREAT
Non-State-Directed Phishing

Alongside significant economic growth, Rwanda has seen rapid development in its ICT sector in recent years, with a competitive ICT market and plenty of investment by the government. However, although more free and open than the offline landscape, the digital landscape in Rwanda is experiencing limitations on internet freedom by the government. Censorship, a key threat faced by 'offline', traditional bodies, is seeping onto digital platforms. Online news websites have seen themselves both blocked, and censored by authorities - particularly when sensitive subjects, such as elections, are being discussed.

Rwanda proved the most difficult country in the region to carry out this research. Many of the CSOs we approached ultimately refused to participate in interviews – a result we have interpreted to be rooted in a fear of reprisals against participants. Also of significance in this regard is that two of the CSOs interviewed felt too uncomfortable to answer the sections of the interview that put a spotlight on the digital threats the organisations felt they faced. Whilst we hypothesised that Rwandan CSOs would recognise a broad amount of threats, particularly from state-actors, the interviews appeared to convey that of the few threats perceived, they mainly saw non-state actors as the perpetrators.

Assets and Development

All but one of the Rwandan CSOs interviewed had either websites or social media platforms that they needed to protect from digital security threats. In addition to this, most used some form of cloud storage service. Rwandan CSOs were less likely than other countries to note that they possessed 'sensitive' data – only four out of seven reported that they had such data in their possession.

Threats Identified

As mentioned above, Rwanda stands out amongst the CSOs in other countries due to two of the organisations feeling too uncomfortable to convey the threats they perceived.

130 Assigning a threat perception rating for Rwanda has proven problematic owing to the polarisation of opinion amongst our participant CSOs. Whereas some CSOs declared that there were no state-directed digital threats, others were so fearful that they refused to give a response. As a result, these ratings should be treated with extreme caution, and may not be representative of the true picture facing Rwandan CSOs. It is also important to note that the ratings are solely based on the self-reporting of the organisations involved.

Added to this, two of the CSOs interviewed claimed that they did not perceive any risks, asserting that they did not have any sensitive data to protect. Given the context of Rwanda, we surmise that this may be due to a gap in digital security knowledge, due to the lack of key digital security support networks for these organisations. In addition, we would note that the organisations perceiving minimal threats from state surveillance and hacking operate in relatively apolitical fields such as poverty alleviation, HIV/AIDS prevention and treatment, and women's health provision. Even if these organisations are at less threat of direct government interference than human rights or media freedom-focused organisations (who recorded high threat perception, or were uncomfortable providing answers), they should be supported to recognise that they too possess sensitive data in need of protection.

In addition to this, and again due to the Rwandan context, there was an initial expectation that state threats would be the primary threat CSOs believed they faced. However, most of the CSOs we interviewed stated that they believed threats were coming from non-state actors.

Hacking

State Threat Profile: **Very Low**
Non-State Threat Profile: **Moderate**

'R3', a women's and children's rights organisation, saw hacking as the primary threat that they faced. They also believed that the hacking threat came from non-state actors:

> *"I don't think hackers can be state actors. Most of the time they are private individuals. They are trying to find information. If they want to access your information, depending on their objective they can attack you. Thus, as far as we are concerned we think hackers [are] private individuals."*[131]

'R6' also believed that hacking efforts originated primarily from non-state actors. The CSO claimed that they have a good relationship with the government, so do not fear that they would be the targets of state-sponsored hacking.

Surveillance

State Threat Profile: **Moderate**
Non-State Threat Profile: **Moderate**

Again, only two CSOs stated that surveillance posed a threat to their organisation. For 'R7', a human rights organisation, surveillance was the biggest digital threat they felt they faced:

> *"The most dangerous [digital security risk] would be communications. The interception of communications on WhatsApp and over the telephone. If someone can get your phone he will access your messages immediately. And also the internet – because if you use mobile internet it's very easy to*

131 R3, personal interview, 24/01/2017

be intercepted – or if your mobile is taken they can then access your online communications."[132]

Both 'R6' and 'R7' believed that the threat of surveillance came from both state and non-state actors. However, 'R7' did emphasise the role of the state, and also said that non-state actors will still be state-sponsored:

> *"The main reason... is because when you are defending human rights, the first person to criticise is the government. And the government sometimes takes human rights defenders as the opponents, but it is not correct. When the government cannot act it acts through someone else. An individual can be manipulated [to] serve the interests of the state – or [to serve] his/her financial interests – to cause you trouble."*[133]

R6 pointed out that given the position of Internet Service Providers (ISPs) in the country, it is likely that surveillance is carried out:

> *"[The] ISPs that give us Internet, they are under the government. They are monitored, supervised by the government which means it is really possible [to carry out surveillance]. When you look at the telecommunication operator they are monitored by the government."*[134]

Censorship

State Threat Profile: **Low**
Non-State Threat Profile: **Very Low**

Only 'R7' stated that censorship posed a threat. This primarily came down to a belief that their website was not very secure, and they thus had to carry out self-censorship:

> *"The problem is that other people can interfere and publish the information on our site. It can cause us problems. We [have to be] sure about what we publish and we are responsible... We decide not to publish some information on the internet. Some content is not put on the website - we only publish information that cannot then expose our members."*[135]

Phishing

State Threat Profile: **Low**
Non-State Threat Profile: **Extreme**

All but one CSO perceived phishing as a threat to their organisation. It was seen as primarily stemming from non-state actors and included typical attempts to glean information from the organisations, and encourage them to click on fake links.

---

132 R7, personal interview, 11/02/2017

133 *Ibid*

134 R6, personal interview, 12/02/2017

135 *Ibid*

Training and Support

Five of the seven CSOs interviewed had not received any form of digital security training. 'R6', who was one of the two that had, did not pass on the knowledge and skills learned to its new recruits. No interorganisational knowledge-sharing practices were implemented. Interestingly, 'R6' stated explicitly that this was less to do with a lack of funding than it was to do with a general lack of awareness about the importance of digital security considerations:

> *"I don't think it is the lack of funds. It is [just] not in our daily plans."*[136]

That being said, other CSOs expressed a willingness to engage with mechanisms for digital security support, though complained that they lacked the resources to effectively confront questions around digital security. In this way, 'R7' established that they did not currently have the capacity to train their staff:

> *"We don't have the means to train our staff on digital security. They are not aware ... We wish to have related trainings."*[137]

Overall, there was no support network for the CSOs in Rwanda to use to facilitate digital security training.

136 R6, personal interview, 12/02/2017

137 R7, personal interview, 11/02/2017

Digital Resilience

DOES YOUR ORGANISATION USE...	RWANDA	
	SCORING	RATING
...TWO-FACTOR AUTHENTICATION	14.29%	VERY LIMITED
...EMAIL ENCRYPTION	28.57%	LIMITED
...DATA ENCRYPTION	14.29%	VERY LIMITED
...PASSWORD MANAGEMENT TOOLS	28.57%	LIMITED
...CLOUD STORAGE SERVICES	71.43%	GOOD
..ANTI-VIRUS SOFTWARE	85.71%	EXCELLENT
...FIREWALL SOFTWARE	28.57%	LIMITED
...FIREWALL HARDWARE	28.57%	LIMITED
RATING	**37.50%**	**LIMITED**

Only one CSO had any form of information security policy and one organisation was in the process of developing one.

Whilst the vast majority of CSOs showed a poor awareness of digital security practices - other than the use of anti-virus software - one organisation, 'R1', had a very thorough knowledge of digital security tools. What makes this most interesting is that 'R1' was one of the organisations that did not feel comfortable stating what threats it perceived. A correlation could thus be inferred between the level of security practices in place and the increasing clamp-down on the digital landscape that is happening at the hands of the Rwandan government.

Overview

From low-level awareness of what needs protecting, to poor knowledge and skills in terms of tackling digital security problems, the digital security capacity of CSOs in Rwanda is worrying. The fact that Rwanda was the only country to have two CSOs refuse to answer questions establishes just how polarised the situation is in the country. Rwanda thus presents as an urgent priority for capacity building programmes.

Tanzania

THREAT PERCEPTION RATING
35 // Low

STATE ACTORS
43 // Moderate

NON-STATE ACTORS
27 // Low

DIGITAL RESILIENCE RATING
35 // Limited

GREATEST PERCEIVED THREAT
// State-Directed Hacking

Public access to ICT has been gradually increasing in Tanzania – as noted in Chapter 1, the Tanzanian regulatory authority TCRA reported a 40% internet penetration rate in December 2016 – but alongside this growth in access, Tanzanian citizens have seen increasing state-directed crackdowns on online expression. Ambiguities in existing cybercrime legislation allow state bodies to carry out censorship and surveillance without proper and independent judicial oversight. As noted in Chapter 1, one of the most significant threats to Tanzanian internet freedom originates from the 2015 Cybercrimes Act, under which numerous netizens have suffered arrest and prosecution. This segment will explore the implications of such policies upon CSO activity in the country.

Assets and Development

All but one Tanzanian CSO we surveyed had both websites and social media platforms that they sought to protect from digital security threats. All of the CSOs surveyed acknowledged that they were in possession of sensitive data that required protection.

Threats Identified

CSOs in Tanzania were concerned about a number of threats. Across the twelve organisations interviewed, there were concerns that their internal systems and networks were susceptible to hacking attempts from both state and non-state actors. There was also significant concern from CSOs that Tanzania's 2015 Cybercrime Act provided the state with overarching powers to surveil and censor their content and communications. The threat posed by phishing also proved to be a point of concern for organisations in the country.

A number of CSOs expressed dismay over the limited digital security awareness of their partner CSOs, and – as our interviews make clear – whilst there is certainly a developing understanding of digital threats in Tanzania, more needs to be done to educate CSOs about the importance of maintaining rigorous digital security standards.

Hacking

State Threat Profile: **High**
Non-State Threat Profile: **Moderate**

CSOs in Tanzania were primarily concerned about hacking – from both state and non-state actors. Organisation 'T9', who, amongst other things, carries out work to encourage transparency and advocates for freedom of

information, was concerned that the state could be targeting them:

> *"I think, there is such a possibility [that hacking could be done by state actors], especially in public institutions, maybe we touched their interests..."*[138]

Another organisation, that also focuses on governance and transparency, made it clear that hacking is an issue of high concern:

> *"We are not safe at all. For example, our email was hacked almost three times. And, last time ... [our email] was totally closed, they hacked it."*[139]

Whilst there was a strong concern among CSOs – particularly those that put a spotlight on government activities – that the state was actively targeting them, with the perceived threat of non-state hacking sitting at 50%, there was also a recognition of threats coming from non-governmental sources. Interestingly, one organisation even expressed concerns about the digital security threats posed by other CSOs:

> *"I am worried because sometimes ... we as local NGOs we are competing... You know these kind of offences can happen here in Tanzania by your own colleagues... different CSOs getting our proposal and information so they can also bid [for] them and get the tender."*[140]

Organisations were also concerned about their online platforms being exploited by individuals seeking to plant advertisements. 'T12', an organisation focusing on empowering women, was concerned about the possibility of false phishing advertisements being placed on their website:

> *"Nowadays, they hack so that they can chip in their advertisements, so if you don't manage your website carefully, you might find that there are some links that were put there by the hackers, so as to do advertisements."*[141]

CSOs in Tanzania saw malicious hackers as posing a significant risk to their organisation and their work. Consequently, we would note that CSOs in Tanzania require additional support to help them feel confident in the resilience of their systems against such attacks.

Surveillance

State Threat Profile: **Moderate**
Non-State Threat Profile: **Very Low**

There was worry among a number of the CSOs concerning the surveillance powers of the state, particularly in the light of recently developed legislation. Organisation 'T3', which focuses on youth advocacy, highlighted Tanzania's

138 T9, personal interview, 28/01/2017

139 T10, personal interview, 27/01/2017

140 T6, personal interview, 31/12/2017

141 T12, personal interview, 03/02/2017

Cybercrime Act as being particularly problematic:

> *"There are new laws that passed ... they deny us freedom of expression because the right to expression is granted from the moment of birth ... therefore these laws hinder [us]; you might want to express yourself but you [end up] fearing [doing so]. Or, if you express yourself, there are some things you can't say."*[142]

This testimony makes clear the relationship between surveillance that takes place in Tanzania and the self-censorship that organisations practice to protect themselves. This pervading sense of paranoia was emphasised by 'T11', a CSO that provides capacity-building services at the local level, who was so concerned by the levels of surveillance that they chose not to disclose organisational information to any of their contacts:

> *"You cannot trust a state person enough to keep secret[s], or [either] trust someone who is not a part of the state."*[143]

And although some organisations felt they had a constructive relationship with the government, these organisations make clear that this close relationship is conditional upon their 'direction of travel' aligning with that of state interests:

> *"Our government is so strict, but in spite of all that since we have managed to have a good relationship with them... they might give us a warning or alert that the direction that we are going isn't safe for our sustainability."*[144]

As established in our policy analysis, Tanzania's government has the legal means to intrude on the privacy of CSOs, so it is unsurprising that there is concern amongst these organisations that the government is doing just that. Support should be provided to CSOs to increase their confidence to communicate free from interception and surveillance.

Censorship

State Threat Profile: **Low**
Non-State Threat Profile: **Very Low**

Although the overall threat perception for censorship is low, there was still a concern among CSOs that censorship practices posed a threat to their organisation's work. 'T3' saw new laws that the government had imposed as a threat, stating that their strict measures required forms of self-censorship on top of the censorship taking place at the state-level:

> *"These laws hinder [you], you might want to express yourself but you end up fearing [for yourself]. Or if you express yourself, there are some things that you can't say. Hence, there are many things on social [media] networks that you can't do. And, if you give out data, you must make sure*

142 T3, personal interview, 15/12/2016

143 T11, personal interview, 31/01/2017

144 T7, personal interview, 10/01/2017

there is a person who gave you such data and he/she approved it."[145]

'T7' had directly experienced censorship

> *"There was a day when we aired some information – it was evidence-based. When we were about to air the information, people from the government came and asked about the information we were about to air, and if it was relevant and true. They asked why we didn't invite them so they could be present during the airing of the information, and why [we] hadn't shared the information with the government first."*[146]

Given the high-profile and heavy-handed implementation of legislation such as the 2015 Cybercrimes Act, it is perhaps surprising that more of the CSOs surveyed did not consider the threat of censorship to be particularly high. We would note that the organisations that did view censorship as an issue of concern were by and large those whose activities could have been considered 'antagonistic' to certain state actors – namely, with regard to anti-corruption campaigns and initiatives to support political freedoms.

Phishing

State Threat Profile: **Moderate**
Non-State Threat Profile: **Moderate**

In addition to censorship, hacking and surveillance, a significant minority of CSOs expressed concerns about the dangers posed by phishing. Again, this threat was perceived as coming from both state and non-state actors, and CSOs were concerned that phishing attempts could not only damage the infrastructure of their organisation, but also its reputation as a CSO:

> *"I once received messages [emails] from my friends saying they are in Nigeria, they are stuck, they need help with a certain amount of US dollars and so on, but it was just a hacker. So they might destroy your name of your business in that way."*[147]

Whilst phishing is a fairly universal threat, it has the potential to significantly undermine the work of CSOs in the country. Phishing was seen as a threat to not just organisational finances, but also to the digital infrastructure of the organisations themselves.

Training and Support

Training support: **Good**
Internal knowledge transfer: **Limited**
Community knowledge transfer: **Very limited**
Access to support networks: **Sufficient**

Just over half of CSOs surveyed have received some form of digital security

145 T3, personal interview, 15/12/2016

146 T7, personal interview, 10/01/2017

147 T11, personal interview, 31/01/2017

training, with half of these also transferring the skills and knowledge they had received onto new recruits. Challenges remain in supporting the dissemination of digital security knowledge between CSOs, with only one organisation communicating the findings of their trainings to their partners. We would also note that although seven of the twelve CSOs surveyed had a relationship with other organisations that could provide digital security support in an emergency, this still means that five CSOs felt they had no-one to turn to in the event of an emergency.

A number of participating organisations expressed concerns about the poor state of their digital security knowledge. 'T1', an organisation focusing on enhancing accountability in public finance management, stated that:

> *"When it comes to digital security, the main concern that we're having here is [that] most of the staff have – like almost all of the staff – do not have digital security knowledge; that is a very big concern because... sometimes we don't know how the information is handled."*[148]

'T10' confirmed the lack of digital security awareness amongst Tanzanian CSOs:

> *"People are not aware [of surveillance], I mean they don't see it as a problem [or] how they are affected by it. They just think it's business as usual when there [are] incidents of surveillance. It only shocks them when they are arrested and detained and start to wonder how they were breached."*[149]

There are a variety of urgent needs within Tanzania's digital security landscape. Whilst there are a number of organisations that have received training, and continue to provide training to members of their organisations, there is also a significant gap in digital security knowledge within a large segment of civil society. Work should be carried out to fill these knowledge gaps, and more generally to raise CSOs' awareness of the potential consequences of failing to consider digital threats.

148 T1, personal interview, 22/12/2016

149 T10, personal interview, 27/01/2017

Digital Resilience

DOES YOUR ORGANISATION USE...	TANZANIA	
	SCORING	RATING
...TWO-FACTOR AUTHENTICATION	16.77%	VERY LIMITED
...EMAIL ENCRYPTION	25%	LIMITED
...DATA ENCRYPTION	33.33%	LIMITED
...PASSWORD MANAGEMENT TOOLS	0%	VERY LIMITED
...CLOUD STORAGE SERVICES	58.33%	SUFFICIENT
..ANTI-VIRUS SOFTWARE	91.67%	EXCELLENT
...FIREWALL SOFTWARE	33.33%	LIMITED
...FIREWALL HARDWARE	25%	LIMITED
RATING	**35.42%**	**LIMITED**

Overall, the digital security capacities of Tanzanian CSOs are limited. Generally speaking, CSO digital security practices seem to start and end with anti-virus software. Few organisations demonstrated a comprehensive working understanding of digital security tools and practices. However, some organisations have received digital security trainings that equipped them with an array of digital security tools – staff members just don't know how to use them. 'T10' best demonstrates this challenge:

> *"I have not received education on how to use [digital security tools]... that is why I usually ignore them all."*[150]

The lack of internal organisational knowledge transfer within CSOs was apparent when discussing basic practices such as two-step verification. Although a number of organisations had received training, when quizzed on two-step authentication a number of CSO Directors did not even know what it was, highlighting the need for organisational-level involvement in digital security trainings.

150 T3, personal interview, 15/12/2016

Equally, whilst others had been trained to use password management software, such as KeePass, they did not then start using it in the day-to-day running of their respective organisations. Additionally, whilst some had an awareness, they did not have trust in the practice, as illustrated by 'T7':

> *"We change [passwords] manually. The reason is that we are worried to use a password that is saved in the internet directly. Because after receiving training we realised that putting our passwords online is risky, since we are not sure [about] password management sites/software and how effective they are at keeping you safe out there. So we think [the] manual management of passwords is more safe."*[151]

In terms of tackling hypothetical digital threat scenarios, there were mixed responses from CSOs. Whilst 'T3' had never been hacked, they stated they have a strong support network to fall back on if it were to happen:

> *"If this happens, we are not working alone, we work with various networks, and we believe that they have experts who would assist us."*[152]

Other organisations, such as 'T11', simply said that they "wouldn't know what to do" if faced with their social media or e-mail accounts being hacked, reflective of a need to increase the digital security capacity of CSOs in the country.[153]

Overall, it is clear that whilst there is a basic knowledge base from which a number of CSOs work, there is still much that needs to be done in terms of digital security practices amongst these organisations.

151 T7, personal interview, 10/01/2017

152 T3, personal interview, 15/12/2016

153 T11, personal interview, 31/01/2017

Overview

Overall, the digital security capacities of Tanzanian CSOs are somewhat developed, although a lot of work is required to ensure that CSOs are truly aware of the nature of the digital security challenges they face, and to encourage them to enforce digital security policies in their organisations.

What is most obvious is that even though there is a training and support network developing, there is a need to ensure that there is sustained engagement between training providers and CSOs to guarantee the implementation of key practices on an organisational level. Even though a number of CSOs have members that have received digital security training, they frequently fail to transfer the skills and knowledge they gain onto their colleagues.

Uganda

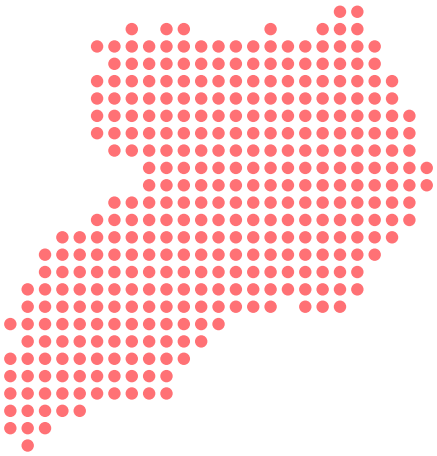
THREAT PERCEPTION RATING
56 // Moderate

STATE ACTORS
73 // High

NON-STATE ACTORS
40 // Moderate

DIGITAL RESILIENCE RATING
44 // Sufficient

GREATEST PERCEIVED THREAT
// State-Directed Surveillance



Ugandan civil society faces an array of substantial digital security threats. As noted in Chapter 1, documents published by both Wikileaks and Privacy International have suggested that Ugandan authorities have been intensifying their efforts to obtain spyware and surveillance equipment in recent years. In a demonstration of its willingness to deploy information controls, access to popular social media platforms was blocked in the run-up to the 2016 elections (and during the May 2016 inauguration), thereby stifling free expression and access to information during a period of critical debate.[154]

In such a context, we were curious as to the impact upon the daily activities of civil society actors. Our research team engaged with ten Ugandan CSOs to ask them about the threats they face, the digital security support they receive, and the threat mitigation practices they currently implement.

Assets and Development

Generally speaking, Ugandan CSOs demonstrated a relatively high level of technical development compared to organisations in the other countries studied. Although "U2" – an LGBTI rights organisation based outside of the capital – had lost the majority of its equipment after the closure of its offices (and could not replace it owing to a lack of funding), all other organisations demonstrated a moderate level of digital activity, with all operating both websites and social media pages. All organisations recognised that they worked with sensitive data that required protection.

Threats Identified

CSOs in Uganda were concerned about a variety of digital security threats arising from both state and non-state actors. Various organisations noted that they were concerned about, or had been victims of hacking attempts on their email accounts and internal networks, that they had been targeted by phishing emails, and that they feared their activities were being surveilled by authorities. A number of CSOs also spoke about the challenges they faced as a result of state censorship of online content.

The high levels of CSO awareness regarding state surveillance, phishing, hacking, and censorship constitute the most striking feature of the threat landscape in Uganda. This is not necessarily to say that the digital security

154 Freedom House, (2016) 'Freedom on the Net 2016: Uganda', retrieved 02/03/2017, https://freedomhouse.org/report/freedom-net/2016/uganda.

threats in Uganda are far more urgent or severe than they are elsewhere in the region, but rather that civil society is particularly well-educated about the dangers that exist. The February 2016 internet shutdown was an incident highlighted in a number of our interviews, and appears to have contributed to many CSOs' comprehension of the information control capacities of the Ugandan government.

Hacking

State Threat Profile: **High**
Non-State Threat Profile: **High**

The danger posed by malicious state and non-state hackers was another threat identified by Ugandan CSOs. The risks identified range from the vandalisation or deletion of organisational websites, attempts to raid funds from online accounts, and the seizure of sensitive personal data from electronic devices or cloud storage.

The ICT Manager of "U1", a media freedom organisation, described how malicious attacks are an ongoing threat to the organisation's online presence:

> *"One time our website was hacked into... and everything was deleted from the website.... Also –and it's still happening – someone, like at around 3:00AM in the night, is trying to tap into our network and... always I come in the morning and find there is an authentication error on our network... [meaning that] someone is trying hard to tap into our network."*[155]

However, the organisations expressing the greatest fears about hacking were those working to defend Uganda's vulnerable LGBTI community. In addition to concerns over hackers gaining access to their financial records and intercepting donor funding, LGBTI organisations were deeply alarmed at the prospect of the personal information of their members and beneficiaries falling into the wrong hands. There was a general fear that non-state actors might use such information to either 'out' LGBTI Ugandans or engage in blackmail, or that the state might use such information to persecute individuals under the existing Penal Code.

LGBTI organisation "U7" described how the threats of hacking attempts hang over their daily activities:

> *"[The greatest threats are from people] 'outing' [us] – you know about these media outings... mostly it is hacking that is our biggest fear... Hacking comes [alongside] media outing... people out people because they have gotten information about them, and that normally happens when people hack people's Facebooks accounts and emails – sometimes taking information about you as an individual, but [sometimes] even as an organisation. You know sometimes [the] media will just share personal [or] organisational information with the world.*
>
> *[This] also leads to attacks, because... sometimes you live in the closet*

155 U1, personal interview, 14/12/2016

and people get to know who you are, and that will lead to attacks [and] cyberbullying – that happens all the time."[156]

Surveillance

State Threat Profile: **Extreme**
Non-State Threat Profile: **Moderate**

Our interviews with CSOs in Uganda suggested that state surveillance was an issue of which effectively all civil society actors are keenly aware. Every single CSO we spoke with alluded to concerns about state surveillance capacities, with many offering detailed explanations as to how surveillance impacts on their work on a daily basis. The chairman of the media freedom organisation 'U3' stated:

He went on to describe the negative effect such surveillance capacities have upon his organisation's work:

> *"These risks have a psychological effect, because if you know that someone is snooping on you, or potentially watching you, you are not going to fully harness the potential provided by online means [of communication]... there is a chilling effect. This causes self-censorship, and that [defeats] the very logic of being able to use online platform[s] for open discussions."*[157]

Another organisation "U5" – an anti-corruption organisation working also to support women's rights initiatives – reported similarly that surveillance was a fact of life in their daily work. Their director recalled one incident that was revealing of the levels of government scrutiny they were under:

> *"[I] once met someone who I knew was a security operative, and he was telling me how we had recently signed a contract. He seemed to have very good details of the contract we had signed with [our donor] – not very detailed, but he seemed to have a clear understanding of what we had done."*[158]

The IT officer of "U6", an organisation working on accountability and anti-corruption efforts, echoed these concerns, and stated that citizens' right to privacy was being violated as a consequence of Uganda's overbearing intelligence apparatus:

> *"Of course my right to privacy is gone... if I know I cannot talk to you and have a phone conversation without someone listening in – I'm not saying they are always listening into everyone's phone conversation – but if they are interested in a particular party, they have the equipment and ability to do it..."*[159]

---

156 U7, personal interview, 29/01/2017

157 Ibid

158 U5, personal interview, 03/02/2017

159 U6, personal interview, 06/02/2017

Ugandan CSOs perceive surveillance as a significant threat to their work, with many organisations operating under the impression that their online activities are being monitored. As we note in our policy analysis, such fears are far from unfounded.

We would also note that LGBTI organisations in Uganda do not just fear surveillance from the government – some also fear that their activities are being monitored by non-state actors who oppose their work defending LGBTI rights. The LGBTI organisation "U2" noted:

> *"We are too sensitive sometimes [about] the people who like our page, because there are some who just want to spy on our work... sometimes we limit the people who like our page, otherwise we have no other avenues [to defend ourselves]."*[160]

On this evidence, we would note that addressing the privacy concerns of Ugandan CSOs should be a key priority for any future capacity-building efforts in the country. It is essential that civil society can operate with the knowledge that their practices protect them from the snooping of both the intelligence and police services, and of vigilantes and blackmailers.

Censorship

State Threat Profile: **High**
Non-State Threat Profile: **Low**

Ugandan CSOs also broadly recognised that the government has the power to censor online content that it deems to be 'unlawful' – seven of the ten CSOs we interviewed in Uganda noted that state censorship was a concern, a figure far higher than we observed in the other countries in this study. In practice, our technical analysis was only able to demonstrate the filtering of websites containing pornography, gambling, and other 'morality'-related topics. That said, our analysis was also unable to identify any filtering of LGBT-related online content – sometimes vulnerable to censorship on the pretext of removing 'immoral' content.

The media freedom organisations "U3" notes that the government began implementing online content censorship at the turn of the millennium, when the anti-Museveni website Radio Katwe was filtered. "U3" hints that the state's recent efforts to engage in 'internet shutdowns' during periods of political unrest mark a clear escalation:

> *"Of course [the government censors websites], we have had instances that go way back as early as around the year 2000, there was an online website called Radio Katwe, there was an attempt to block it, more than 10 years ago. That shows you that already there was an attempt to stifle online presence. Again there was a journalist called Timothy Kalyegira was arrested – he had an online website called Uganda Record – he published some information and he became the first guy to be charged for his digital activity. Then also during the walk to work protests, there was an*

160 U2, personal interview, 18/01/2017

interference in internet service providers from the Uganda Communications Commission. Then more recently during the February elections. This is a very clear indication of interference."[161]

The LGBTI organisation "U7" echoed these concerns, stating that their organisation's activities have been directly impacted by the government's censorship policies. Interestingly, "U7" perceives the government to be pursuing such censorship policies less aggressively now than they had in the past:

> *"Sometimes our website is blocked. There was a document that was pulled down – a human rights violation report that was pulled down – but that was sometime back... now I think [the] government has become a little more liberal."*[162]

Although censorship remains a high concern for local CSOs, our network analysis was unable to substantiate claims that civil society is being targeted directly by the state (see Chapter 3 for more details). All the same, the majority of CSOs surveyed in Uganda expressed fears about the potential for the government to censor online content. The high-profile internet shutdowns during the 2016 presidential elections and inauguration were clear demonstrations of the Ugandan government's ability to use its powers over Uganda's internet infrastructure to restrict online communications. As a consequence, there is a widespread perception that the government is willing and able to limit online expression where it is deemed problematic for authorities, even if there is limited evidence that such targeted content censorship is taking place.

Phishing

State Threat Profile: **Moderate**
Non-State Threat Profile: **Moderate**

Out of all the hacking threats that were identified by Ugandan organisations, phishing was one of the most frequently cited dangers. A number of organisations reported that their email accounts had been hacked into using phishing, and the majority mentioned that they received suspicious phishing emails on a fairly regular basis, to the extent that they have developed and implemented organisational procedures to handle such emails.

Anti-corruption organisation "U6" described their practices in detail: Organisations in Uganda were generally well-aware of the dangers of phishing, and had solid practices in place for dealing with suspicious emails. Nonetheless, local CSOs must remain vigilant about increasingly sophisticated phishing techniques, and should be provided with briefings and updates as new threats emerge.

161 U3, personal interview, 20/01/2017

162 U7, personal interview, 29/01/2017

Training and Support

Training support: **Excellent**
Internal knowledge transfer: **Good**
Community knowledge transfer: **Limited**
Access to support networks: **Excellent**

Out of all the countries surveyed, Ugandan CSOs had the best access to digital security training and support. Nine of the ten organisations surveyed had received specialised digital security trainings from local digital security providers. Similarly, CSOs in Uganda also have access to the best support networks of digital security providers. All ten of the CSOs interviewed noted that they were connected with networks that provide digital security support.

The main challenge areas that we were able to highlight were those of knowledge transfer – both internally within organisations, and between CSOs. Although six out of the ten CSOs explained processes to disseminate digital security knowledge within their organisations, there is more work to be done to ensure that digital security trainings have an impact upon the practices of entire organisations, and not just staff members tasked with ICT management. Similarly, only two CSOs noted that they had imparted their digital security knowledge onto other CSOs in their networks – a better record than in other countries, but evidently the potential for CSOs to themselves support digital security knowledge dissemination remains largely untapped.

Also, we would emphasise that the delivery of digital security training and support must be provided on an ongoing and regular basis. This theme was picked up upon by the Director of "U3" who noted:

> *"I think digital threats online are continuous, and the threats manifest themselves differently and keep changing because of the evolving nature of technology. So if you came today and said 'Okay, these are the threats', after six months another threat may have emerged – or even after a day."*[163]

Given the extensive digital security challenges faced by Ugandan CSOs, it is encouraging that the digital security support landscape is favourable here when compared to other countries in the region. Digital security trainers should continue to develop strong relationships with CSOs, and consider intensifying efforts to ensure that the practices taught are adopted on an organisational basis.

Digital Resilience

Likely as a result of the widespread provision of digital security training described above, Ugandan CSOs demonstrated the most consistent and widespread adoption of digital security tools and threat mitigation techniques out of the countries studied. That said, the digital security capacities of Ugandan CSOs remain patchy, and the limited implementation of email and data encryption, and the near-non-existent adoption of password management tools demonstrates that there is a great more work to be done

163 U3, personal interview, 20/01/2017

to ensure that local CSOs implement the recommendations provided to them at trainings.

DOES YOUR ORGANISATION USE...	UGANDA	
	SCORING	RATING
...TWO-FACTOR AUTHENTICATION	50%	SUFFICIENT
...EMAIL ENCRYPTION	20%	LIMITED
...DATA ENCRYPTION	30%	LIMITED
...PASSWORD MANAGEMENT TOOLS	10%	VERY LIMITED
...CLOUD STORAGE SERVICES	80%	EXCELLENT
..ANTI-VIRUS SOFTWARE	80%	EXCELLENT
...FIREWALL SOFTWARE	60%	GOOD
...FIREWALL HARDWARE	20%	LIMITED
RATING	**43.75%**	**SUFFICIENT**

The Chairman of "U3" noted that an organisation's consideration of digital security challenges is not often something that frequently comes at the beginning of its lifecycle – infrastructure and assets are often accumulated before threat mitigation methods are considered and put in place. Describing his own organisation's situation, he noted:

The same individual also expressed a desire to implement additional threat mitigation techniques – namely email encryption – but stated that a lack of technical knowledge posed a barrier:

> *"I have been wanting to encrypt emails but technically I haven't figured out how – but I would want to use [it] a lot."*[164]

The IT Officer at "U1" also expressed concerns that security measures such as encryption were too technically challenging for some members of staff, and that this knowledge gap posed a serious obstacle to the uptake of email encryption on an organisational basis:

164 Ibid

> *"They find it hard. I think they haven't had enough training on how to use email encryption, so they find it hard to use... and then also, the way encryption works – because they don't have so many contacts that they can share encrypted emails with – that also limits them from adopting the encryption of emails."*[165]

Similarly, "U7" expressed some concern that although they were equipped with digital security tools, they did not know how to use them properly, and therefore felt that they were ineffective:

Based on the content of our interviews with Ugandan CSOs, we would note that there appears to be a strong understanding of the importance of maintaining high standards of digital security, and a general awareness of the tools and practices required. Yet a clear implementation gap remains, and as a consequence we would recommend that CSOs be supported to overcome their technical anxieties about digital security tools and practices, and that staff members at all levels of these organisations be encouraged to consistently implement these measures.

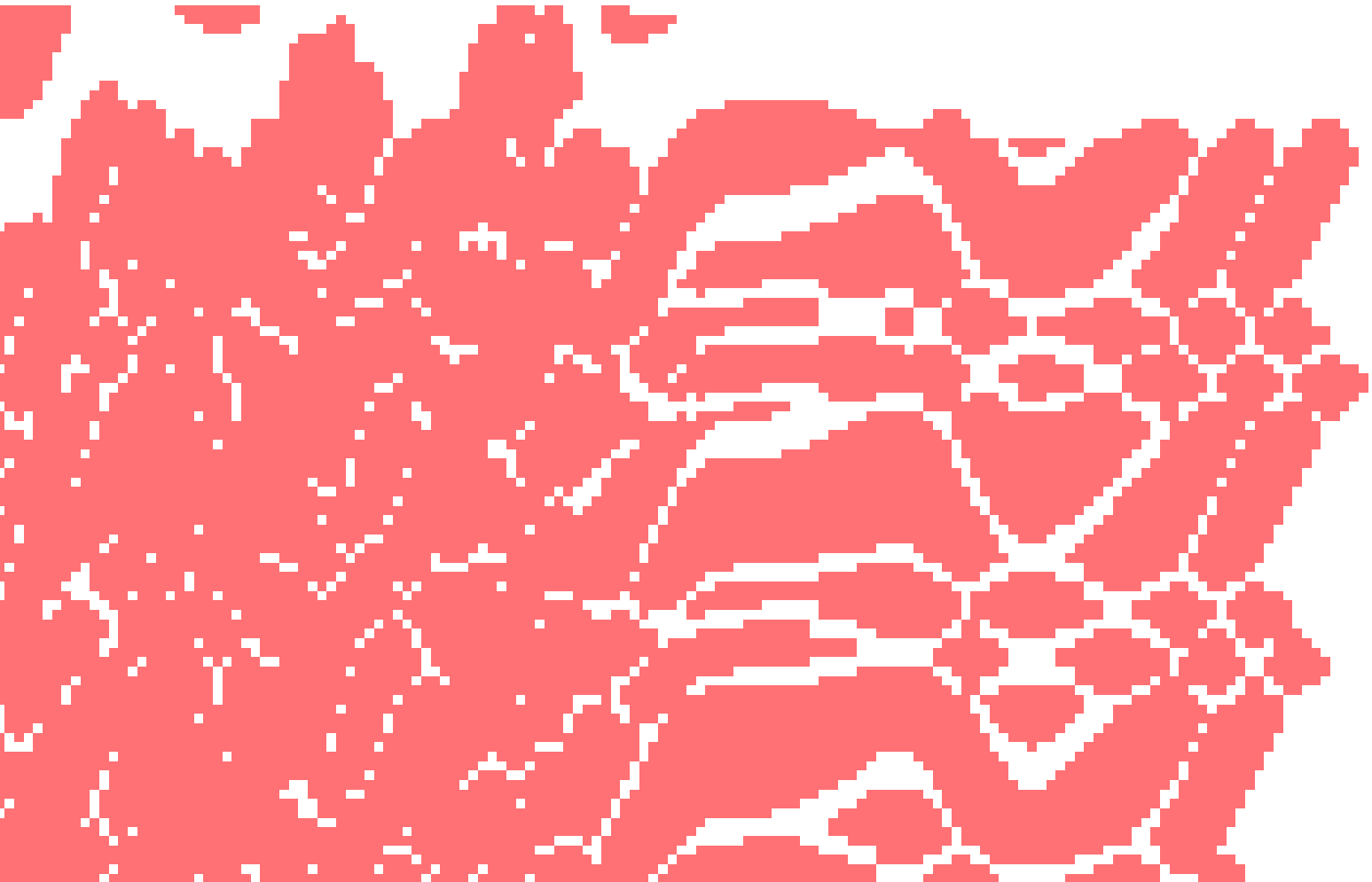
Overview

Ugandan CSOs operate in a particularly challenging security environment in which surveillance is widespread, and the government has extensive influence over the country's internet infrastructure. As a consequence, civil society has been forced to become keenly aware of the risks that may arise from unsecured communications and lax digital security infrastructure.

Although Ugandan CSOs operate in a challenging landscape of digital threats, we would note they enjoy levels of digital security support and networking unparallelled in the other countries in this study. Further development in this area should seek to support CSOs to share digital security tools and knowledge within their organisations and their broader organisational networks, and to ensure that practices are implemented in a systematic fashion by staff.

165 U1, personal interview, 14/12/2016

Chapter 3



Network Measurements

This section seeks to investigate the relationship between physical internet infrastructure and internet freedom in Burundi, Rwanda, Uganda and Tanzania. Physical internet infrastructure is used here to mean the networking layer of the internet connecting end users in these countries to the global ecosystem from national gateways, exchange points and service providers.

We aim to ascertain whether the organisation of the existing infrastructure facilitates government authorities to engage in information controls on the internet through censorship, communication interception, surveillance, or intentional shutdown of internet connectivity.

Using the network-monitoring tools OONI Probe and Centinel on selected ISPs in the four countries, we tested for censorship and surveillance for 90 days between 1 December 2016 and 28 February 2017.[166] For more information on our methodology, see Annex IV.

From the data collected, we can infer that the extent of information controls online in the four countries appears inclined more towards the possibility of surveillance and less towards censorship. Incorporating existing literature on information controls on the internet in the region, the conclusion we draw is that as the penetration of internet increases in a country, there is a relative increase in surveillance and relative decrease in censorship.[167] There is no significant statistical correlation demonstrating that government-owned ISPs engage in censorship more frequently than non-government-owned ISPs. We assume this to be related to the fact that in all four of the countries studied,

166 OONI, 'New OONI tests examine the blocking of WhatsApp and Facebook Messenger', retrieved 07/03/2017, https://ooni.torproject.org/post/whatsapp-and-facebook-tests/

167 Citizen Lab, Global Test-Lists, retrieved 07/03/2017, https://github.com/citizenlab/test-lists/blob/master/lists/global.csv and Citizen Lab, Bi Test-Lists, retrieved 07/03/2017, https://github.com/citizenlab/test-lists/blob/master/lists/bi.csv

government-owned ISPs have the lowest number of subscribed users.

This chapter is divided into two main sections. The first section documents confirmed evidence of existing information controls in a number of selected networks across the four countries studied (as noted earlier, field work could not be carried out in South Sudan). The second part of this chapter offers a brief comparison of the types of information controls implemented across the four countries, and proposes recommendations to limit Information controls and support digital rights across East Africa.

Network Measurements Overview

Using the data collected, we classified the findings to get a better understanding of how information controls in the research countries compare. The *Websites Blocked* column captures the total number of websites that are unavailable on the networks tested during the research period. The *Middle-Boxes Discovered* column is the cumulative instances in which we detected internet traffic manipulation tools on the tested networks.

TABLE 1
Summary of the information controls observed on the internet in Burundi, Rwanda, Uganda and Tanzania between 1 December 2016 and 28 February 2017 on ICLAB & OONI platforms.

Country	Websites	Boxes
Burundi	0	0
Rwanda	9	0
Uganda	0	3
Tanzania	0	1
Total	**9**	**4**

Burundi had no recorded website blockages while Rwanda had the highest number of blocked websites which additionally were notable for their political nature. It is important to note that some websites that appear blocked as per our tests may be available on other networks that were not tested.

Uganda and Tanzania had middle-box equipment detected on the networks tested (3 and 1, respectively). The fact that our research did not detect middle-boxes in Burundi and Rwanda does not mean that there is no traffic manipulation on the networks in the two countries, only that none were found through our current methodology.

What is a Middle-Box?

A middle-box is a tool deployed by network managers to inspect incoming traffic and – based on its nature – decide how to treat it. This may be used for good or bad, depending on existing access policies.[168] A case in point would be a university limiting access to pornography on their network – all traffic on their network passes through the middle-box for inspection (thereby surveilling users). If it is non-pornographic, it would be allowed to proceed to its final destination, but if it is pornographic it would be terminated (thereby censoring use). Decisions about which content to terminate or tolerate is a network management issue, opening it to abuse by governments or corporates that may want to censor content deemed unfriendly.

168 For more on Middle-Boxes, see, among other resources, Middleboxes: Taxonomy and Issues. B. Carpenter, S. Brim. February 2002

Burundi

TABLE 2
Networks tested in Burundi

Network	Ownership
Econnet-Leo	Private
Lacel	Private
Viettel	Private
Onatel	Government
Spider Net	Private

None of the 1,258 websites tests on web connectivity showed signs of censorship. Two messengers were also tested - WhatsApp and Facebook Messenger - and for the duration of the research, none presented any anomalies.[169] In addition to this, traffic manipulation tests run during the testing period did not present any evidence of tampering.

These results, as indicated in our methodology in Annex IV, are limited to tested networks, test times, and the test lists used.[170]

There have been documented incidences of blocked websites in Burundi in the past, but the tests run did not pick this up, inferring that they are no longer blocked – during the 2015 political protests, the websites of Radio Publique Africaine (RPA) and Inzamba News were inaccessible and the building hosting the RPA station was burned down, alongside its signals being cut off.[171] These websites are currently being used to collect content from journalists whose media outlets were also shut-down after the May 2015 political protests.

169 OONI, 'New OONI tests examine the blocking of WhatsApp and Facebook Messenger', retrieved 07/03/2017, https://ooni.torproject.org/post/whatsapp-and-facebook-tests/

170 The list of all tested websites is available here: Citizen Lab, Global Test-Lists, retrieved 07/03/2017, https://github.com/citizenlab/test-lists/blob/master/lists/global.csv and Citizen Lab, Bi Test-Lists, retrieved 07/03/2017, https://github.com/citizenlab/test-lists/blob/master/lists/bi.csv

171 VOA News, 'Burundi Journalists Protest Closing of Radio Station', retrieved 07/03/2017, http://www.voanews.com/a/burundi-journalists-protest-closing-of-radio-station/2746796.html

Rwanda

TABLE 3
Networks tested in Rwanda

Network	Ownership
Tigo Rwanda	Private
Airtel Rwanda	Private
Liquid (former RwandaTel)	Private
MTN Rwanda	Private
OllehRwanda	Public Private Partnership

TABLE 4
Summary of Rwanda Web Connectivity Measurements between 1 December 2016 and 28 February 2017. Source: Small Media Data Compilation

Nine of the 1,108 websites tested on web connectivity showed signs of censorship. WhatsApp and Facebook Messenger presented no anomalies when tested, and traffic manipulation tests also did not present any evidence of tampering.

Website	Networks Blocked	Category
http://www.musabyimana.be	2	Politics
http://rwandarwabanyarwanda.over-blog.com	1	Human Rights Issues
http://www.veritasinfo.fr/	1	News
http://ireme.net	2	News
http://www.umusingi.net/en/	1	News
http://www.umusingi.net/kn/	3	News
http://www.inyenyerinews.org/	4	Human Rights Issues
http://therwandan.com/	5	Political Criticism
http://leprophete.fr/	2	Political Criticism

The number of websites blocked in Rwanda during our research period suggests that there has been a top-down decision targeting specific websites. All the websites blocked (Table 4) host content critical of the government, or report on human rights issues in Rwanda.

Our research did not identify any middle-boxes in the tested networks. It is important to highlight that our tests may potentially register false negatives in the hypothetical instance that ISPs are using highly sophisticated censorship and/or surveillance software that is specifically designed to not trigger errors when receiving invalid HTTP request lines like the ones in this test.

Transparency on Dual-Use Technologies

Internet traffic filtering tools, also referred to in this report as middle-boxes, are used to control content access depending on organization or company policies. Institutions like schools, banks and religious centers may use these tools to restrict specific content on their networks in line with their internal operational policies. On the same note, this capacity can be simultaneously used to restrict content or inspect traffic on national level ISPs and telecommunication companies without clear or consented policies. This is what constitutes dual-use technology.

Internet filtering and interception tools can and have been used for legitimate tasks like breaking child pornography syndicates but they have also been used to target human rights defenders and political dissidents or censor politically contentious content from populations. Reconciling these two extremes has increasingly got complex especially as the demand and supply of these tools grows exponentially across the world.

Detecting a middle box in a network is not conclusive on the intentionality of its use by the ISP or for that matter the tool vendors. If and when middle-boxes are detected through third party research, the popular position from the middle-boxed networks and their affiliate vendors has been that the equipment is on the network for 'quality of service' improvement and not for censorship or surveillance.

To allow for more transparent audit of their purpose on networks serving national populations, there have been efforts to steer the discussion to higher transparency in their acquisition and use. The 2013 amendments to the Wassenaar Arrangement on export controls included network communications surveillance systems or equipment and intrusion software as a way to curb these tools finding their way to jurisdictions likely to use them for human rights violations. As much as this is a positive way forward on bringing more transparency to this field, international agreements are hard to enforce globally and there could be circumventions by middle-agents who are located in fairly democratic jurisdictions as seen from NSO (United States) and Netsweeper (Canada).

Signatories of the Wasseenaar Agreement and whose ISPs and telecommunication companies operate in the East African countries must take concrete steps to promote transparency and responsible deployment of dual-use technologies in their operations. Research has shown that several companies in Europe and North America have sold tools like Blue Coat, registered in California, United States, Forcepoint (formerly Websense registered in Austin, Texas, US) and Netsweeper registered in Canada to countries at war or to regimes with well-documented human rights violations. The governments of these countries have a window of opportunity to shape this discussion, especially through the lens of human rights.

For more on Dual-Use Technologies, see Citizen Lab's November 2016 testimony to the Canadian Senate Standing Committee on Human Rights and the September 2016 adopted proposal on setting up a regime for exports, transfer, brokering, technical assistance and transit of dual-use items.

Uganda

TABLE 5
Networks tested in Uganda

Network	Ownership
MTN Uganda	Private
Airtel Uganda	Private
Uganda Telecom	Public Private Partnership
DataNet	Private
Roke	Private

None of the 1,330 websites tested on web connectivity showed signs of censorship. Neither WhatsApp or Facebook Messenger presented any anomalies, whilst the traffic manipulation tests run during the testing period showed three networks using middle-boxes.

Our research identified three middle-boxes on three ISPs; DataNet, AirTel Uganda and Roke. Due to the dual-use of middle-box tools, we cannot say with certainty that it is for censorship or surveillance. However, there is need for transparency from the ISPs in disclosing for which purpose they have deployed the middle-boxes.

Tanzania

TABLE 6
Networks tested in Tanzania

Network	Ownership
Tigo	Private
Vodacom	Private
Viettel	Private
StarTel	Private
TTCL	Government

A total of 1,157 websites were tested for web connectivity, with none of them showing signs of censorship. WhatsApp and Facebook Messenger presented no anomalies, whilst traffic manipulation tests run during the testing period showed one network using middle-boxes.

Our research also identified a middle-box on one ISP; StarTel. As noted above, due to the dual-use of middle-box tools, we cannot say with certainty that they are being used for censorship or surveillance. However, there is need for transparency from the ISPs in disclosing the purposes for which they have deployed the middle-boxes.

Governments, ISPs and Information Controls

Below is a tabulation of market share comparing government-owned or affiliated ISPs and privately operated ones. The statistics for comparison are compiled from national communication regulators' quarterly reporting documents.[172]

TABLE 7

Publicly owned versus privately owned ISPs. Source: Compilation from national regulators' reports.

Country	% of market share (government owned or affiliated ISP)	% of market share (privately owned ISP)
Burundi	4.5	95.5
Rwanda	2.25	97.75
Uganda	2	98
Tanzania	1	99
Average	2.5	97.5

Government-owned ISPs carry the least internet traffic to the end users in the four countries under study, with private companies being the dominant agents of connectivity. According to national communication regulators' reports, an estimated 97% of end-user internet subscriptions are on private companies, with government – in public-private-partnerships or exclusive ownership – carrying the remaining 3%.[173]

It can be argued that there is no significant correlation between government-owned ISPs and censorship. Governments, it can be deduced, must work with private companies to effect requests for information controls on the internet. This could be through legal means, such as through legislation that allows for government interception of communications, as explored in our policy and legal analysis, or bureaucratic sanctions in the form of conditional renewal of licenses based on the execution of government requests by ISPs.

We have seen this enacted in the countries included in this study. The Burundian government blocked access to social media sites through ordering telecommunications operators to block mobile access to them. Worryingly, Rwanda's 2013 Interception of Communications Law not only requires

---

172 Burundi: http://www.arct.gov.bi/images/statistique/anasetic1.pdf
Rwanda: http://www.rura.rw/fileadmin/docs/statistics/STATISTICS_AND_TARIFF_INFORMATION_IN_THIRD_QUARTER_2016.pdf
Uganda: http://www.ucc.co.ug/files/downloads/Market_&_Industry_Report_for_Q3_July-September_2016.pdf
Tanzania: http://www.tcra.go.tz/images/documents/telecommunication/CommStatMarch16.pdf

173 See Annex on Internet Landscape

communication service providers to allow for backdoor access, but the law also allows for the use of technologies that do not require cooperation with providers. South Sudan's 2014 National Security Law also provides authorities with practically limitless authority to intercept and surveil citizens' communications. The Tanzania Communications Regulatory Authority Act of 2003 allows the authority to obtain information, documents and evidence related to communications in the performance of its functions (Section 17). This provision may be misused by state agencies to compel ISPs to release user information to the government. Lastly, in Uganda under the 2010 Interception of Communications Act, providers are required to install hardware and software facilities to enable the interception of communications at all times.

Within this landscape, the case can be made that private companies are central to the struggle for internet freedom in the target countries, and that their relationship with governments is one of the main determining factors of internet freedom in the region.

Conclusions and Recommendations

This report has demonstrated the necessity for civil society to mobilise itself in defence of internet freedom across East Africa. We have shown how in each of the countries assessed in this study, government policy is out of alignment with the core values of the African Declaration on Internet Rights and Freedoms – in some cases to such an extent that citizens' human rights are at risk of being trampled.

Human rights and internet freedom advocates should continue to press their governments to review and adjust their policies in such a manner as to come into compliance with the ADIRF, and to support the online rights of citizens across the region.

Our general recommendations are as follows:

Regional Governments

- Regional governments must respect human rights online. They must take steps to ensure that all legal, policy, and administrative measures are in compliance with national constitutions and generally accepted human rights standards stipulated in Africa-wide and international human rights instruments.

- In addition to generally accepted international human rights standards, regional governments should recognise and endorse the African Declaration on Internet Rights and Freedoms, and work to bring their policies and legislation into line with its core principles.

- In order to safeguard freedom of expression, media pluralism, and cultural diversity, regional governments should take steps to ensure the protection of net neutrality, and oppose discriminatory access to the internet.

- Regional governments should recognise their obligations to guarantee freedom of expression online under the provisions of their respective constitutions. Legislation requiring unduly strenuous regulation of the press should be repealed, and should not be used to threaten or undermine the legitimate work of journalists – online or offline.

- All governments must recognise the right of citizens to online privacy and secure online communications. Any laws providing for interception of communications for legitimate security purposes (communications that legitimately threaten national security or peace) should be revised to ensure maximum transparency and accountability.

- Governments should take active steps to protect the online privacy and freedom of expression of marginalised groups, including women, ethnolinguistic minorities, LGBTI people, the elderly, young people and children, and people with disabilities. Efforts should be made to involve stakeholders from marginalised communities in multi-stakeholder discussions about the development of the internet in the region.

- Governments should, through a consultative process, draft and pass data protection laws that will guarantee privacy of citizens' information and offer legal recourse to citizens when their data is illegally accessed or compromised.

- Provide judicial training on the internet and human rights. Judicial oversight on the relationship between human rights and national security is a best practice in democratic societies but without capacity in appreciating the fast moving digital landscape, the effectiveness of this oversight is limited.

In line with these points, we offer the following recommendations to specific regional governments:

Burundi

- The government of Burundi should, through a consultative process that includes key stakeholders, develop a data protection law that demonstrates strong and transparent processes behind the protection of its citizens' information.

- More should be done to facilitate the internet as a platform for the sharing of information. A freedom of information law should be enacted and implemented as part of this process.

- In line with this, the internet should be recognised as a means for citizens to express themselves freely, and more should be done to provide legislation that promotes freedom of expression in the country.

Rwanda

- The government should enact sufficient legislation regarding surveillance, to ensure that current legislation does not result in abuse and citizens do not face unwarranted surveillance that curtails their freedom on the internet.

- In line with this, the Interception of Communication Act (2013) should be amended to ensure that there is more transparency in its processes.

- More should be done to recognise the internet as a platform for the freedom of expression. Legislation should be put in place that supports this recognition, and the wholesale blocking of critical websites should be curtailed.

South Sudan

- The government should develop a data protection law that protects its citizens' rights to privacy and the protection of their information. Transparency should be increased over government access to citizens' information.

- In line with this, the government should amend its national security legislation to make sure it falls in line with regional and international norms and practices, that do not unnecessarily infringe on citizens' rights.

- Become party to, and comply with, key regional and international human rights treaties.

- Continue to push for greater investment in the ICT sector, to ensure that the internet becomes affordable and accessible to all.

Tanzania

- Laws that limit freedom of expression, including the Electronic and Postal Communications Act (2010) and Cybercrimes Act (2015), should be amended to ensure that citizens' digital rights are not curtailed when authorities pursue legitimate national security concerns.

- The government should develop data protection and privacy law(s) that respect the need for privacy and and the protection of citizens' information. There should also be more transparency regarding the collection of citizens' information.

Uganda

- The Regulation of the Interception of Communications Act (2012) should be amended to ensure there is more transparency in its processes.

- Legislation that actively targets marginalised and minority groups should be revoked, and legislation that seeks to promote an inclusive digital landscape should be enacted, in order for the government to comply with the African Declaration on Internet Freedom, and other international human rights laws and norms.

Digital Security Organisations

- Continue to raise awareness of, and train civil societies on, the digital threats that face them, and the best practices and tools needed to mitigate them.

- In line with this, continue to work towards the creation of a strong digital security network that civil society can rely on for further training, development and support.

- Ensure that there is a sustained engagement with those that have received training, to make sure that the knowledge and skills learned are in use, and that they have been passed on to the rest of the organisation.

Internet Freedom Researchers

- Work to develop a more robust and non-technical method of contributing websites or applications from average internet users into the sample frames for OONI Probe and Centinel.

Internet Service Providers

- To ensure that the services they provide adhere to regional and international standards for human rights, and to work to prevent services being blocked and websites being censored when such action represents

a crackdown on internet freedom.

- Increase transparency on licensing terms to allow civil society and citizens (who double up as consumers of their services) to see what safeguards are available, and any concerns they should have regarding tampering with the services.

Technology Companies

- Manufacturers and the support ecosystem around software and hardware tools that produce dual-use technologies that can be used for law enforcement should design their deployment in a transparent way, especially on how their products are used, and should also pro-actively verify if the purchase objectives are matched in practice. To the extent possible, the sale and utilisation of technologies that can be repurposed for mass surveillance and censorship should be vetted with wider public participation.

- In line with this, to increase transparency over the use of middle-boxes by ISPs, to make sure that they are used for legitimate purposes, and not to curtail internet freedom.

International Community

- Ensure that companies based outside of the East Africa region are not contributing to the curtailing of internet freedom, by better regulating the sale of dual-use technologies, and making sure that digital tools that could be used against CSOs and citizens are not utilised in this way.

Annex I

Methodology

To gauge civil society's readiness to protect itself from online surveillance and other digital security threats in East Africa (specifically Burundi, Rwanda, Uganda and Tanzania), our researchers conducted a series of in-depth interviews with Civil Society Organisations (CSOs) from across the region.

In order to build a strong picture of the digital security landscape for regional CSOs, we interviewed 39 CSOs: 12 in Tanzania, 10 in Uganda, 7 in Rwanda and 10 in Burundi. These organisations conduct work across a range of fields, including: LGBTI rights, women's rights, freedom of expression, and environmental rights.

Our on-the-ground researchers conducted semi-structured interviews, covering three areas of interest:

1. Threat perception
2. Training and support
3. Digital resilience

Threat Perception

To establish threat perception, CSOs were asked: 'What are the digital security risks that your organisation is most concerned about?' To expand on the question, participants were then asked if they believed the threats came from a state or non-state actor. From collating the answers to this question, we established four finite answers: phishing, surveillance, hacking and censorship.

Answers were coded into the two categories of state threat and non-state threat. The value of 0 represented that no threat was perceived, whilst the value of 1 that a threat was perceived:

CSO Code	State Threat From...				Total	Score
	Phishing	Surveillance	Hacking	Censorship		
T1	1	0	0	0	1	25.00%

CSO Code	Non-State Threat From...				Total	Score
	Phishing	Surveillance	Hacking	Censorship		
T1	0	0	0	0	0	0.00%

The overall average of the score for each country was then taken, leaving us with a total percentage for the overall threat perceived from the state, and the overall threat perceived from non-state actors.

To give us a more detailed representation of specific threats we also tallied the individual threats within their categories of state and non-state. This score was then divided by the number of participant CSOs. For example, with five out of twelve CSOs in Tanzania perceiving a threat of state-directed phishing attempts, the total score given was 41.67%.

Finally, to establish the total threat perception rating of each country we assigned the value of 1 to threats that were perceived to be from the state, or from non-state actors. Those that perceived a threat to come from both were assigned the value of 2. This left the total value for each CSO to be 8. The total score for each CSO was then added together and divided by the total value of 8, leaving us with their final threat perception rating:

CSO Code	Surveillance Threat				Total	Score
	Phishing	Surveillance	Hacking	Censorship		
T5	0	2	2	2	6	75.00%

The average of the final percentage we had was then taken, to establish the total digital threat perception for the country.

Training and Support

To establish the training needs and priority development areas for CSOs in the region we asked a series of questions about the types of digital security training and support that CSOs received, and how the knowledge gained from trainings was transferred to staff members and associate CSOs. See Annex II for our interview guide.

The results of our interviews were coded according to CSOs' responses, and aggregated scores taken for CSOs in each country. See these coded results in Annex III. The ratings were assigned as follows, based on a CSO's score for each question:

0-19 // **Very Limited**
20-39 // **Limited**
40-59 // **Sufficient**
60-79 // **Good**
80-100 // **Excellent**

Digital Resilience

To establish the digital resilience scores for each country, we asked CSOs a series of questions about the types of digital security practices they implemented into their daily operations [see Annex II]. If an organisation utilised a digital security tool or practice, they were given a score of 1. If they did not, they were scored a 0. The scores for each practice were then tallied on the country-level, and the total score divided by the number of organisations interviewed in each country, giving us our final percentage for each practice/tool. To gain the overall rating, the average was taken of the totals for each practice/tool:

	Does your organisation use...								Rating
	... two-factor authentication?	...email encryption?	...data encryption?	...password management tools	...cloud storage services?	...anti-virus software?	...firewall software?	...firewall hardware	
Score	16.67%	25.00%	33.33%	0.00%	58.33%	91.67&	33.33%	25.00%	35.42%
Rating	Very limited	Limited	Limited	Very limited	Sufficient	Excellent	Limited	Limited	Limited

The ratings were assigned as follows:

0-19 // **Very Limited**
20-39 // **Limited**
40-59 // **Sufficient**
60-79 // **Good**
80-100 // **Excellent**

Annex II

Interview Guide

This annex contains the interview guide that was used by our field researchers to gather the data for our digital resilience and threat assessments for regional CSOs. The interviewers asked questions on the CSOs' organisational make-up, the risks they perceived, their assets, and their existing threat mitigation policies.

On average, interviews took between 45 - 90 minutes.

Organisational Questions

In this section we would like to learn about your organisation, its mission, activities and size.

- *Please describe the mission and the work of your organisation.*
- *Where does your organisation operate and which geographical areas does it cover?*
- *Who are your organisation's main beneficiaries?*
- *On what issue or issues do you focus?*
- *Can you briefly describe some of the projects that you are currently working on?*
- *How many employees does your organisation have?*
- *Please describe briefly what you use internet in your organisation for?*

Risk Perception

In this section we would like to understand some of the digital security risks that you think your organisation is exposed to. We would like to know both the perceived ones and any actual digital security incidents that you might have experienced in the past.

- *What are the digital security risks that your organisation is most concerned about?*
  - + *Why are you worried about this threat?*
  - + *Does this threat come from a state or non-state actor?*
  - + *How likely do you think it is that you'll be affected by this risk?*

- *Do you think that there is surveillance in your country? If yes, how do you think you are affected by it? Please probe for details and evidence.*

- *Is there online content censorship in your country? If yes, please probe for details and specific cases.*

- *As the result of working at your organisation, what kinds of physical or digital attacks have you experienced in the past 2 years?*
  - + *Follow-up question for as many technical details as possible. Try to ascertain if it is a targeted attack or generic. Take documentation of malware, phishing emails, social engineering, etc if possible.*

Assets

In this section we would like to get a rough idea of some of the assets that you seek to protect. Which type of assets (e.g., hardware, network, data, online services, websites etc.) are you most keen to protect?

- *Does your organisation have a website? If so, what is the address? Please also ask who has developed the site and how it is being hosted. Please also ask if they have faced any issue with the site and the hosting?*

- *Is your organisation active on Social Media? If so, please ask for the profile addresses.*

- *Does your organisation have an internal network? If so, please ask who maintains it? Are there any issues with it?*

- *Does your organisation store sensitive data? If so, can you tell us about the nature of data and where it is stored? Please note that we are not interested in the details of sensitive data, we just would like to know what areas there might be in.*

Preparedness and Threat Response

In this section we would like to know what measures you take to prevent attacks (e.g. training, pen testing etc.) and how you would respond to attacks.

Training and Support

- *Has your organisation received any digital security training before? If so, when and by whom? Please list if more than one?*
- *Do you offer digital security training to new recruits/ existing staff?*
- *How often is security discussed with staff? If you have digital security policies, how often are they discussed with staff?*
- *Do you offer digital security training to your partners?*
- *Are you engaged with any civil society networks or organisations that support digital security initiatives? If so, which one?*
- *Who would you contact if there was a digital security incident that you cannot deal with internally?*

Policy and Practices

- *Is there a protocol around information security when people move positions or leave the organisation?*
- *Do you have an information security policy? What does it specify? Is it possible to obtain a copy,? How is this policy communicated to staff? If there is no written policy, please ask if there is any informal procedure around the following areas:*
  - + *Do you have a data backup policy?*
  - + *Do you have a policy for destroying sensitive/unwanted info?*
  - + *Do you have a policy for traveling with digital devices? What is this policy? Are you happy with it?*

Audit

- *Have you conducted any digital security risk assessment for your organisation? If so, please ask for details. How and who?*
- *Do you conduct digital security audits of your internal information system? If so, please ask for details. How and who?*
- *Do you conduct digital security audit of your partner information system? If so, please ask for details. How and who?*
- *Do you review the digital security of your platforms before launching them publicly? If so, please ask for details. How and who?*

Background on security practices

- *Do you use two-factor authentication on your accounts (wifi, social media, websites, servers, intranets)?*

- *Do you routinely encrypt emails? If so, how?*
- *Do you encrypt sensitive data? If so, how?*
- *Do you use password management software? If so, which one?*
- *Do you use cloud services such as Dropbox or Google Drive?*
- *Do you have anti-virus software installed on company laptops and PCs?*
- *Do you have firewall software installed on company laptops and PCs?*
- *Do you use any digital security hardware (firewall, etc)? If so, which one?*
- *Are there any other steps your organisation takes to prevent breaches?*

Hypothetical Scenarios

- *A member of your staff receives a suspicious email. What is typically done?*
- *A member of your staff fears their email/social media account has been compromised. What is typically done? Is there a set procedure? Is this followed instinctively? Whom do you contact?*

Annex III

CSO Threat Perception, Training, and Digital Resilience Scores

Perception of Digital Security Threats **STATE ACTORS**

TANZANIA

	PHISHING	SURVEILLANCE	HACKING	CENSORSHIP		
T 01	■	■			35.00%	LOW
T 02		■	■		50.00%	MODERATE
T 03				■	25.00%	LOW
T 04					0.00%	VERY LOW
T 05		■	■	■	75.00%	HIGH
T 06	■		■		50.00%	MODERATE
T 07		■		■	50.00%	MODERATE
T 08	■		■		50.00%	MODERATE
T 09		■	■	■	75.00%	HIGH
T 10		■	■		50.00%	MODERATE
T 11	■	■	■		50.00%	MODERATE
T 12	■		■		50.00%	MODERATE
TOTAL	5	5	8	4	42.86%	MODERATE

UGANDA

	PHISHING	SURVEILLANCE	HACKING	CENSORSHIP		
U 01	■	■	■	■	100.00%	EXTREME
U 02	■	■		■	75.00%	HIGH
U 03	■	■	■	■	100.00%	EXTREME
U 04		■	■	■	75.00%	HIGH
U 05	■	■	■		75.00%	HIGH
U 06		■			35.00%	LOW
U 07		■	■	■	75.00%	HIGH
U 08		■	■	■	75.00%	HIGH
U 09	■	■	■	■	100.00%	EXTREME
U 10		■			35.00%	LOW
TOTAL	5	10	7	7	72.50%	EXTREME

RWANDA

	Financing	Surveillance	Evasion	Corruption		
R 01	■	■	■	■	!	EXCLUDED
R 02	■	■	■	■	!	EXCLUDED
R 03					0 %	VERY LOW
R 04					0 %	VERY LOW
R 05					0 %	VERY LOW
R 06		■			25.00%	LOW
R 07	■	■		■	75.00%	HIGH
TOTAL	1	2	0	1	20.00%	LOW

BURUNDI

	Financing	Surveillance	Evasion	Corruption		
B 01		■	■		50.00%	MODERATE
B 02	■		■		50.00%	MODERATE
B 03			■		25.00%	LOW
B 04	■	■	■		75.00%	HIGH
R 05					0 %	VERY LOW
B 06	■	■	■	■	100.00%	EXTREME
B 07	■	■	■		75.00%	HIGH
B 08		■	■		50.00%	MODERATE
R 09		■		■	50.00%	MODERATE
B 10					0 %	VERY LOW
TOTAL	4	6	7	2	47.50%	MODERATE

Perception of Digital Security Threats **NON STATE ACTORS**

TANZANIA

	PHISHING	SURVEILLANCE	HACKING	CENSORSHIP		
T 01					0 %	VERY LOW
T 02					0 %	VERY LOW
T 03					0 %	VERY LOW
T 04	■		■		50 %	MODERATE
T 05		■	■	■	75.00%	HIGH
T 06					0 %	VERY LOW
T 07			■		50.00%	MODERATE
T 08	■		■		50.00%	MODERATE
T 09					0 %	VERY LOW
T 10					0 %	VERY LOW
T 11	■		■		50.00%	MODERATE
T 12	■		■		50.00%	MODERATE
TOTAL	5	1	6	1	27.08%	LOW

UGANDA

	PHISHING	SURVEILLANCE	HACKING	CENSORSHIP		
U 01	■	■	■	■	100.00%	EXTREME
U 02	■	■			50.00%	MODERATE
U 03	■		■		50.00%	MODERATE
U 04		■	■	■	75.00%	HIGH
U 05					0 %	VERY LOW
U 06					0 %	VERY LOW
U 07			■		25.00%	LOW
U 08			■		25.00%	LOW
U 09	■		■		50.00%	MODERATE
U 10		■			25.00%	LOW
TOTAL	4	4	6	2	40.00%	MODERATE

RWANDA

	[illegible]	[illegible]	[illegible]	[illegible]		
R 01	■	■	■	■	!	EXCLUDED
R 02	■	■	■	■	!	EXCLUDED
R 03	■		■		50.00 %	MODERATE
R 04	■				0 %	LOW
R 05					0 %	VERY LOW
R 06	■	■	■		25.00%	HIGH
R 07	■	■			50.00 %	MODERATE
TOTAL	4	2	2	0	40.00%	MODERATE

BURUNDI

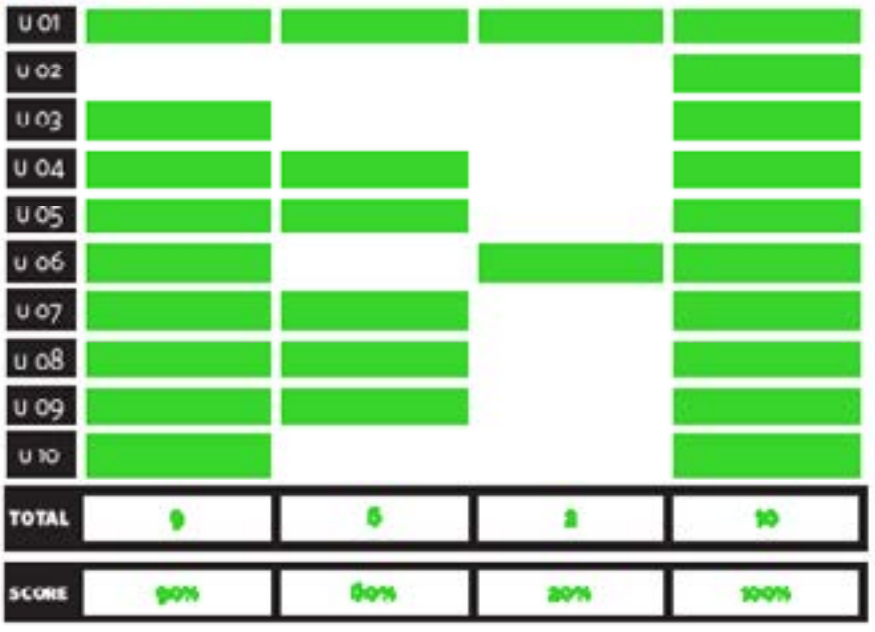
	[illegible]	[illegible]	[illegible]	[illegible]		
B 01					0 %	VERY LOW
B 02	■		■		50.00%	MODERATE
B 03					0 %	VERY LOW
B 04	■	■	■		75.00%	HIGH
B 05			■		0 %	LOW
B 06					0 %	VERY LOW
B 07					0 %	VERY LOW
B 08					0 %	VERY LOW
B 09					0 %	VERY LOW
B 10	■				25.00 %	LOW
TOTAL	3	1	3	0	17.50%	LOW

Digital Security Support Assessment

TANZANIA

	HAS CSO RECEIVED DIGITAL SECURITY TRAINING?	DOES CSO GIVE NEW RECRUITS DIGITAL SECURITY TRAINING?	DOES CSO GIVE PARTNER ORGANISATIONS DIGITAL SECURITY TRAINING?	IS CSO CONNECTED TO ANY NETWORKS THAT SUPPORT DIGITAL SECURITY INITIATIVES?
T 01				
T 02	■			■
T 03				
T 04	■			
T 05	■	■	■	■
T 06	■			■
T 07	■			■
T 08				■
T 09	■	■		■
T 10	■	■		■
T 11				
T 12	■	■		
TOTAL	8	4	1	7
SCORE	66.67%	33.33%	8.33%	58.33%

UGANDA



U 01	■	■	■	■
U 02				■
U 03	■			■
U 04	■	■		■
U 05	■	■		■
U 06	■		■	■
U 07	■	■		■
U 08	■	■		■
U 09	■	■		■
U 10	■			■
TOTAL	9	6	2	10
SCORE	90%	60%	20%	100%

RWANDA

	HAS CSO RECEIVED DIGITAL SECURITY TRAINING?	DOES CSO GIVE NEW RECRUITS DIGITAL SECURITY TRAINING?	DOES CSO GIVE PARTNER ORGANISATIONS DIGITAL SECURITY TRAINING?	IS CSO CONNECTED TO ANY NETWORKS THAT SUPPORT DIGITAL SECURITY INITIATIVES?
R 01				■
R 02	■			■
R 03	■			
R 04	■			
R 05				
R 06	■			■
R 07				
TOTAL	4	0	0	3
SCORE	57.14%	0%	0%	42.86%

BURUNDI

B 01	■			
B 02		■		
B 03	■			■
B 04		■		
B 05	■			■
B 06	■			■
B 07	■			
B 08	■			
B 09				■
B 10				
TOTAL	5	2	0	4
SCORE	50%	20%	0%	40%

Digital Resilience Assessment

DOES YOUR ORGANISATION USE...

TANZANIA

	...TWO FACTOR AUTHENTICATION?	...EMAIL ENCRYPTION?	...DATA ENCRYPTION?	...PASSWORD MANAGEMENT TOOLS?	...CLOUD STORAGE SERVICES?	...ANTI-VIRUS SOFTWARE?	...FIRE-WALL SOFTWARE?	...FIRE-WALL SOFTWARE?	SCORE	RATING
T 01									0%	V. Limited
T 02		■			■	■			37.50%	Limited
T 03						■			12.50%	V. Limited
T 04						■	■	■	37.50%	Excellent
T 05	■	■	■		■	■	■	■	87.50%	Good
T 06	■		■		■	■	■		62.50%	V. Limited
T 07						■			12.50%	V. Limited
T 08						■			12.50%	Limited
T 09					■	■			25%	Limited
T 10			■		■	■			37.50%	Limited
T 11					■	■			25%	Good
T 12		■	■		■	■	■	■	75%	Limited
TOTAL	3	3	4	0	7	11	4	3		
SCORE	18.8%	25%	33.33%	0%	58.33%	91.67%	33.33%	25%		

AVERAGE THREAT MITIGATION: 35.42%

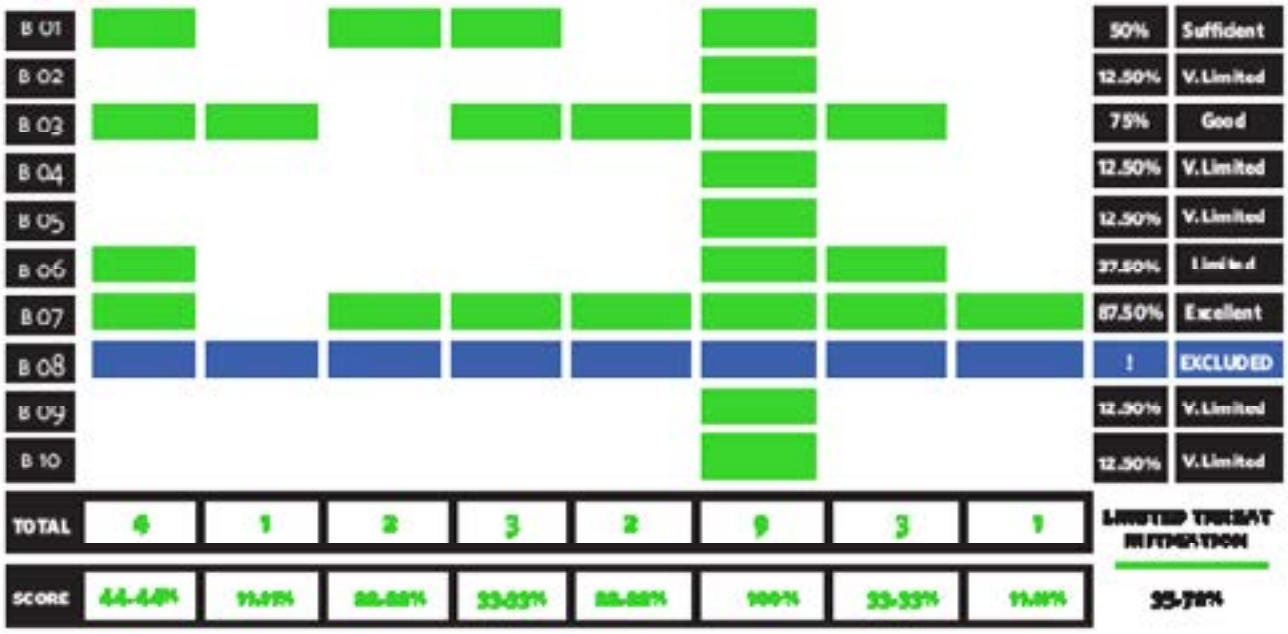
UGANDA

U 01	■		■	■	■	■	■	■	87.50%	Excellent
U 02	■								12.50%	V. Limited
U 03	■				■	■	■		50%	Sufficient
U 04	■				■	■	■		50%	Sufficient
U 05		■	■		■	■	■		62.50%	Good
U 06		■			■	■	■	■	62.50%	Good
U 07	■				■	■			37.50%	Limited
U 08			■		■	■	■		50%	Sufficient
U 09									0%	V. Limited
U 10					■	■			25%	Limited
TOTAL	5	2	3	1	8	8	6	2		
SCORE	50%	20%	30%	10%	80%	80%	60%	20%		

AVERAGE THREAT MITIGATION: 43.75%

RWANDA

BURUNDI



Annex IV

Network Measurements Methodology

For the purpose of this study, the network measurement activities included:

1. Assembling the network measurement software on portable machines
2. Creation of country specific test lists
3. Conducting actual network measurements and
4. Data analysis

The research team used two software platforms to conduct the tests; Centinel, a project of the Information Controls Lab (ICLab)[174] at Stony Brook University, and ooniprobe, a project of the Open Observatory of Network Interference (OONI).[175] The two software packages were installed on similar laptops across the four study countries.

Both platforms are designed to access selected websites (test lists), inspect their connectivity status and examine whether traffic manipulation is happening on the networks being tested. Creation of a country-case test list from the millions of potential test websites (sampling phase of the research) was a critical phase of the research. Lists of websites and communication applications that are relevant and commonly accessed in the case countries were created alongside top accessed websites globally. As purposive sampling, the research used Alexa web tool that lists websites based on a combination of average daily visitors and page-views over the past month.[176] From this list, country specific researchers were requested to add relevant websites that may not be popular globally yet they attract citizen and government attention domestically. The result was two test-lists – global and country-specific - which formed the sample for the research. Each website was categorised based on the content it carries which would help understand which type of content is likely to be censored in such a region, thus offering a guide to what other content the research should look into that may not

174 See more about ICLab here: https://iclab.org/what-is-iclab/

175 See more about OONI: https://ooni.torproject.org/about/

176 See Burundi, Rwanda, Uganda, Tanzania and global pages here http://www.alexa.com/top-sites

be included in the test list. The inclusion of objectionable websites such as pornography is because they are more likely to be blocked due to their content, offering the researcher to develop heuristics for detecting how other content is or can be blocked. All test lists are centrally hosted by the Citizen Lab on GitHub, supporting network measurement projects in the creation and maintenance of lists of URLs to test for censorship.[177]

We selected five local vantage points from Internet Service Providers (top two highest subscribed service providers, one medium level subscription provider, one government owned provider and one lowly subscribed provider).[178] From these, tests were run at least once from urban and rural geographic locations. The testing, an automated way of trying to access multiple websites and applications and sending requests over a network, were run between 1 December 2016 and completed 28 February 2017, covering a range of 90 days.

Once network measurement data was collected from these tests, the data was subsequently processed and analyzed based on a set of heuristics for detecting Internet censorship and traffic manipulation. The software platform is designed to flag websites that present anomalies or networks that present sign of network tampering. Further confirmation tests are run on preliminary results to ascertain the veracity of the tests. This sense checking is through manual access of said websites in the said countries where they presented anomalies.

Tests Run

Web Connectivity

This test examines whether websites are reachable and if they are not, it attempts to determine whether access to them is blocked through DNS tampering, TCP connection RST/IP blocking or by a transparent HTTP proxy. Specifically, this test is designed to perform the following:

- Resolver identification
- DNS lookup
- TCP connect
- HTTP GET request

By default, this test performs the above (excluding the first step, which is performed only over the network of the user) both over a control server and over the network of the user. If the results from both networks match, then there is no clear sign of network interference; but if the results are different, the websites that the user is testing are likely censored. Further information is provided below, explaining how each step performed under the web connectivity test works.

---

177 see https://github.com/citizenlab/test-lists

178 This information was aggregated from official communication regulator reports where Internet Service Providers are expected to make quarterly usage reports.

1. Resolver identification
The domain name system (DNS) is what is responsible for transforming a host name (e.g. torproject.org) into an IP address (e.g. 38.229.72.16). Internet Service Providers (ISPs), amongst others, run DNS resolvers that map IP addresses to hostnames. In some circumstances though, ISPs map the requested host names to the wrong IP addresses, which is a form of tampering.

As a first step, the web connectivity test attempts to identify which DNS resolver is being used by the user. It does so by performing a DNS query to special domains (such as whoami.akamai.com) that will disclose the IP address of the resolver.

2. DNS lookup
Once the web connectivity test has identified the DNS resolver of the user, it then attempts to identify which addresses are mapped to the tested host names by the resolver. It does so by performing a DNS lookup, which asks the resolver to disclose which IP addresses are mapped to the tested host names, as well as which other host names are linked to the tested host names under DNS queries.

3. TCP connect
The web connectivity test will then try to connect to the tested websites by attempting to establish a TCP session on port 80 (or port 443 for URLs that begin with HTTPS) for the list of IP addresses that were identified in the previous step (DNS lookup).

4. HTTP GET request
As the web connectivity test connects to tested websites (through the previous step), it sends requests through the HTTP protocol to the servers which are hosting those websites. A server normally responds to an HTTP GET request with the content of the webpage that is requested.

Comparison of results: Identifying censorship

Once the above steps of the web connectivity test are performed both over a control server and over the network of the user, the collected results are then compared with the aim of identifying whether and how tested websites are tampered with. If the compared results do not match, then there is a sign of network interference.

Below are the conditions under which the following types of blocking are identified:

- DNS blocking: If the DNS responses (such as the IP addresses mapped to host names) do not match.
- TCP/IP blocking: If a TCP session to connect to websites was not established over the network of the user.
- HTTP blocking: If the HTTP request over the user's network failed, or the HTTP status codes don't match, or all of the following apply:

+ The body length of compared websites (over the control server and the network of the user) differs by some percentage

+ The HTTP headers names do not match

+ The HTML title tags do not match. It is important to note, however, that DNS resolvers, such as Google or a local ISP, often provide users with IP addresses that are closest to them geographically. Often this is not done with the intent of network tampering, but merely for the purpose of providing users with localized content or faster access to websites. As a result, some false positives might arise in OONI measurements. Other false positives might occur when tested websites serve different content depending on the country that the user is connecting from, or in the cases when websites return failures even though they are not tampered with.

HTTP invalid request line

This test tries to detect the presence of network components ("middle box") which could be responsible for censorship and/or traffic manipulation. Instead of sending a normal HTTP request, this test sends an invalid HTTP request line - containing an invalid HTTP version number, an invalid field count and a huge request method – to an echo service listening on the standard HTTP port. An echo service is a very useful debugging and measurement tool, which simply sends back to the originating source any data it receives. If a middle box is not present in the network between the user and an echo service, then the echo service will send the invalid HTTP request line back to the user, exactly as it received it. In such cases, there is no visible traffic manipulation in the tested network. If, however, a middle box is present in the tested network, the invalid HTTP request line will be intercepted by the middle box and this may trigger an error and that will subsequently be sent back to OONI's server.

Such errors indicate that software for traffic manipulation is likely placed in the tested network, though it's not always clear what that software is. In some cases though, censorship and/or surveillance vendors can be identified through the error messages in the received HTTP response. Based on this technique, OONI has previously detected the use of BlueCoat, Squid and Privoxy proxy technologies in networks across multiple countries around the world.

It's important though to note that a false negative could potentially occur in the hypothetical instance that ISPs are using highly sophisticated censorship and/or surveillance software that is specifically designed to not trigger errors when receiving invalid HTTP request lines like the ones of this test. Furthermore, the presence of a middle box is not necessarily indicative of traffic manipulation, as they are often used in networks for caching purposes.

HTTP header field manipulation

This test also tries to detect the presence of network components ("middle box") which could be responsible for censorship and/or traffic manipulation.

HTTP is a protocol which transfers or exchanges data across the internet. It does so by handling a client's request to connect to a server, and a server's response to a client's request. Every time a user connects to a server, the user (client) sends a request through the HTTP protocol to that server. Such requests include "HTTP headers", which transmit various types of information, including the user's device operating system and the type of browser that is being used. If Firefox is used on Windows, for example, the "user agent header" in the HTTP request will tell the server that a Firefox browser is being used on a Windows operating system.

This test emulates an HTTP request towards a server, but sends HTTP headers that have variations in capitalization. In other words, this test sends HTTP requests which include valid, but non-canonical HTTP headers. Such requests are sent to a backend control server which sends back any data it receives. If OONI receives the HTTP headers exactly as they were sent, then there is no visible presence of a "middle box" in the network that could be responsible for censorship, surveillance and/or traffic manipulation. If, however, such software is present in the tested network, it will likely normalize the invalid headers that are sent or add extra headers.

Depending on whether the HTTP headers that are sent and received from a backend control server are the same or not, OONI is able to evaluate whether software – which could be responsible for traffic manipulation – is present in the tested network.

False negatives, however, could potentially occur in the hypothetical instance that ISPs are using highly sophisticated software that is specifically designed to not interfere with HTTP headers when it receives them. Furthermore, the presence of a middle box is not necessarily indicative of traffic manipulation, as they are often used in networks for caching purposes.

Data analysis

Through the data pipelines, Centinel and OONI processes all network measurements collected, including the following types of data:

Country code

The tests by default collects the code that corresponds to the country from which the user is running tests from, by automatically searching for it based on the user's IP address through the IP databases. This enables the mapping out of global network measurements and to identify where network interferences take place.

Autonomous System Number (ASN)

The tests also collect the Autonomous System Number (ASN) that corresponds to the network that a user is running ooniprobe tests from. This reveals the specific network provider (such as AS37035 Tigo in Tanzania) of a user. Such information can increase transparency in regards to which network providers are implementing censorship or other forms of network interference. The ASNs are as followed:

Burundi:

Network	Autonomous Service Number	Ownership
Econnet-Leo	AS327734	Private
Lacel	AS327720	Private
Viettel	AS327799	Private
Onatel	AS37586	Government
Spider Net	AS37429	Private

Rwanda:

Network	Autonomous Service Number	Ownership
Tigo Rwanda	AS37124	Private
Airtel Rwanda	AS327707	Private
Liquid (former RwandaTel)	AS2117	Private
MTN Rwanda	AS36890	Private

Uganda:

Network	Autonomous Service Number	Ownership
MTN Uganda	AS20294	Private
Airtel Uganda	AS37075	Private
Uganda Telecom	AS21491	Public Private Partnership
DataNet	AS36901	Private
Roke	AS37063	Private

Tanzania:

Network	Autonomous Service Number	Ownership
Tigo	AS37035	Private
Vodacom	AS36908	Private
Viettel	AS327885	Private
StarTel	AS12143	Private
TTCL	AS33765	Government

Date and time of measurements
The tests collect by default the time and date of when tests were run that helps evaluate when network interferences occur and to compare them across time.

IP addresses and other information
The tests do not deliberately collect or store users' IP addresses. OONI, for example, takes measures to remove users' IP addresses from the collected measurements, to protect its users from potential risks.

However, the tests may unintentionally collect users' IP addresses and other potentially personally-identifiable information, if such information is included in the HTTP headers or other metadata of measurements. This, for example, can occur if the tested websites include tracking technologies or custom content based on a user's network location.

Network measurements

The types of network measurements data collected depends on the types of tests that are run. The data collected is in an attempt to answer the following types of questions:

- Which tests were run?
- In which countries were those tests run?
- In which networks were those tests run?
- When were tests run?
- What types of network interference occurred?
- In which countries did network interference occur?
- In which networks did network interference occur?
- When did network interference occur?
- How did network interference occur?

Acknowledgement of limitations

The findings of this study present various limitations, and do not necessarily reflect a comprehensive view of Internet censorship in Burundi, Rwanda, Uganda and Tanzania during the test period.

The main limitation is the amount and type of URLs that were tested for censorship. As mentioned in the methodology section the criteria for selecting case country's sample websites was biased to the extent of the researcher's knowledge of which websites are relevant to the said country as to attract censorship or manipulation. The possibility of censorship of other websites left out of the sample frame is real.

The study was limited to five local network vantage points in each country. Censorship or network interference could be taking place on other networks not covered in the research. This is partly a logistical capacity concern, considering the more networks are tested, the more resources (time and financial) are required.

Finally, the heuristics used as part of Centinel and OONI methodology present limitations. This is due to the fact that many false positives and false negatives occur within collected data (as explained in the methodology section of this report), limiting ability to confirm cases of censorship with confidence in many cases. One example being how limited to a sample of censorship equipment fingerprints are, limiting the ability to identify other types of equipment that may have been used within tested networks.

Annex V

Network Measurement Results

Due to the extensive nature of the network measurement results, we have provided a link to access them on a publicly shared GoogleDoc:

http://bit.ly/Network_Measurements_East_Africa

	Internet penetration rate *The internet penetration rate as of September 2016, as a percentage of total population.*	**Websites blocked** *The number of censored websites we were able to detect.*	**Middle-boxes** *ISP-operated devices that can be used for purposes of censorship and surveillance.*
BURUNDI	**8.2**	**0**	**0**
RWANDA	**33**	**9**	**0**
TANZANIA	**45**	**5**	**3**
UGANDA	**40**	**0**	**1**