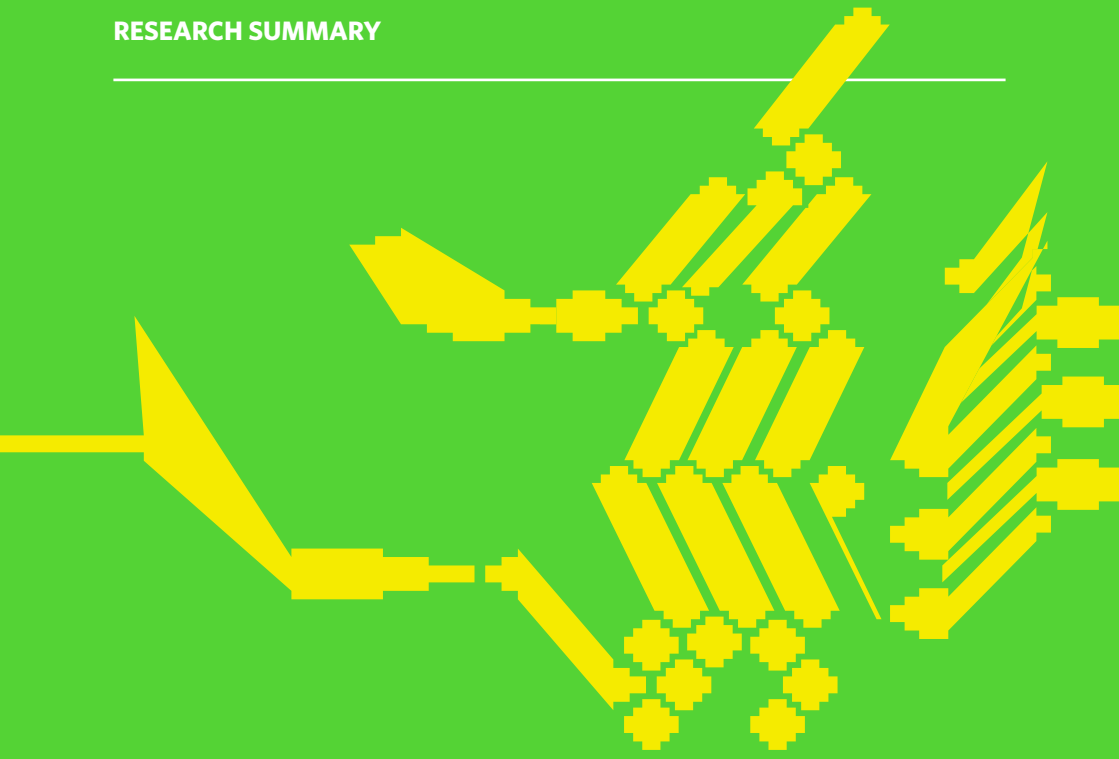
Safeguarding Civil Society

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

RESEARCH SUMMARY



SMALL MEDIA CIPESA DEFEND DEFENDERS CIPIT

This booklet contains a concise summary of our report's key findings. To access our full report on the **state of internet freedom in East Africa**, visit the link below:
smallmedia.org.uk/work/safeguarding-civil-society-east-africa

For more information, get in touch at
contact@smallmedia.org.uk

Contents

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 Researchers**
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**

SMALL MEDIA

CIPESA

DEFENDDEFENDERS
East and Horn of Africa Human Rights Defenders Project

CIPIT
CENTRE FOR INTELLECTUAL PROPERTY AND INFORMATION TECHNOLOGY LAW

Executive Summary

Over the past decade, East Africa has seen a tremendous boom in connectivity and online participation that is beginning to transform the way that 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 advocates, it also offers the possibility for regional state and non-state actors to interfere with their work, surveil them, and censor their voices.

Over the course of this research, we have found that there is an urgent need for East African civil society to be given support to improve their digital resilience in the face of growing threats of surveillance and censorship across the region. In all of the countries surveyed in this report, CSOs failed to demonstrate a baseline of digital security knowledge, or else failed to implement practices effectively.

At the same time, we found that governments across the region require support to bring their policies into compliance with the principles of the African Declaration on Internet Rights and Freedoms – a set of principles developed by

African internet freedom stakeholders to guarantee a free and open internet in Africa.

Small Media, CIPESA, DefendDefenders and CIPIT hope that this research can help to support the security of civil society actors, empower activists to support the principles of the African Declaration, and press their governments to adopt it.

Introduction

In this report Small Media, 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 have 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 global internet freedom organisations – establishes a set of rigorous principles by which governments and other 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.

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 policymakers 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 regional threats.

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 continent, 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]

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 support internet freedom and freedom of expression globally. The principles of the Declaration are noted below.

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

---

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

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 under-representation in decision-making roles, especially in internet governance.

1 State Compliance with the ADIRF

Although the principles of the ADIRF were devised in a collaborative effort between a broad variety of stakeholders, there is a lot of work to be done to persuade regional governments to come on board and adopt the principles of the ADIRF in full.

Overleaf is a table summarising state compliance with the ADIRF. It notes the areas in which regional governments are in alignment with the principles of the ADIRF, and highlights areas in which urgent policy reviews should be undertaken. For full details about our assessment of ADIRF compliance, see our full report at: smallmedia.org.uk/work/safeguarding-civil-society-east-africa

OVERVIEW

Compliance with the African Declaration on Internet Rights and Freedoms

FULL COMPLIANCE 

PARTIAL COMPLIANCE 

NON COMPLIANCE 

NO DATA X

	PRINCIPLE					
	Openness	Internet access and affordability	Freedom of expression	Right to information	Freedom of Assembly and Association and the Internet	Cultural and linguistic diversity
BURUNDI						X
RWANDA						X
SOUTH SUDAN						X
TANZANIA						X
UGANDA						X

Right to development and access to knowledge	Privacy and personal data protection	Security, stability and resilience of the internet	Marginalised groups and groups at risk	Right to due process	Democratic multi-stakeholder internet governance	Gender equality
X	○	○	X	●	X	X
X	●	○	○	○	○	○
X	●	●	X	X	X	○
X	●	X	●	○	○	X
X	●	○	●	●	○	○

2 CSO Digital Resilience

In our report, we show how restrictive policies and state practices are negatively impacting civil society's ability 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.

We undertook a series of 39 interviews with civil society organisations (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 of digital security knowledge and practices within an organisation's staff and across their organisational networks.

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. For full details on how we assigned these scores, take a look at our full report at: smallmedia.org.uk/work/safeguarding-civil-society-east-africa

Digital Resilience Summary Table

DOES YOUR ORGANISATION USE...	BURUNDI		RWANDA	
	SCORING	RATING	SCORING	RATING
...TWO-FACTOR AUTHENTICATION	44.44%	SUFFICIENT	14.29%	VERY LIMITED
...EMAIL ENCRYPTION	11.11%	VERY LIMITED	28.57%	LIMITED
...DATA ENCRYPTION	22.22%	LIMITED	14.29%	VERY LIMITED
...PASSWORD MANAGEMENT TOOLS	33.33%	LIMITED	28.57%	LIMITED
...CLOUD STORAGE SERVICES	22.22%	LIMITED	71.43%	GOOD
..ANTI-VIRUS SOFTWARE	100%	EXCELLENT	85.71%	EXCELLENT
...FIREWALL SOFTWARE	33.33%	LIMITED	28.57%	LIMITED
...FIREWALL HARDWARE	11.11%	VERY LIMITED	28.57%	LIMITED
RATING	**34.72%**	**LIMITED**	**37.50%**	**LIMITED**

TANZANIA		UGANDA	
SCORING	**RATING**	**SCORING**	**RATING**
16.77%	VERY LIMITED	50%	SUFFICIENT
25%	LIMITED	20%	LIMITED
33.33%	LIMITED	30%	LIMITED
0%	VERY LIMITED	10%	VERY LIMITED
58.33%	SUFFICIENT	80%	EXCELLENT
91.67%	EXCELLENT	80%	EXCELLENT
33.33%	LIMITED	60%	GOOD
25%	LIMITED	20%	LIMITED
35.42%	**LIMITED**	**43.75%**	**SUFFICIENT**

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

Threat Perception

The most prominent threats that Burundian CSOs felt they faced were hacking, phishing and surveillance. Of these, surveillance and hacking threats were seen as originating primarily from state actors. A number of CSOs actively pointed out that they were "in the sights of power", due to engaging in work critical of the Burundian government. Despite fears around surveillance, interestingly only one organisation noted online censorship as being an issue of concern.

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

"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." **– A political organisation**

In 2015, a wave of 'spearphishing' (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.

Training

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.

RWANDA

THREAT PERCEPTION RATING	// **30** // Low
STATE ACTORS	// **20** // Low
NON-STATE ACTORS	// **40** // Moderate
DIGITAL RESILIENCE RATING	// **37** // Limited
GREATEST PERCEIVED THREAT	// Non-State-Directed Phishing

Threat Perception

Although allowing more space for free expression than otherwise available in Rwanda, the country's digital landscape is experiencing increasing limitations on internet freedom. Censorship, a key threat faced by 'offline', traditional bodies, is also taking place on digital platforms. Online news websites and political pages have been blocked by authorities – particularly during politically sensitive periods, such as election season.

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.

"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 be

intercepted – or if your mobile is taken they can then access your online communications." **- A Human Rights organisation**

"The main reason... is because when you are defending human rights, the first person to criticise it 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." **- A Human Rights organisation**

"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." **- A Human Rights organisation**

Training

Five of the seven CSOs interviewed had not received any form of digital security training. One of the organisations that had received training, did not pass on the knowledge and skills learned to its new recruits. Interestingly, one organisation 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.

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

Threat Perception

CSOs in Tanzania were concerned about a number of threats. 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.

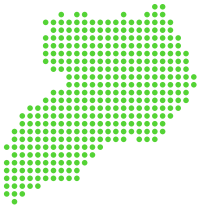
"These laws hinder [you], you might want to express yourself but you end up fearing [for yourself]. Or if you express yourself, there are some things that you can't say. Hence, there are many things on social [media] networks that you can't do. And, if you give

out data, you must make sure there is a person who gave you such data and he/she approved it." **- A youth organisation**
"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." **- A political organisation**

"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." **- An environmental organisation**

Training

Just over half of CSOs surveyed have received some form of digital security training, with half of these also transferring the training 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 such an event.



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

Threat Perception

CSOs in Uganda were concerned about a variety of digital security threats arising from 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 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.

"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." **- A media freedom organisation**

"[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." - **An LGBT rights organisation**

Training

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.

3 Network Measurements

We investigated 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.

We aimed 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.

From the data collected, the extent of Information controls online in the four countries appears inclined more towards surveillance than towards censorship, with dual-use 'middle box' technology being deployed by ISPs in Uganda and Tanzania. Content filtering was also detected in Rwanda.

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, government-owned ISPs have the lowest number of subscribed users. More information is available about our findings in our full report.

For a comprehensive analysis of the results of our network measurements, take a look at our full report at: smallmedia.org.uk/work/safeguarding-civil-society-east-africa/

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 follow:

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 society organisations 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 East Africa 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.