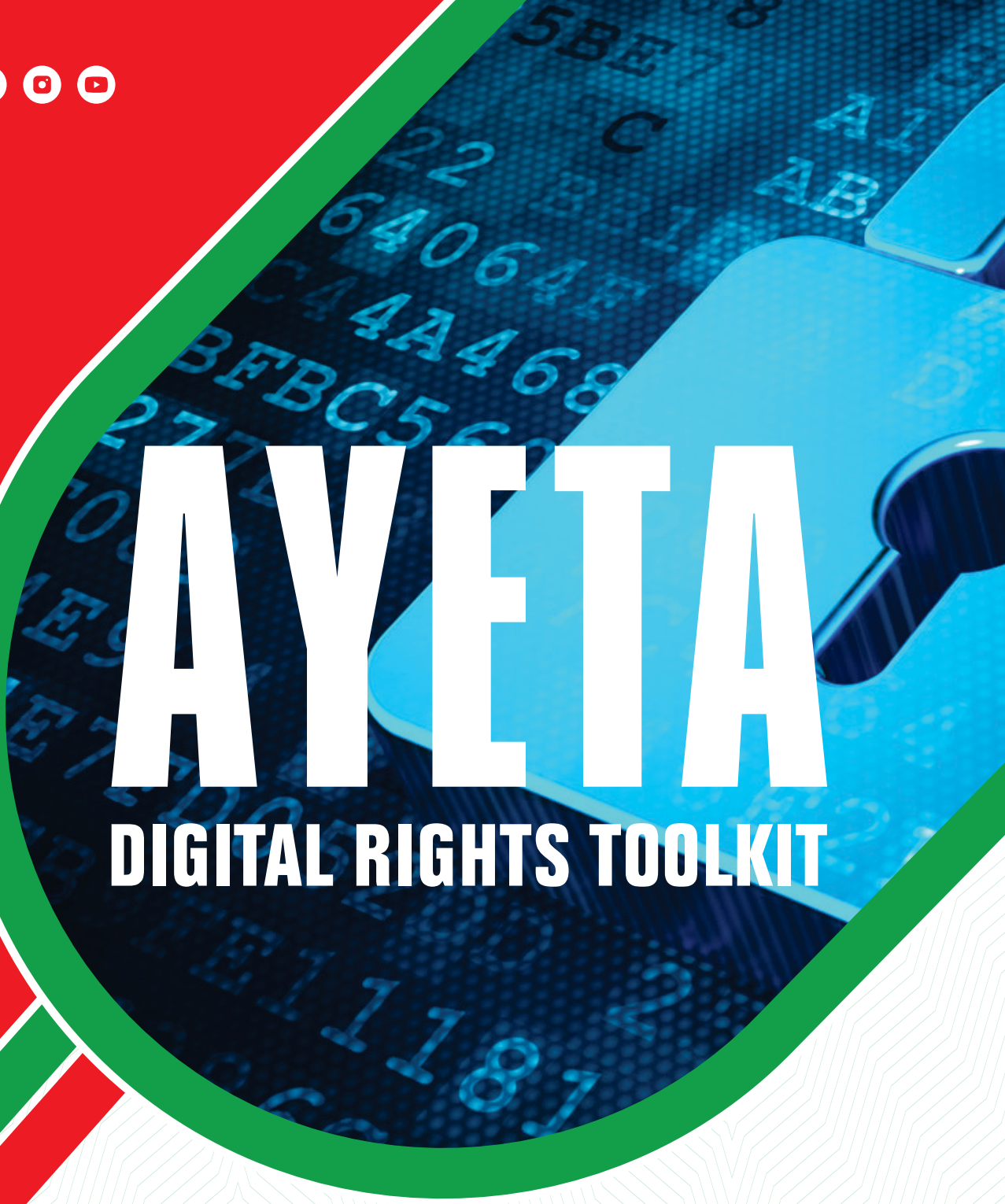


AYETA

DIGITAL RIGHTS TOOLKIT

Kingdom of the Netherlands

PARADIGM INITIATIVE

Stanford PACS
Center on Philanthropy and Civil Society
—
Digital Civil Society Lab

AYETA

DIGITAL RIGHTS TOOLKIT

Published by Paradigm Initiative

Published in April 2024

Researcher: Khadijah El-Usman, Ihueze Nwobilor, Angela Onyegbuna,
Bridgette Ndlovu, Miriam Wanjiru and Sani Suleiman
Research Assistants: Dinchi Ikpa, Ifiokobong Uko and Joshua Oke
Edited By: Khadijah El-Usman and 'Gbenga Sesan
Copy Editor: Izak Minnaar
Design & Layout: Luce Concepts

FOREWORD

As digital rights advocates increasingly become concerned about their digital security, it is critical that they take measures to protect themselves while in the line of duty. This new version of the Ayeta toolkit provides updated digital security tips and measures that can be taken against potential threats. It also includes lists of digital security actors, relevant digital rights events on the continent, links to digital security case studies from selected African countries, model policy briefs and model coalition statements. A section of the toolkit is dedicated to network disruptions, what you can do to circumvent disruptions, how to keep records, and advocacy resources for such incidents.

The first toolkit was developed as a 2020 Stanford Digital Civil Society Fellowship project[1], with additional support from the Netherlands Human Rights Fund. 'Gbenga Sesan, assisted by Bonface Witaba, led project coordination, curriculum development, writing and editing, with support from the Paradigm Initiative team.

We are grateful to the PIN partners who provided feedback on how to improve the previous edition, and their useful insight has helped us to make the toolkit better for today's world. A lot of work went into researching and updating the toolkit, and that was taken care of by PIN team members Angela Onyegbuna, Sani Suleiman, Khadijah El-Usman, Bridgette Ndlovu, Ihueze Nwobilor, Joshua Oke and Miriam Wanjiru. We appreciate the copy editing work done by Izak Minnaar. PIN's Judith Ogutu, Giyo Ndzi and Samuel Ojezele led work on the

1. https://pacscenter.stanford.edu/person/gbenga-sesan/

survey while Kenneth Oyeniyi and David Chima took care of designs. Links were reviewed by Dinchi Ikpa, Ifiokobong Uko and Angela Onyegbuna and this version of the toolkit was edited by Khadijah El-Usman, Angela Onyegbuna and 'Gbenga Sesan.

The toolkit is designed with the overarching aim of addressing the growing need to safeguard digital rights defenders, journalists, whistleblowers and others working with sensitive information in the global South. PIN is committed to ensuring it remains a living resource by publishing updated versions. We rely on your feedback to achieve this – please send comments, ideas, criticism, and stories to hello@ayeta.africa

> ***"This new version of the Ayeta toolkit provides updated digital security tips and measures that can be taken against potential threats."***

Contents

CHAPTER 01

DIGITAL RIGHTS

The advent of the internet and its subsequent opening up to the world in 1989 has witnessed human rights defenders innovating in their use of online spaces to advance the freedom of expression, the freedom of association online, as well as enhance the capacity of a digital society.

The internet today is viewed as a social good, connecting more than half the world. However, it has increasingly become more volatile and on the rise are incidences of challenges posed to activists, human rights defenders, dissidents and journalists.

Authoritarian regimes have resorted to using digital tools and tactics such as internet shutdowns, online censorship and digital surveillance to clamp down on free expression.

As documented in Paradigm Initiative's 2019 Digital Rights in Africa Report,[2]

"Over the past decade, there has been an increase in the impact of African organisations championing digital rights - affordable and quality internet connectivity, privacy, freedom of opinion, expression and association, amongst others. In sharp contrast to this renaissance of digital rights amongst citizens on the continent, the vision of African governments regarding the role of internet connectivity and digital access to the continent has largely been about retaining political power and control by all means. The overwhelming instinct has been largely toward subordinating rights and access in order to retain political control over citizens."

The 2022 Londa Digital Rights and Inclusion in Africa report[3] highlights an evolution in area of new issues coming to the fore:

"emerging technologies like Artificial Intelligence (AI) gain traction, awareness and adoption are growing on the continent" as well as "data privacy and governance and the lack of accountability and oversight."

In 2022, report by Access Now revealed the highest-ever number of internet shutdowns in a single year: 35 countries globally experienced internet shutdowns. Of these, seven were in Africa (Burkina Faso, Ethiopia, Sierra Leone, Nigeria, Somaliland, Uganda, and Zimbabwe). Notably, the previous year witnessed internet shutdowns in 12 African nations.[4]

The actions of these countries directly contravene Principle 38.2 *("States shall not engage in or condone any disruption of access to the internet and other digital technologies for segments of the public or an entire population.")* of the 2019 Declaration of Principles on Freedom of Expression and Access to Information in Africa[5] issued by the African Commission on Human and Peoples' Rights (the 2019 ACHPR Declaration), as well as the Universal Declaration of Human Rights.[6]

2. https://paradigmhq.org/report/digital-rights-in-africa-2019
3. https://paradigmhq.org/wp-content/uploads/2023/04/Londa-2022.pdf
4. https://www.accessnow.org/wp-content/uploads/2023/03/2022-KIO-Report-Africa.pdf
5. https://achpr.au.int/en/node/902
6. https://www.un.org/en/about-us/universal-declaration-of-human-rights

1.1
What are Digital Rights

Digital rights are basically human rights in the internet era. The rights to online privacy and freedom of expression, for example, are really extensions of the equal and inalienable rights laid out in the United Nations Universal Declaration of Human Rights.[7] Digital rights pertain to the rights of individuals to computer access and the ability to use and publish digital contents. It refers to the allowed permissions to fair use of digital materials and the right to privacy. According to the UN, disconnecting people from the internet violates these rights and goes against international law.[8]

Furthermore, the preamble to the 2019 ACHPR Declaration affirms that the same rights that people have offline should be protected online, and acknowledges that the exercise of the rights of freedom of expression and access to information using the internet are central to the enjoyment of other rights and essential to bridging the digital divide[9]- effectively applying the Article 9 rights of access to information and freedom of expression in the African Charter on Human and Peoples' Rights to be effective in the digital age.

1.2
Digital/Human Rights Charters, Declarations, Protocols and Treaties

Human rights apply to all human interactions whether online or offline, as noted above. The principles enshrined in digital rights and general human rights must be synced to apply across the internet environment and the spectrum of internet policy-making domains.

i. UN Declaration of Human Rights[10]

The Universal Declaration of Human Rights (UDHR) is a milestone document in the history of human rights. Drafted by representatives with different legal and cultural backgrounds from all regions of the world, the Declaration was proclaimed by the United Nations General Assembly in Paris on 10 December 1948 (General Assembly resolution 217 A) as a common standard of achievements for all peoples and all nations. It sets out the fundamental human rights to be universally protected

7. https://www.un.org/en/about-us/universal-declaration-of-human-rights
8. https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf
9. https://achpr.au.int/en/node/902
10. https://www.un.org/en/about-us/universal-declaration-of-human-rights

and it has been translated into over 500 languages.

ii. African Charter on Human and People's Rights[11]

The African Charter on Human and Peoples' Rights (also known as the Banjul Charter) is a multilateral human rights instrument that is intended to promote and protect human rights and basic freedoms on the African continent. The Charter was adopted on June 1 1981, came into force on October 21, 1986 and remains the pivotal human rights instrument of the African Union (AU). The Charter established the African Commission on Human and Peoples' Rights to oversee the implementation of individual rights, socio-economic, civil and political rights covered in the charter.[12]

iii. The Malabo Convention[13]

The AU Convention on Cyber Security and Personal Data Protection, also known as the Malabo Convention, is the only binding regional treaty on data protection outside Europe. It came into force on June 8, 2023 after ratification by 15 states, nine years after its adoption on June 27, 2014. The covenant offers a holistic continent-wide framework to harmonise policies on data protection, digital rights, privacy and internet freedom. The Malabo convention seeks to, among other things, achieve two major objectives. Firstly, it requires member states to establish an adequate legal framework that protects fundamental rights and personal data. Secondly, it seeks to balance the fundamental rights of data subjects with that of the prerogatives of the state and the rights of local communities.[14]

iv. ACHPR Declaration of Principles on Freedom of Expression and Access to Information in Africa[15]

The 2019 ACHPR Declaration replaces the 2002 Declaration on Freedom of Expression in Africa, and features new sections on access to information and online rights, guided by hard-law and soft-law standards drawn from African and international human rights instruments and standards, including the jurisprudence of African judicial bodies. The Declaration includes principles on states' obligations to protect online rights, the provision of universal, equitable, affordable and

11. https://au.int/en/treaties/african-charter-human-and-peoples-rights
12. https://achpr.au.int/en
13. https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection
14. https://www.ejiltalk.org/the-african-unions-malabo-convention-on-cyber-security-and-personal-data-protection-enters-into-force-nearly-after-a-decade-what-does-it-mean-for-data-privacy-in-africa-or-beyond/
15. https://achpr.au.int/en/node/902

meaningful access to the internet, protection of personal information online, and communication surveillance.

v. African Union Data Policy Framework[16]

The AU Data Policy Framework (DPF) published in July 2022 is one of the most significant instruments on data governance on the continent. Developed by the AU Commission in consultation with partners inside and outside the AU ecosystem, the DPF was endorsed by the AU Executive Council in February 2022. The DPF is an extensive blueprint to guide African countries' efforts to establish effective data governance regimes to leverage the evolving data and digital revolution. Like most regional and international policy instruments, the DPF is not legally binding on AU member states. Nonetheless, it is an authoritative reference source for governments and advocates of Africa's data revolution.[17]

vi. African Declaration on Internet Rights and Freedoms[18]

The African Declaration on Internet Rights and Freedoms (AfDec) is a pan-African civil society coalition driven 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 peoples' rights on the internet, and to cultivate an internet environment that can best meet Africa's social and economic development needs and goals. AfDec builds on well-established African human rights documents including the African Charter on Human and Peoples' Rights, the Windhoek Declaration on Promoting Independent and Pluralistic Media[19] of 1991, the African Charter on Broadcasting of 2001,[20] the initial Declaration of Principles on Freedom of Expression in Africa of 2002 and the African Platform on Access to Information Declaration[21] of 2011.

vii. African Union Declaration on Internet Governance[22]

The 2017 AU Declaration on Internet Governance was developed through a consultative process with the aim of using the benefits of the digital economy to create a conducive environment for African stakeholders to deliberate on critical

16. https://au.int/sites/default/files/documents/42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf
17. https://cipesa.org/wp-content/files/briefs/Five_Takeaways_From_the_2022_African_Union_Data_Policy_Framework_Brief.pdf
18. https://africaninternetrights.org/about/
19. https://www.veritaszim.net/sites/veritas_d/files/Windhoek-Declaration%281%29.pdf
20. http://www.mediaombudsmannamibia.org/pdf/African_Charter_on_Broadcasting.pdf
21. https://www.africanplatform.org/fileadmin/Content/PDF/APAI-Declaration-English.pdf
22. https://au.int/sites/default/files/newsevents/workingdocuments/33025-wd-african_declaration_on_internet_governance_en_0.pdf

emerging issues and contribute to the development of internet public policies that take into account the needs of Africa. The Declaration acts as the guiding principles for stakeholders and constitutes the shared values for deliberations on the future of the internet from an African standpoint.

1.3
Sub-regional Treaties

Africa has various sub-regional organisations, usually referred to as the RECs (the regional economic communities) - these are:

- the Southern African Development Community (SADC),
- the Intergovernmental Authority on Development (IGAD),
- the Economic Community of Central African States (ECCAS),
- the Arab Maghreb Union (AMU), the Community of Sahel-Saharan States (CEN-SAD),
- the Common Market for Eastern and Southern Africa (COMESA),
- the East African Community (EAC) and
- the Economic Community of West African States (ECOWAS).

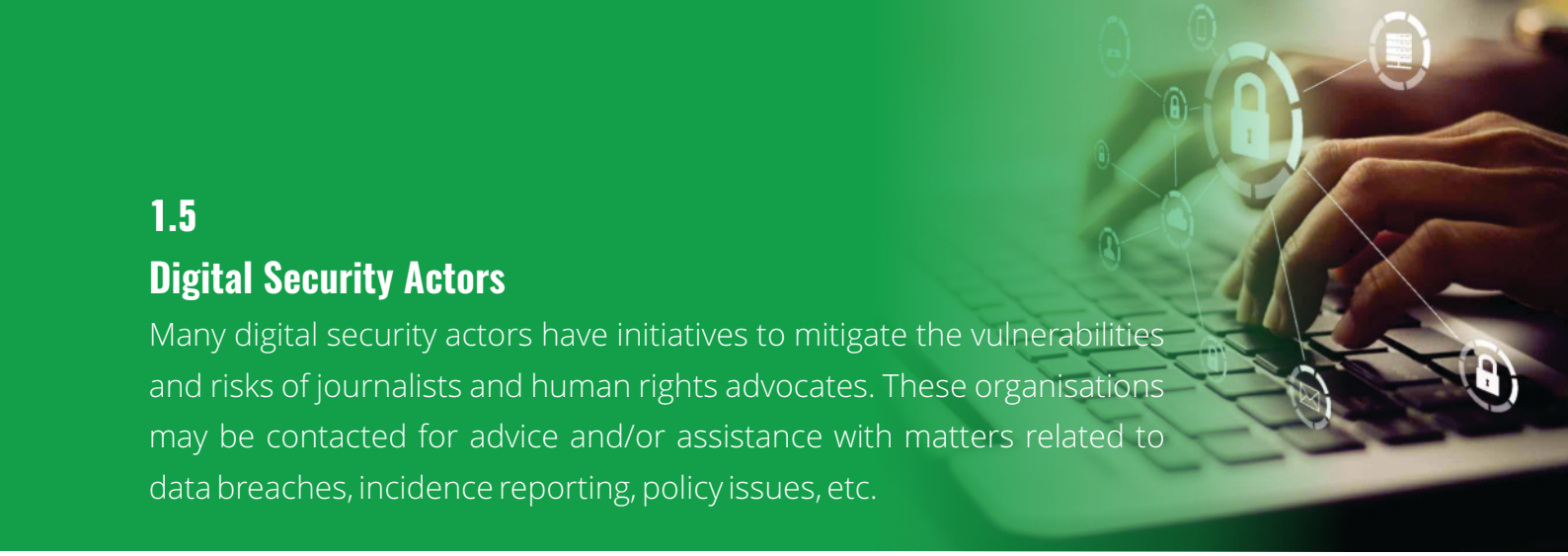
Some of these communities have their own treaties such as the ECOWAS Regional Critical Infrastructure Protection Policy[23] and the ECOWAS Cybercrime Directive (adopted in 2011), the EAC's Model ICT Policy Framework,[24] and SADC has a Model Law on Computer Crime and Cybercrime (2012).[25]

1.4
Country Laws

On a state level, aspects of these charters, declarations and protocols are enforced by human rights law, national data protection laws and sometimes cybercrime laws. According to information published by Data Protection Africa, by January 2024, 35 African countries had passed national data protection legislation and three countries had drafted bills on data protection.[26]

> ***"Digital rights pertain to the rights of individuals to computer access and the ability to use and publish digital contents."***

23. https://www.ocwarc.eu/wp-content/uploads/2021/02/ECOWAS-Regional-Critical-Infrastructure-Protection-Policy-EN.pdf
24. https://eaco.int/admin/docs/publications/EAC_MODEL_ICT_POLICY.pdf
25. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/SADC%20Model%20Law%20Cybercrime.pdf
26. https://dataprotection.africa/



1.5
Digital Security Actors

Many digital security actors have initiatives to mitigate the vulnerabilities and risks of journalists and human rights advocates. These organisations may be contacted for advice and/or assistance with matters related to data breaches, incidence reporting, policy issues, etc.

AccessNow[27]

AccessNow provides a round the clock digital security helpline, evidence-based policy analysis, advocacy and grants to grassroots organisations and activist groups that are working with users and communities most at risk of digital rights violations.

www.accessnow.org

AfricanDefenders[28]

A pan-African human rights defenders network of five African sub-regional organisations,[29] dedicated to the promotion and protection of human rights defenders (HRDs) across the African continent.

www.africandefenders.org

Africa Digital Rights Hub (ADRH)[30]

The Hub is a not-for-profit "think and action tank" that promotes pan-African research and capacity building on digital rights. Focusing on the impact of digital technology on people, the Hub brings together academic researchers, stakeholders, policy makers, regional and international bodies to address digital rights issues in Africa.

www.africandigitalshub.org

27. https://www.accessnow.org/
28. https://africandefenders.org/
29. https://africandefenders.org/members/
30. https://africadigitalrightshub.org/

African Digital Rights Network (ADRN)[31]

This is a network of activists, academics and analysts who carry out research on digital rights in Africa. They carry out novel studies, produce unique reports, and publish a groundbreaking series of digital rights books.

www.africandigitalrightsnetwork.org

Africtivists[32]

A pan-African network of online activists and bloggers for democracy, comprising a community of 200 cyber-activists from 35 different countries.

www.africtivistes.org

Association for Progressive Communication (APC)[33]

The APC works to build a world in which all people have easy, equal and affordable access to the creative potential of ICTs to improve their lives and create more democratic and egalitarian societies.

www.apc.org

Association of Media Women in Kenya (AMWIK)[34]

The AMWIK is a national media association with a focus on enhancing the visibility of women in society and promoting their participation in leadership and decision-making.

www.amwik.org

31. https://www.africandigitalrightsnetwork.org/
32. https://www.africtivistes.org/
33. https://www.apc.org/
34. http://amwik.org/

Association of Privacy Lawyers in Africa (APLA)[35]

APLA is a membership organisation founded in 2022 with a mission to have a centralised effort towards defining, promoting and improving the data privacy legal profession in all African countries.

www.aplaafrica.com

Article 19[36]

Article 19 – working on two interlocking freedoms: the Freedom to Speak, and the Freedom to Know – seeks to make people everywhere express themselves freely and actively engage in public life without fear of discrimination.

www.article19.org

CoCreation Hub Nigeria[37]

Commonly referred to as Cc-HUB or the HUB, it is a platform where technology-oriented people share ideas on solving social problems in Nigeria and beyond.

www.cchub.africa

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)[38]

Based in Kampala, Uganda, CIPESA is an internet policy organisation promoting effective and inclusive ICT policy and practice for improved governance, livelihoods, and human rights in Africa.

www.cipesa.org

35. https://aplafrica.com/
36. https://www.article19.org/
37. https://cchub.africa
38. https://cipesa.org/

Committee to Protect Journalists (CPJ)[39]

An independent, not-for-profit, non-governmental organisation, based in New York City, with correspondents around the world. CPJ promotes press freedom and defends the rights of journalists around the world.

www.cpj.org

Cyber Security Africa[40]

An information security consulting firm offering a comprehensive range of services and products to help organisations protect their valuable assets.

www.cybersecurityafrica.com

Defenders Coalition, Kenya[41]

A national coalition in Kenya to strengthen the capacity of human rights defenders to work effectively and to reduce their vulnerability to the risk of persecution, including by advocating for a favourable legal and policy environment.

www.defenderscoalition.org

Digital Society of Africa (DSA)[42]

The DSA works to strengthen the resilience and ability of frontline activists, human rights defenders and other at-risk groups in the region to independently recognize and respond to digital threats and attacks.

www.digitalsociety.africa

39. https://cpj.org/
40. https://www.cybersecurityafrica.com/
41. https://defenderscoalition.org/
42. https://digitalsociety.africa/

Digital Security Alliance (DSA)[43]

A coalition of organisations and individual digital security experts in Uganda working towards securing the digital assets of civil society, human rights defenders, journalists and other activists in the face of threats posed by powerful corporations, unscrupulous criminals, the state and other non-state actors.

www.defendersprotection.org/dsa/

Freedom House[44]

A US-based not-for-profit, non-governmental organisation that conducts research and advocacy on democracy, political freedom and human rights.

www.freedomhouse.org

Frontline Defenders[45]

A human rights organisation founded in Dublin, Ireland in 2001 to protect those who work non-violently to uphold the human rights of others as outlined in the Universal Declaration of Human Rights.

www.frontlinedefenders.org

Gambia Cyber Security Alliance[46]

The organisation aims to create awareness and increase understanding of Gambians about cyber security, cyber threats, espionage, and empowering them to be safer and more secure online.

www.twitter.com/CyberGambia

43. https://www.defendersprotection.org/dsa/
44. https://freedomhouse.org/
45. https://www.frontlinedefenders.org/
46.https://twitter.com/CyberGambia

Gambia Press Union[47]

The Gambia Press Union is a trade union for journalists in the Gambia, established in 1978 by a group of journalists, with a mission to foster a free and vibrant media.

www.gpu.gm

Human Rights Defenders Network - Sierra Leone (HRDN-SL)[48]

HRDN-SL is a coalition of human rights civil society organisations and individuals working for the protection and promotion of human rights in Sierra Leone.

www.grassrootsjusticenetwork.org

Kenya ICT Action Network (KICTANET)[49]

A multi-stakeholder think tank for stakeholders interested and involved in ICT policy and regulation. Its work is guided by four pillars: policy advocacy, capacity building, research, and stakeholder engagement.

www.kictanet.or.ke

Media Foundation for West Africa (MFWA)[50]

Established in 1997 and based in Accra, Ghana, MFWA is a regional non-governmental organisation to promote and defend the right to freedom of expression of all persons, and particularly the media and human rights defenders in West Africa.

www.mfwa.org

47. https://gpu.gm/
48. https://grassrootsjusticenetwork.org/connect/organization/pan-african-human-rights-defenders-network/
49. https://www.kictanet.or.ke
50. https://www.mfwa.org/

Media Defence[51]

A non-governmental organisation established in 2008 to provide legal assistance to journalists and independent media. It also supports training in media law and promotes the exchange of information, litigation tools and strategies for lawyers working on media freedom cases.

www.mediadefence.org

Paradigm Initiative (PIN)[52]

PIN is a social enterprise that builds an ICT-enabled support system and advocates for digital rights in order to improve livelihoods for under-served youth. PIN's digital rights advocacy programme is focused on the development of public policy for internet freedom in Africa.

www.paradigmhq.org

PeaceWomen[53]

The Women, Peace and Security Programme of the Women's International League for Peace and Freedom (WILPF),[54] a global feminist peace building organisation.

www.peacewomen.org

Pollicy[55]

A feminist collective of technologists, data scientists, creatives and academics working at the intersection of data, design and technology to craft better life experiences by influencing a culture of responsible data use, promoting appropriate data governance practices and

51. https://www.mediadefence.org/
52. https://paradigmhq.org/
53. https://www.peacewomen.org/
54. http://wilpf.org/
55. https://pollicy.org/

advocating for policies that support an enabling data ecosystem.

www.pollicy.org

Safe Sisters[56]

Safe Sisters is a fellowship programme for women human rights defenders, journalists, media workers and activists. Fellows are trained to understand and respond to the digital security challenges they face in their work and daily life.

www.safesisters.net

Women of Uganda Network (WOUGNET)[57]

WOUGNET promotes the use of information and communication technologies among women and girls as tools to share information and address issues such as gender equality and sustainable development.

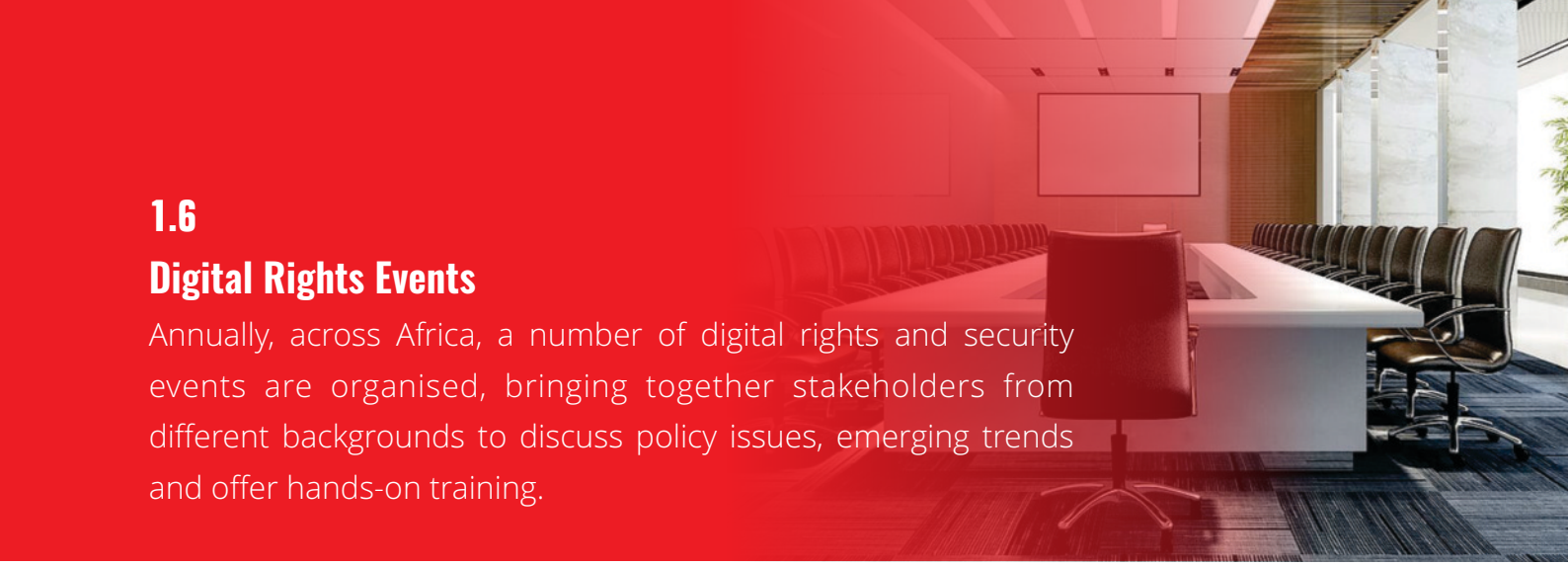
www.wougnet.org

Zambian Cyber Security Initiative Foundation[58]

The ZCSI is an organisation that provides knowledge and tools to stay safe and secure in today's digital world and protect individuals and organisations from the harm caused by cyber threats.

www.zcsi-foundation.org

56. https://safesisters.net/
57. https://wougnet.org
58. https://zcsi-foundation.org/



1.6
Digital Rights Events

Annually, across Africa, a number of digital rights and security events are organised, bringing together stakeholders from different backgrounds to discuss policy issues, emerging trends and offer hands-on training.

i. African School on Internet Governance (AfriSIG)[59]

A multi-stakeholder training initiative that aims to give Africans the opportunity to gain knowledge and confidence to participate effectively in internet governance processes and debates nationally, regionally and globally.

Other internet governance schools on regional and national levels include:

- West Africa School of Internet Governance (WASIG)[60]
- Kenya School of Internet Governance (KeSIG)[61]
- Nigeria School on Internet Governance (NSIG)[62]
- South Sudan School of Internet Governance (SSSIG)[63]
- Arusha Women School of Internet Governance (AruWSIG)[64]

ii. Digital Rights and Inclusion Forum (DRIF)[65]

DRIF is a bilingual forum hosted every April by Paradigm Initiative where tough topical global issues around internet rights, especially in Africa, are discussed between civil society, technology companies, government, academia and other stakeholders.

iii. Forum on Internet Freedom in Africa (FIFAfrica)[66]

Hosted annually in September by CIPESA,[67] FIFAfrica focuses on promoting a free and open internet in Africa.

59. https://afrisig.org/
60. https://waigf.org/about-wasig/
61. https://kigf.or.ke/kesig/
62. https://sig.ng/
63. https://ssigf.org.ss/about-ss-sig/
64. https://www.ksgen.or.tz/aruwsig/
65. https://drif.paradigmhq.org/
66. https://internetfreedom.africa/
67. https://cipesa.org/service/forum-on-internet-freedom-in-africa/

1.7

Digital Rights Case Studies

Attempts by states to violate the rights of journalists and digital rights defenders through legislation, internet shutdowns and court actions, amongst other means, are demonstrated with the following examples across Africa:

Case Studies

Cameroon

In this country it is impossible for a media outlet to adopt a critical and independent editorial policy without being exposed to significant threats and harassment if its reporting endangers the interests of the government and its representatives. This repressive environment fuels self-censorship and results in most media outlets falling in line with the views of the authorities or those close to them. Cameroonian journalists, especially those who are critical or outspoken, are constantly at risk of verbal or physical attack, for example journalist Martinez Zogo's badly mutilated body was found five days after he was abducted in January 2023.[68] As the host of a popular daily radio show, Embouteillage (or Gridlock in English), he regularly tackled cases of corruption and alleged embezzlement, not hesitating to mention important personalities by name. The murder of Martinez Zogo left many people shocked as NGOs continued to call out violations of press freedom and freedom of speech.[69]

Egypt

On August 22, 2023 plainclothes state security forces arrested Gamal Abdelhamid Ziada, the father of Belgium-based freelance Egyptian journalist Ahmed Gamal Ziada, on a street in Giza, according to news reports and a tweet by the journalist.[70] The next

68. https://rsf.org/en/country/cameroon
69. Cameroonian prosecutors wind up probe into the murder of Martinez Zogo | Africanews
70. زيادة جمال أحمد المصري الناشط والد اعتقال

day prosecutors charged the father Gamal Ziada with misusing social media, spreading false news and belonging to a banned group, and ordered his detention pending trial. Ahmed Gamal Ziada covers human rights issues and Egyptian foreign policy for regional independent news websites including Raseef, Daraj and Middle East Eye.[71] The Egyptian government continued to silence critics through arrests and unfair prosecutions of journalists and bloggers, and the parliament issued severely restrictive laws that further curtail freedom of speech and access to information. In addition to using the state security courts, where judgments cannot be appealed, authorities continue to prosecute thousands of civilians in military courts. Both court systems are inherently abusive and do not meet minimum due process standards, according to the Human Rights Watch 2019 World report.[72]

Nigeria

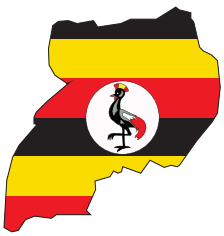
Surveillance technology has been used to spy on peaceful activists, opposition politicians and journalists, singling them out for harassment, arrest and torture, in violation of international human rights law and supplier companies' own self-policing measures. Nigeria is a leading customer of every major surveillance technology, including internet and mobile and internet interception, social media monitoring, biometric ID data and the so-called *'safe city'* monitoring of citizens in public spaces. For instance, Omoyele Sowore, a human rights activist and former presidential candidate, found that the Nigerian government had deactivated his biometric identification in January 2022. This meant that his national identification card, permanent voter card, foreign passport and driver's licence were among the deactivated documents, preventing him from travelling, driving or voting.[73]

71. https://cpj.org/2023/08/egyptian-authorities-arrest-father-of-freelance-journalist-ahmed-gamal-ziada/
72. https://www.hrw.org/world-report/2019/country-chapters/egypt
73. https://www.ids.ac.uk/press-releases/nigeria-spending-billions-of-dollars-on-harmful-surveillance-of-citizens/

Tanzania

According to a 2022 US State Department report on human rights practices,[74] on June 27, 2022 the government issued a letter to DarMpya Media accusing the media outlet of misrepresenting a June 17 demonstration outside the Kenyan Embassy in Dar es Salaam, related to tension between Maasai residents and authorities in Loliondo. The government accused DarMpya of operating without a licence and prohibited the outlet from publishing online content. DarMpya applied to renew its publishing licence in August of the same year, which was subsequently denied by the Tanzania Communications Regulatory Authority (TCRA).

Uganda



Internet Shutdown During 2021 Elections and arrest of journalist and oppositions (January 2021): The Ugandan government shut down internet access and social media platforms during the January 2021 presidential and parliamentary elections, hindering communication and access to information.[75] Network data from the NetBlocks Internet Observatory confirms widespread restrictions to social media and online communication platforms on major internet providers in Uganda from Tuesday 12 January, two days before the elections. The findings by NetBlocks reveal the extent of restrictions issued by order[76] of the Uganda Communications Commission ahead of the elections on the 14th.[77] The blackout was lifted on the Monday after the elections, more than 100 hours after imposing it. Authorities apologised for the inconvenience and said the shutdown was to avoid outside interference in the elections, which long-time leader Yoweri Museveni was declared to have won against popular singer-turned-politician Bobi Wine.[78]

74. https://www.state.gov/reports/2022-country-reports-on-human-rights-practices/tanzania/
75. https://www.hrw.org/world-report/2022/country-chapters/uganda
76. https://www.reuters.com/article/us-uganda-election/uganda-bans-social-media-ahead-of-presidential-election-idUSKBN29H0KH
77. https://www.business-humanrights.org/en/latest-news/uganda-shuts-down-internet-ahead-of-general-election/
78. https://www.reuters.com/article/us-uganda-internet-rights-trfn-idUSKBN29P1V8/

1.8
Model Policy Briefs

The roles of digital rights advocates, journalists and other social activists are better appreciated when they are seen to contribute to providing solutions to the myriad of challenges facing society.

Here is a toolkit[79] to develop effective policy briefs, and examples of such policy briefs include:

- Africa's Absence in Emerging Technologies[80]
- Assessing The United Nations Cybertreaty Process[81]
- Artificial Intelligence in Kenya[82]
- Censorship and Content Moderation in Angola, Central African Republic and Democratic Republic of Congo[83]
- Towards an Inclusive National Action Plan on Business and Human Rights in Nigeria[84]

1.9
Model Coalition Statements

The rise within African governments' circles to regulate the use of social media through legislation with vague or broad terms serve

79. https://socialwork.utoronto.ca/wp-content/uploads/2021/06/Policy-Toolkit-Final-v2-Apr27.pdf
80. https://paradigmhq.org/report/policy-brief-africas-absence-in-emerging-technologies/
81. https://paradigmhq.org/report/policy-brief-assesing-the-united-nations-cybertreaty-process/
82. https://paradigmhq.org/report/policy-brief-artificial-inteligence-in-kenya/
83. https://paradigmhq.org/report/policy-brief-censorship-and-content-moderation-in-angola-central-african-republic-and-democratic-republic-of-congo/
84. https://paradigmhq.org/report/policy-brief-towards-an-inclusive-national-action-plan-on-business-and-human-rights-in-nigeria/

to decrease the openness of the internet, mask human rights violations and create barriers to long-term stability and peaceful dialogue. The ability to oppose this tendency is strengthened when stake-holders come together with a single voice. Examples of coalition statements made to address such issues include:

- A 2023 open letter signed by a range of organisations on the blocking of Telegram in Kenya.[85]
- A 2023 joint statement on behalf of 59 countries presented at the UN Human Rights Council on the heightened risks associated with surveillance technologies and the importance of safeguards in the use of these tools.[86]
- An international group of organisations and experts calling on the Indian government to withdraw the 2023 Telecommunications Bill and to protect fundamental rights.[87]
- A statement of the NetRights Coalition condemning raids on digital technologies of civil society actors in Zimbabwe during the 2023 elections.[88]
- A 2023 NetRights Coalition statement against blanket social media regulation in Nigeria.[89]

85. https://www.accessnow.org/press-release/open-letter-clarification-on-telegram-blocking-in-kenya/
86. https://freedomonlinecoalition.com/joint-statement-heightened-risks-associated-with-surveillance-technologies-and-the-importance-of-safeguards-in-the-use-of-these-tools/
87. https://www.accessnow.org/press-release/india-must-withdraw-the-telecommunications-bill-2023/
88. https://paradigmhq.org/press-release-the-netrights-coalition-condemns-raids-of-digital-technologies-of-civil-society-actors-in-zimbabwe-during-the-2023-elections/
89. https://paradigmhq.org/the-netrights-coalition-strongly-condemns-the-call-for-blanket-social-media-regulation-in-nigeria/

CHAPTER 02

DIGITAL SAFETY AND SECURITY

Digital safety, interchangeably referred to as internet safety, online safety or cyber safety, refers to an array of practices and precautions adhered to by an individual when using the internet in an effort to ensure that sensitive personal information and that of their device(s) remain secure.

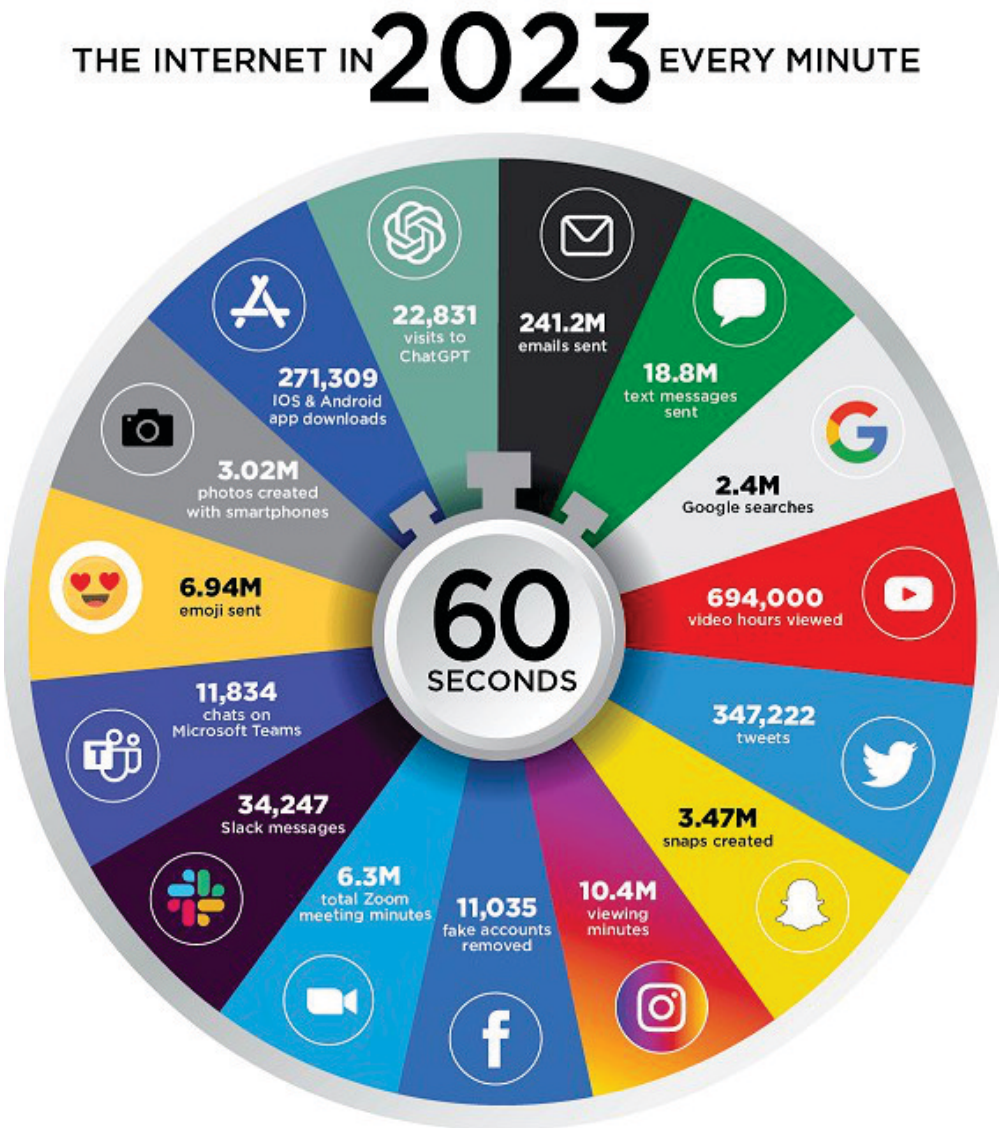
According to a 2023 *"What happens in an internet minute"* infographic,[90] 241.2 million mails, 347,222 tweets, and 18.8 million text messages are sent every 60 seconds. With ITU 2023 statistics[91] indicating that over 5.4 billion people, or 67 per cent of the world's population are connected online, this could only mean that more bad actors, hackers, threats and online scams lurk than ever before.

90. https://ediscoverytoday.com/2023/04/20/2023-internet-minute-infographic-by-ediscovery-today-and-ltmg-ediscovery-trends/
91. https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

241.2 Million
Mail

347,222
Tweets

18.8 Million
Text Messages



2.1
Digital Safety Threats

Here are some common digital safety threats everyone needs to be aware of.

i. Malware

Malware is short for "malicious software." It is a programme or file designed to be disruptive, invasive and harmful to a computer system and mobile devices. It is most frequently transmitted through e-mail attachments, instant messages (IM), downloads, phishing and misleading websites. Malware outbreaks cause harm by destroying data on infected devices and/or by increasing network traffic that can cause complete network breakdowns. Furthermore, malware can allow attackers to get any information they want from a compromised computer, including a journalist's personal information, data and sources.

Types of malware include:

Adware - This is a type of software that maliciously instals itself on your device and is designed to display unsolicited advertisements and pop-ups.

Cryptojacking - This type of malware hijacks a device for the purpose of using it for bitcoin mining, significantly increasing processing on the device which slows it down and drains the battery.

Ransomware - A type of malware that is designed to block access to all or part of a computer system until a sum of money is paid, although payment does not guarantee that access will be restored. Because attackers are looking to maximise their payday, the targets are typically larger entities (organisations, departments, colleges, businesses) that not only are likely to have the funds, but also experience a significant loss when they cannot access their systems. However, individuals are still a target of ransomware because they can be a doorway into an organisation's systems.

Spyware - This is malicious software that is secretly installed on a person's computer or mobile device in order to obtain the owner's private information, such as lists of websites visited, passwords and credit card numbers.[92]

Trojans - These are deceptive programmes maliciously downloaded to a device that allows a cybercriminal remote access to the host device, subjecting the device to a variety of malicious or destructive activities, or even just monitoring (spying) activities or interactions on the device.

Viruses - A type of malware that attaches itself to another programme and has the ability to spread between devices and cause damage to data and software. If viruses are not halted quickly, the flood of emails can swamp servers, disrupting email services for all.

Worms - A computer worm is a type of malware that automatically replicates itself as it spreads to other computers across a network.

92. https://www.britannica.com/technology/spyware

Hints of Possible Malware Infection on Your Device

- Unusually slow or frozen system functionality.
- Spam and pop-up ads.
- Frequent system crashes.
- Unknown icons on the desktop.
- Redirection from a popular website to an unknown one.
- New files or folders created without your permission.
- Battery power runs out quickly.

ii. Digital Surveillance Threats

It includes location tracking, facial recognition, mass monitoring and the interception of communications. Surveillance has a detrimental effect on writers' and reporters' ability to research and publish stories, and makes it harder for them to protect sources.

iii. Social Engineering Attacks

Social engineering is a technique used to deceive users into disclosing certain information, performing a specific action for illegitimate reasons, or providing an entry point for malware. This can be an attempt by a stranger to extract information from you that you normally wouldn't share online, for example credit card details, date of birth, favourite vacation spot, pet's name. Do they really need that information? The answers to these questions may result in compromised accounts.

Some forms of Social Engineering include:

Phishing attacks - "Phishing" or "spear phishing" campaigns often use links or attachments in e-mail or on social media that carry malware. Once these links are clicked on, they can do significant damage.[93]

Smishing - Also known as SMS-phishing, it is a type of social engineering assault that is carried out through SMS messages. Scammers try to trick the user into clicking on a link that takes them to a malicious website in this attack.[94]

Vishing - A form of phishing in which individuals are tricked into disclosing sensitive information over the phone or via voicemail.[95]

93. https://www.exabeam.com/information-security/cyber-security-threat/
94. https://www.aura.com/learn/types-of-social-engineering-attacks
95. https://www.exabeam.com/information-security/cyber-security-threat/

Baiting - A form of social engineering attack in which scammers offer something of value to the victim in exchange for the victim providing sensitive personal information. For instance, the victim might get an email promising them a free gift card in exchange for clicking on a link.[96]

Pretexting - A type of social engineering where cybercriminals impersonate a trustworthy source to convince victims to share valuable or sensitive information.[97]

iv. Fake Domain Attacks

These are websites created to impersonate legitimate ones for malicious purposes. Independent media and civil society websites have often been victims. The fake sites serve up malware or publish false information in an effort to discredit the real media site or a particular journalist.

v. Man-in-the-Middle (MitM) Attacks

A man-in-the-middle attack is a cyberattack in which the attacker can secretly intercept messages between two or more parties who believe they are communicating with each other.[98] For example, a wireless router is configured to act as a Wi-Fi hotspot in a public place, to trick people into thinking it's legitimate. When individuals connect to it, the attacker has instant access to the data passing through the router.

vi. Distributed Denial of Service (DDoS) Attacks

These attacks are quite common, and involve one or more computers and internet connections flooding a server with traffic, making it inaccessible to others. For news websites, these attacks prevent information from reaching the public and can become costly, as visitor numbers drop and technical help is needed.

96. https://www.aura.com/learn/types-of-social-engineering-attacks
97. https://www.aura.com/learn/types-of-social-engineering-attackshttps://www.aura.com/learn/types-of-social-engineering-attacks
98. https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/man-in-the-middle-attack-mitm/

Cyberstalking

The use of the internet or other electronic means to stalk and/or harass an individual, group, or organisation. It may include false accusations, defamation, slander and libel. It may also include monitoring, identity theft, threats, vandalism, or gathering information that may be used to threaten, embarrass or harass.

Cyberbullying

The use of electronic means such as e-mail, social media, instant messaging and other forms of online communication with the intent to abuse, intimidate, or overpower an individual or group.

Preventive Measures for Digital Threats

With a little bit of effort, you can protect your computer and help avert more wide-ranging problems. The following steps will prevent an attack or deal with viruses if a computer becomes infected:[99]

- **Install antivirus software:** Anti-malware tools help to detect and remove malware from your computer or mobile device.
- **Keep applications updated:** Ensure all applications are up to date. Outdated applications that don't have the most recent security patches make them vulnerable to malware.
- **Limit access to network file shares:** Only allow the level of access required by the user's business function. Limiting access to network file shares will prevent a device infected with ransomware spreading it to other devices on the network.
- Don't open or execute unexpected attachments.
- Turn off the preview feature in your programmes for added protection.
- Turn off any programme features that may automatically open an email, instant message, attachment file or download.

99. https://it.osu.edu/security

2.2

Digital Hygiene

To guarantee the digital safety of journalists, digital rights defenders and other internet users, an array of digital hygiene measures are available to help curb digital security threats and incidents.

Digital hygiene (or cyber hygiene or internet hygiene) is the catch-all term for the practices and behaviours related to cleaning up and maintaining our digital world. This includes everything from organising the files on your digital device to protecting your digital identity and the associated data, and it also includes installing new apps or technologies to make your digital life easier and more secure.

By safeguarding the information you share online and/or securing the devices you use, you reduce both the likelihood of getting attacked and the severity of a successful attack. Whatever you post online can become a source or a piece of information used by a bad actor to launch a scam or cyber-attack against you. As a digital rights actor, maintaining good digital hygiene practices is key to keeping you safe on the internet.

The rest of the chapter lists some easy things you can do, without purchasing expensive technology or investing a lot of time in reconfiguring your home network, to make your online computing safer.

2.3
Passwords

If you are looking for a way to improve your cyber security, password security is where you should start. A password is a basic security mechanism that ideally consists of a secret passphrase created using alphabetic, numeric, alphanumeric and symbolic characters, or a combination. This security mechanism is used to restrict access to a system, application or service to only those users who have memorised or stored and/or are authorised to use it.

The standard digital safety practice involves creating strong passwords, not reusing passwords, using passphrases and multi-factor authentication, carefully considering password reset questions, not writing down passwords, and last but not least, using a password manager.

> ***"A password is a basic security mechanism that ideally consists of a secret passphrase created using alphabetic, numeric, alphanumeric and symbolic characters, or a combination."***

Password Generators

A password generator is a software tool that creates random or customised passwords for users. It helps users create stronger passwords that provide greater security for a given type of access.

Password generators help those who have to constantly come up with new passwords to ensure authorised access to programmes and to manage a large number of passwords for identity and access management.

Password Managers

A password manager is a tool that creates and stores passwords so that many different passwords may be used on different sites and services without having to memorise them.

Password managers:

- generate strong passwords that a human being would be unlikely to guess.
- store several passwords (and responses to security questions) safely.
- protect all passwords with a single master password (or passphrase).[100]

If your computer or device gets compromised and spyware is installed, the spyware can watch you type your master

100. https://ssd.eff.org/glossary/passphrase

password and could steal the contents of the password manager. So it is still very important to keep your computer and other devices clean of malware when using a password manager.

Note!

Using password managers is like putting all your eggs in one basket and protecting them with your life. The risk with hacked password managers is that access to the "basket" means access to all your "eggs".

Syncing Passwords Across Multiple Devices[101]

Many password managers allow access to passwords across devices through a password-synchronisation feature. This means when a password file is synced on one device, it is automatically available on all other devices.

Password managers can store passwords *"in the cloud,"* meaning encrypted on a remote server. When the passwords are needed, these managers will retrieve and decrypt[102] the passwords automatically. Password managers that use their own servers to store or help synchronise passwords are more convenient, but are slightly more vulnerable to attacks. If passwords are stored both on the computer and in the cloud, an attacker does not need to take over the computer to find out the passwords. (They will need to break the password manager's passphrase though.) If this is concerning, do not sync passwords to the cloud, instead opt to store them on just the devices.

Note!

Keep a backup of the password database just in case. Having a backup is useful if the password database is lost in a system crash, or if the device is taken away. Password managers usually have a way to make a backup file, or one can use the regular backup programme.

101. https://ssd.eff.org/en/module/creating-strong-passwords#3
102. https://ssd.eff.org/glossary/decrypt

Common Password Attacks

One of the easiest and most common ways to hack into an account is to try[103] common passwords or to do a little research on the intended victim and try some passwords related to that person. A 2024 Cybernews report revealed that the top 10 most commonly-used and hacked passwords were:

1. 123456
2. 123456789
3. qwerty
4. password
5. 12345
6. qwerty123
7. 1q2w3e
8. 12345678
9. 111111
10. 1234567890

These are VERY insecure passwords. They are easy to guess and cyber criminals will start trying to access accounts with perceived weak passwords like these.

NEVER use passwords that contain the following information:

- Your name or the names of your family and friends,
- Your birthday or those of your family and friends,
- Pets names, and
- Places you live or have lived including cities or street names.

It is amazing how much information about a person is out there on the internet. So if your password contains information that pertains to you in a way that can be discerned from the internet or by talking to your friends, it can be easily guessed.

Brute Force Attack

A brute force attack simply tries every possible combination of allowed characters until it finds a match. This kind of attack is very effective on shorter passwords and it will even be able to hack passwords composed of randomised characters. But the length does matter. A brute force attack is not very efficient, and if your password is long enough, it may be impractical to hack. Take a look at the table that shows the time it would take to detect a password on a file with a brute force attack, based on the password length and complexity. Keep in mind that this table assumes that the computer can try significantly more than 1000 passwords per second.

103. https://edition.cnn.com/2019/04/22/uk/most-common-passwords-scli-gbr-intl/index.html

Password Length	All Characters	Only Lower Case
3 characters	0.86 seconds	0.02 seconds
4 characters	1.36 minutes	0.46 seconds
5 characters	2.15 hours	11.9 seconds
6 characters	8.51 days	5.15 minutes
7 characters	2.21 years	2.23 hours
8 characters	2.10 centuries	2.42 days
9 characters	20 millennia	2.07 months
10 characters	1,899 millennia	4.48 years
11 characters	180,365 millennia	1.16 centuries
12 characters	17,184,705 millennia	3.03 millennia
13 characters	1,627,797,068 millennia	78.7 millennia
14 characters	154,640,721,434 millennia	2,046 millennia

Notice that the time to hack a password increases exponentially with each character added. For a password that consists of randomised characters of all types, the difference between 6, 7, 8 and 9 characters is days, years, centuries and millennia! Also, notice how much longer it takes to hack a password that contains all types of characters compared to a password of the same length that uses only lower case characters.

Creating and Maintaining Strong and Secure Passwords

Reusing passwords is an exceptionally bad security practice. If a bad actor gets hold of a password that you've reused across multiple services, they can gain access to many of your accounts. This is why having multiple, strong, unique passwords is so important. Fortunately, a password manager can help.[104]

104. https://ssd.eff.org/en/glossary/password-manager

Tips for creating strong passwords:

- Use a combination of capital and lower-case letters, numbers and symbols.
- A strong password should be between eight and twelve characters long.
- Avoid the use of personal data.
- Change it regularly.
- Never use it for multiple accounts.
- Use multi-factor authentication.

There are a few passwords that you should memorise and that need to be particularly strong. These include:

- passwords for your device
- passwords for encryption (like full-disk encryption)[105]
- the master password,[106] or "passphrase,"[107] for your password manager
- your email password[108]

Creating Strong Passwords Using Dice

One of the many difficulties when people choose passwords themselves is that people are not very good at making random, unpredictable choices.[109] An effective way of creating a strong and memorable password[110] is to use dice[111] and a word list[112] to randomly choose words.

Together, these words form your "passphrase." A "passphrase" is a type of password that is longer for added security. For disk encryption and your password manager, we recommend selecting a minimum of six words.

Why use a minimum of six words? Why use dice to pick words in a phrase randomly?

The longer and more random the password, the harder it is for both computers and humans to guess. To find out why you need such a long, hard-to-guess password, here's a video explainer:[113]

105. https://ssd.eff.org/en/glossary/encryption
106. https://ssd.eff.org/glossary/master-password
107. https://ssd.eff.org/en/glossary/passphrase
108. https://ssd.eff.org/en/glossary/password
109. http://people.ischool.berkeley.edu/~nick/aaronson-oracle/
110. https://www.eff.org/deeplinks/2016/07/new-wordlists-random-passphrases
111. https://www.eff.org/dice
112. https://www.eff.org/deeplinks/2018/08/dragon-con-diceware
113. https://ssd.eff.org/en/module/animated-overview-how-make-super-secure-password-using-dice

when you log in with your username and password that account server is going to ask for a second, independent form of authentication before it will actually let you into the system. It is similar to when a bank account is opened and they ask to see a picture ID and some other form of identification, like the social security card or international passport. It is much harder to pretend you are someone you are not when you have to prove who you are in two different ways.

2.4
Multi-Factor Authentication (MFA)

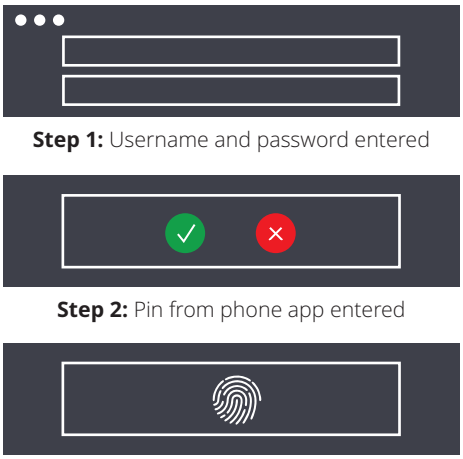
Strong, unique passwords make it much harder for bad actors to gain access to digital accounts. To further protect your digital accounts, enable two-factor authentication.[114]

MFA is a security feature offered by many websites, applications and devices that dramatically improves account security. Technically, MFA refers to a system where there are more than two forms of authentication.

How Multi-Factor Authentication works

If you have an MFA setup for a given account (website, application or device),

Multi-Factor Authentication



Step 1: Username and password entered

Step 2: Pin from phone app entered

Step 3: Fingerprint verified

> ***"Strong, unique passwords make it much harder for bad actors to gain access to digital accounts."***

114. https://ssd.eff.org/en/glossary/two-factor-authentication

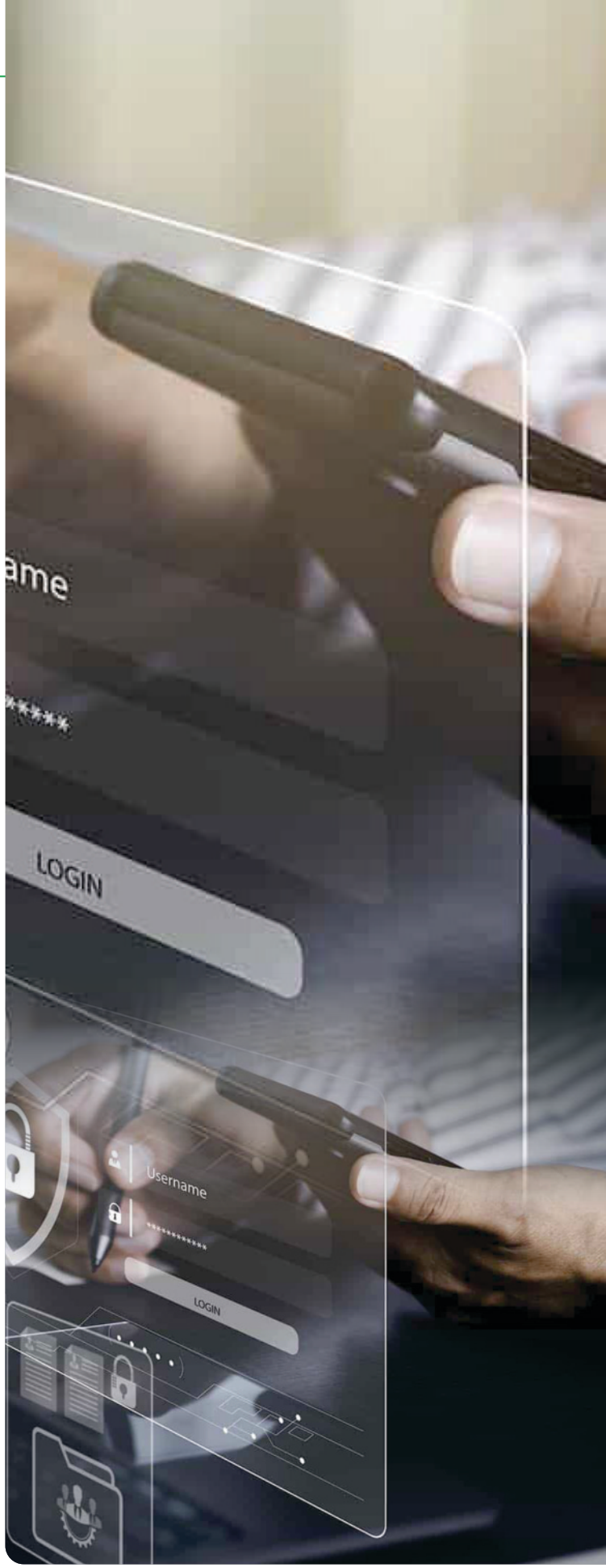
Multi-Factor Authentication Methods

We recommend registering at least two devices for multi-factor authentication, so if you lose one device, you can protect yourself by wiping off the data remotely and then use the other device to authenticate. With MFA, the second authentication can be done using one of several different methods.

The most common methods include:

i. Mobile Device Application "Push Notification" Method

The most popular way to get the second form of authentication is through a "push" to an application on your mobile device. With this method, the account server that you are trying to log into will send a notification to your mobile device. The notification will pop up on the mobile device and say something along the lines of, *"Hey, someone is trying to log in to this website, is it you? Should we let them in?"* Usually there is a big green button and a big red one so that you can easily answer "Yes" or "No". If you hit "Yes", you are in. But if you did not make the original login request, you know that someone has your password and is trying to log in to your account. You can hit the "No" button and their access will be denied. You can then go and log in yourself and change your password so that the attacker is back to square one.



ii. Mobile Device Authenticator Apps

Sometimes the account server will not send you a push notification but it may ask you to type in a unique code that is generated by the authenticator app on your mobile device. These codes are short (maybe 6 digits or more) so it may seem like they are not very secure. The cool thing is that the codes are re-generated every minute or so and they are based on an algorithm that is known only to your authenticator app and the account server you are trying to connect to. It would be extremely difficult for a cyber-criminal to correctly guess the 6 digit code under those circumstances since the time frame is so short. Again, the main advantage here is that the attacker has to have physical access to your mobile device and the ability to log in to it. One downside is that you do not get any real-time notification if someone tries to log into your account. Usually this method is an option as a backup to the push method as well. Most authenticator apps will support both methods.

iii. SMS Code Method

This method also uses your mobile device but it does not use an application. Therefore, it works with non-smartphones. If you set up this method of MFA, when you log in with your username and password, the account server will send your mobile phone a text message with a one-time code. You will then type that code into the website or device portal where you entered your password. This basically has all the advantages of the "push" method, it just isn't quite as convenient because you have to type in the code. You will get that real-time notification of a login attempt and you will get a text message per attempt. One downside is that an attacker doesn't necessarily have to be able to log in to your phone. They do have to physically have the phone as text messages often pop up on the screen of the phone, even when the phone is locked.

iv. Email Code Method

This method works very much like the SMS code method, except that the code is sent to an email account that you have registered with the account server you are trying to access. You will most often set this up when you register for the multi-factor service you are using. If you are going to use this kind of MFA, you will need to make sure that your email account itself is secure, which probably means that you should have MFA enabled for access to your email account. The reason is that email can be checked from anywhere, including the same computer terminal where the cybercriminal is trying to log in to your account. In other words, this method does

not require physical access to any independent device. That is why you should have a strong password for your email that is not used anywhere else. If you do that, then this method would essentially require the attacker to know two of your passwords. However, forcing them to have access to another device is a stronger, more secure option. If a website allows only this type of MFA, that is fine. Go ahead and set it up, and then request authentication to your mobile device for access to your email.

v. Physical Token

This method was more popular before the advent of smartphones. A physical token is a small device that continuously generates codes in the same way that an authentication app on your mobile device would. It works just as well, but it has the added downside that you have to keep track of this other device. These days, our lives are tied to our mobile phones. You can imagine the possibility of losing a token and not even realising it is gone for a while. If you have one of these, keep it in a safe location. If you have to carry it around, maybe attach it to your keychain.

vi. Biometrics

Biometric MFA relies on the unique physical or behavioural characteristics of the user, such as facial recognition, fingerprint scan,

iris scan, voice recognition, etc. Because everyone has a unique fingerprint and face, this can be quite secure. Biometrics is commonly used as an MFA for apps with sensitive data.

Biometric MFA can provide a higher level of assurance that the user is who they claim to be, as biometric data is harder to forge, steal, or guess than passwords or tokens. However, it also has its disadvantages, such as privacy concerns. Biometric authentication systems store sensitive information. If this information falls into the wrong hands, it can be exploited for identity theft or other malicious purposes. Despite its challenges, biometric authentication is more reliable and harder to compromise than other types of authentication methods, and there are ways to mitigate any potential security risks by carefully implementing additional strong security practices using MFA, which combines biometrics with other authentication factors to provide an extra layer of security.

2.5

Two-Factor Authentication (2FA)

Two-Factor Authentication is a type, or subset, of MFA and it is a way to let users identify themselves to service providers by requiring a combination of two different authentication methods. These may be something that the user knows (like a password or PIN), something that the user possesses (like a hardware token or mobile phone), or something that is attached to or inseparable from the user (like their fingerprints).

How does 2FA work online?

Several online services – including Facebook, Google, and X – offer 2FA as an alternative to password-only authentication. If you enable this feature you will be prompted for both a password and a secondary method of authentication. This second method is typically either a one-time code sent by SMS or a one-time code generated by a dedicated mobile app that stores a secret (such as Google Authenticator, or Duo Mobile). In either case, the second factor is your mobile phone, something you (normally) possess. Some websites (including Google) also support single-use backup codes, which can be downloaded, printed on paper, and stored in a safe location as an additional backup

Once you have opted-in to using 2FA, you will need to enter your password and a one-time code from your phone to access your account.

Why should you enable 2FA?

2FA offers you greater account security by requiring you to authenticate your identity with more than one method. This means that, even if someone were to get hold of your primary password, they could not access your account unless they also have your mobile phone or another secondary means of authentication.

Are there downsides to using 2FA?

Although 2FA offers a more secure means of authentication, there is an increased risk of getting locked out of your account if, for example, you misplace or lose your phone, change your SIM card[115] or travel to a country without turning on roaming.

115. https://ssd.eff.org/en/glossary/sim-card

Similarly, using 2FA means you may be handing over more information to a service than you are comfortable with. Suppose you use X, and you signed up using a pseudonym.[116] Even if you carefully avoid giving X your identifying information, and you access the service only over Tor or a VPN,[117] as long as you enable SMS 2FA, X will necessarily have a record of your mobile number. That means if compelled by a court, X can link your account to you via your phone number. This may not be a problem if you already use your legal name on a given service, but if maintaining your anonymity is important, think twice about using SMS 2FA.

Universal Factor Authentication

Universal authentication, also known as single sign-on (SSO), is a network identity verification method that allows users to navigate from site to site securely without having to enter identifying information multiple times. With universal authentication a subscriber enters one set of parameters (such as a username and password) at the start of every network session. The authentication data for any site visited thereafter is automatically generated for the duration of that session. One of the biggest challenges with internet security is the fact that every website has its own authentication system. A typical internet user who has two or three web-based e-mail addresses and frequents half a dozen online vendors to buy or sell things, must memorise several usernames and passwords. This can be difficult unless the authentication data is written down or stored as a text file, which then becomes a security issue. Universal authentication can eliminate this problem without compromising security or privacy.

Note!

If you have a choice, pick the authenticator application or stand-alone hardware device instead of receiving codes by text message. It is easier for an attacker to redirect these codes to their own phone than it is to bypass the authenticator.

> ***"Universal authentication is a network identity verification method that allows users to navigate from site to site securely without having to enter identifying information multiple times."***

116. https://ssd.eff.org/en/glossary/pseudonym
117. https://ssd.eff.org/en/glossary/vpn

2.6
Firewalls

A network security system that protects a computer from unwanted connections to or from local networks and the internet, especially intranets, firewalls can be implemented as both hardware and software, or a combination of both. A firewall[118] might have rules that forbid outgoing email, or connections to certain websites. Firewalls can be used as a first line of defence to protect a device from unexpected interference. They can also be used to prevent users from accessing the internet in certain ways.

Hardware and Software Firewalls

Firewalls can be either hardware or software but the ideal configuration will consist of both. In addition to limiting access to your computer and network, a firewall is also useful for allowing remote access to a private network through secure authentication certificates and logins.

Hardware firewalls can be purchased as a stand-alone product but are typically found in broadband routers, and should be considered an important part of your system security and network set-up. Most hardware firewalls will have a minimum of four network ports to connect other computers, but for larger networks, a business networking firewall solution is available.

Software firewalls are installed on your computer, like any software programme, and you can customise it, allowing you some control over its function and protection features. A software firewall will protect your computer from outside attempts to control or gain access to your computer.

Firewalls may also be a component of your computer's operating system. For example, Windows Firewall is a Microsoft Windows application that notifies users of any suspicious activity. The app can detect and block viruses, worms, and hackers to execute harmful activities.

118. https://ssd.eff.org/en/glossary/firewall

Firewall Filtering Techniques

Firewalls are used to protect both home and corporate networks. A typical firewall programme or hardware device filters all information coming through the internet to your network or computer system. There are several types of firewall techniques that will prevent potentially harmful information from getting through:

i. Packet Filter

Looks at each packet[119] entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.[120]

ii. Application Gateway

Applies security mechanisms to specific applications, such as FTP[121] and Telnet[122] servers. This is very effective, but can impose a performance degradation.

iii. Circuit-level Gateway

Applies security mechanisms when a TCP[123] or UDP[124] connection is established. Once the connection has been made, packets can flow between the hosts without further checking.

iv. Proxy Server

Intercepts all messages entering and leaving the network. The proxy server[125] effectively hides the true network addresses.

In practice, many firewalls use two or more of these techniques in concert. A firewall is considered a first line of defence in protecting private information. For greater security, data can be encrypted.

119. https://www.webopedia.com/TERM/P/packet.html
120. https://www.webopedia.com/TERM/I/IP_spoofing.html
121. https://www.webopedia.com/TERM/F/ftp.html
122. https://www.webopedia.com/TERM/T/Telnet.html
123. https://www.webopedia.com/TERM/T/Telnet.html
124. https://www.webopedia.com/TERM/U/User_Datagram_Protocol.html
125. http://ebopedia.com/TERM/P/proxy_server.html

2.7
Encryption

Encryption involves scrambling information or a message mathematically (encrypt), so that it seems meaningless, but can still be restored to its original form by a person or device that possesses a piece of data that can unscramble it (a decryption key). This limits who can access the information or message because without the right key, it is nearly impossible to reverse the encryption and recover the original information. Encryption is one of several technologies that make up the field called cryptography.

End-to-end encryption ensures that a message is turned into a secret message by its original sender, and decoded only by its final recipient. Other forms of encryption may depend on encryption performed by third-parties. That means that those parties have to be trusted with the original text. End-to-end encryption is generally regarded as safer, because it reduces the number of parties who might be able to interfere or break the encryption.

2.8
Virtual Private Networks (VPNs)

A VPN is a method for connecting a computer securely to the network of an organisation elsewhere on the internet. When connected to a VPN, all web browsing data appears to originate from the VPN itself, rather than one's own internet service provider (ISP).[126] Using a VPN masks the IP address[127] assigned by your ISP from the sites that you access, adding a layer of privacy. Along with masking your IP address, it also encrypts your data while in transit to the site you are accessing.

i. Commercial VPNs

A commercial VPN is a private service that offers to securely relay your internet communications via their own network. The advantage of this is that all of the data you send and receive is hidden from local networks, so it is safer from nearby criminals, untrusted local ISPs, or anyone else spying on your local network. A VPN may be hosted in a foreign country, which is useful both for protecting communications from a local government, and bypassing national censorship. The downside is that the traffic is decrypted at the commercial VPN's[128] end. That means you need to trust the commercial VPN (and the country

126. https://en.wikipedia.org/wiki/Internet_service_provider
127. https://ssd.eff.org/en/glossary/ip-address
128. https://ssd.eff.org/en/glossary/commercial-vpn

where it is located) not to spy on your traffic. While a commercial VPN may offer "safety", it does not necessarily guarantee security.

Examples of these VPNs are CyberGhost VPN,[129] NordVPN,[130] Private Internet Access VPN[131] and TunnelBear (with 2gb of bandwidth free trial).[132]

ii. Free VPNs

A free VPN is a service that gives you access to a VPN server network, along with the necessary software, without you having to pay for anything. While a free VPN may save you money, it may however pose a security risk of you losing control of your data. An example is Windscribe VPN, which is free with a bandwidth limit for every 30 days.[133]

2.9
Develop Safe Online Habits

Here is a list of online habits and security measures to adopt to help safeguard your personal data and guarantee a secure online experience:

- Keep your systems and software up to date.
- Always have a current/updated anti-virus running.
- Avoid phishing scams.
- Use a complex password or a password manager.
- Be careful what you click on; a disreputable website can link you to cyber-criminals and bad actors.
- Never leave your computer or devices unattended. Lock your screens when you head to the restroom. An open system is an open invitation to your data.
- Protect your data.
- For all personal files, back up your data! You never know when you may lose your hard drive, and if the data will be recoverable. There are many cloud storage options, and an external drive is also an option. Consider encrypting your data before backing it up to an external storage device or to the cloud.
- When shopping online, or sharing sensitive data, be sure you are sending information encrypted by looking for "https" or the lock icon in your address bar.
- Be smart about what you share (and don't share) on social media.
- In the physical world, be careful of social engineering attacks, as described above.
- Be sure to monitor your financial and social media accounts for suspicious activity.

129. https://www.cyberghostvpn.com/en_US/
130. https://nordvpn.com/
131. https://www.privateinternetaccess.com/pages/techradar
132. https://www.tunnelbear.com
133. https://windscribe.com/

Virtual Work Cyber Safety Tips

Telecommuting (working from home), for whatever reason, comes with its own challenges with regards to cyber security threats. Virtual work has grown in popularity as more people and businesses use technology to carry out activities remotely.

Here is a list of remote working safety guidelines:

Tips for Remote Workers

- Only use Wi-Fi you trust. With an insecure connection, people in the near vicinity can snoop your traffic.
- For home networks encrypt the connection between your devices and your Wi-Fi router, such as using the WEP[134] encryption algorithm.
- Use company sanctioned devices.
- Update antivirus software.
- Update all software and the operating system.
- Remember to back up periodically. All-important files should be backed up regularly. In a worst case scenario, staff could fall foul of ransomware for instance. Then all is lost without a backup.
- Make sure you are using a secure connection to your work environment. This means using a VPN or some other secure means like Teamviewer.
- Beware of phishing emails. One should be suspicious of any e-mails asking to check or renew your credentials even if it seems to come from a trusted source. Please try to verify the authenticity of any significant or suspicious request through other means; do not click on suspicious links or open any suspicious attachments.

134. https://www.techtarget.com/searchnetworking/feature/Wireless-encryption-basics-Understanding-WEP-WPA-and-WPA2

Tips for Employers

- Focus on securing systems that enable remote access, such as VPNs. Ensure these systems are fully patched, firewalls are properly configured, and anti-malware and intrusion prevention software is installed.
- Never directly expose Remote Desktop Protocol (RDP) to the internet (connect to VPN first).
- Implement multi-factor authentication wherever possible.
- Consider restricting access to sensitive systems where applicable.
- Send out phishing awareness emails to your employees.
- The use of unauthorised software for official purposes (known as shadow IT) can increase when working remotely, raising security and privacy risks. Ensure staff are aware of the policy, privacy and legal obligations that apply to your organisation's information.
- Examine your incident response plans and, if necessary, update these to account for staff working remotely.
- Review your business continuity and contingency plans. Ensure these are up-to-date.

Video Conferencing

With video meetings experiencing a boom since COVID times, this development also witnessed a reported surge in "Zoom bombing", where meetings were intruded into by malicious individuals, and causing disruption to conference calls.

To avert incidences like this, the tips below highlight measures that can be adopted:

- Ensure participants can join via invitation only.
- Require a password to join the meeting.
- Activate administrator approval before someone can join the meeting.
- Do not post meeting links to social media.
- Ensure video conferencing and chat software are always up to date.

Video Conferencing Tools

- Zoom[135]
- Google Meet[136]
- Microsoft Teams[137]
- WhatsApp[138]
- Signal[139]
- Jitsi[140]
- Cisco Webex[141]

2.10
Digital Rights and Safety Tools

i. Ayeta Digital Rights Toolkit[142]

The interactive toolkit educates people to understand and identify digital security risks, set security goals, learn how to stay safe online and provides them with a password generator.

ii. Feedshield[143]

An online toolkit to help human rights defenders turn the tide, by documenting the abuse and unmasking the trolls.

iii. Ripoti[144]

A platform that enables you to report digital rights violations. Ripoti is dedicated to safeguarding the principles of digital freedom.

iv. Kuram[145]

An online gender-based violence (OGBV) response website designed to provide an avenue for women and other vulnerable groups to report cases of digital violence perpetrated against them.

135. https://zoom.us/
136. https://workspace.google.com/products/meet/
137. https://www.microsoft.com/en-us/microsoft-teams/group-chat-software
138. https://www.whatsapp.com/
139. https://www.signal.org/
140. https://jitsi.org/
141. https://www.webex.com/
142. https://paradigmhq.org/ayeta/game.html
143. https://feedshield.africa/en/
144. https://ripoti.africa/
145. https://kuramng.org/

CHAPTER 03

THREAT MITIGATION

3.1
Digital and Physical Security

i. Digital Security at Protests

At some point in their line of work, digital rights actors find themselves involved in protests in the quest to have their voices heard. Carrying digital devices to these protests can however be used against protestors, considering law enforcement groups have digital surveillance tools such as fake cell phone towers and facial recognition technology that could be used to identify protestors and monitor their movements and communications, thus jeopardising their security and privacy. Before heading to peaceful demonstrations, protesters should take steps to

ensure their digital privacy. Below are some things they should bear in mind.

ii. Keeping Protest Preparation Private

Having a trustworthy VPN service could help protest organisers disguise their internet traffic. Alternatively, protestors can make use of tools such as the Tor browser,[146] which masks a user's online activity by blocking trackers and encrypting their network traffic multiple times. Also vital, is ensuring protest-related organising is conducted over end-to-end encrypted apps rather than using plain text messages (otherwise known as SMS).

iii. Full Disc Encryption of Digital Devices

In the event that your device is confiscated by law enforcement officers, or is lost or stolen, full-disk encryption can ultimately help protect the data stored on your device. Android[147] and iOS[148] devices have inbuilt full-disk encryption capabilities. These devices should be protected using strong passwords to avoid being breached using a brute-force attack.

iv. Install Signal

Signal is an app available on both iOS[149] and Android[150] that offers strong end-to-end encryption to protect both text messages and voice calls. In addition to encrypting one-to-one communication, Signal enables encrypted group chats. The app also recently added the functionality of having messages disappear anywhere from within 10 seconds to four weeks after they are first read. In contrast to some other services like SnapChat, these ephemeral messages will never be stored on any server, and are removed from your device after disappearing.

v. Back Up Your Data

Take precautions to limit the potential costs of losing access to your device, whether it is lost, stolen or confiscated by law enforcement. Back up your data regularly and store that backup in a safe place to save yourself from a headache later on.

vi. Burner Phone

For protestors worried about having their phones tracked, a temporary but ideal solution would be getting a "burner phone", a prepaid device paid for in cash and used for the express purpose of staying in touch with people during a peaceful protest. Burner phones can give users the benefit of being able to stay in touch with people -

146. https://www.torproject.org/
147. https://source.android.com/security/encryption/full-disk.html
148. https://www.apple.com/business/docs/iOS_Security_Guide.pdf
149. https://ssd.eff.org/en/module/how-use-signal-ios
150. https://ssd.eff.org/en/module/how-use-signal-android

especially if things get dicey – without exposing all the data on their everyday device. Alternatively, putting your phone in aeroplane mode could serve the same purpose.[151]

vii. Physical Security

Physical threats to digital rights activists are as real as digital security threats. These threats range from arrests, harassment, confiscation of devices and detention by state actors. This puts them at a potentially high risk, a factor that jeopardises their security. In order to mitigate physical security threats, digital rights activists are urged to be alert to signs of threats to their personal security, taking into consideration their environment, the laws and the type of people in the community. The rule of thumb is - in order for a digital rights actor to succeed in protecting others, their own security must be guaranteed.

> ***"Physical threats to digital rights range from arrests, harassment, confiscation of devices and detention by state actors."***

3.2
Mitigating Physical Security Threats

To mitigate risk, digital rights actors are encouraged to take the following into consideration:

i. Accepting the risk

The victim who is in need of protection should be able to know that he or she can be at risk while executing his or her activities. With such awareness, the person is expected to be prepared to mitigate the risk or potential of risk. For example, when you are going out for humanitarian work in a war zone, you need to know that your security is at stake; therefore you need to be prepared to run when necessary, to call for help and you need to contact and explain your mission to the combatants involved in the fighting so that they can grant you access into the area.

Also, when you know that your data can be at risk of cyber-attack, you need to create a strong password, do fact checking of the digital platforms you intend to use, share your data to trusted persons and also store your data on different storage devices.

151. https://ssd.eff.org/en/module/attending-protest

ii. Avoiding the risk

Knowing the risk is one thing and avoiding it is another. When you learn of a risk, you need to avoid it by all means; you do not need to claim rights or power at that time. To avoid risk, your communication and actions should reflect and change according to the situation you find yourself in. You need to check your body language and use your words wisely, you need to evaluate the environment before you start any activities or engage with people, you need to understand whether there is a potential risk or not, and finally when it proves that you are a target, you need to respond fiercely to resist your attacker.

iii. Present your ideology to the right people

Your ideology may pose a risk when you publicise it. As a human rights advocate, you need to have a level of knowledge on whom to entrust with your information or associate with, because people are not obliged to accept your ideas.

iv. Personal and organisational credentials

As a spokesperson for an organisation or its representative in a potentially unsafe environment it is important to be armed with information such as who you are, what you do and the people you represent.

Such evidence becomes very handy in cases when you may be taken into custody as a suspect. Very often the way you present yourself, your position and organisation have a significant influence on how you will be treated by your captors. In most cases innocent suspects will be released after properly presenting themselves. Body language, choice of words and composure need to be well managed while under arrest and investigation.

v. Situational/environmental awareness

When in trouble, you must remain conscious of your environment at all times, taking into account your own role, where you are, and who your adversaries are - these are important issues to consider in a tricky situation to ensure your security. For example, a human rights advocate cannot be within the army barracks and condemn the atrocities committed by the soldiers.

vi. Avoid risk zones

Areas like borders of towns, crowds, banks, traffic areas, public gatherings, conflict or war areas are risk zones and you need to consider appropriate times to visit such areas, taking into consideration your profession and position. For example, a human rights activist is not advised to visit conflict zones without a guarantee of safety

from the belligerents. For instance, in the Anglophone regions of Cameroon where there is conflict between the separatists and government forces, for security reasons humanitarian workers cannot access confrontation zones without safe passage assurance from the combatants. This is because they may be hurt by stray bullets, arrested or kidnapped if they fail to have security assurance from the combatants.

vii. Clothing

You need to be conscious of your appearance and understand how to dress when carrying out humanitarian activities. For example, when going out for field work you need to wear light shoes and dress in such a way that you can easily escape a scene or run when there is a need. If your area is not secured, avoid dressing expensively because you may be targeted based on how you dress.

viii. Do not resist at gunpoint or in the army barracks

When you are arrested or kidnapped or surrounded, do whatever you are told in order to protect your life. Do not resist and consider your security first.

ix. Be prepared for everything

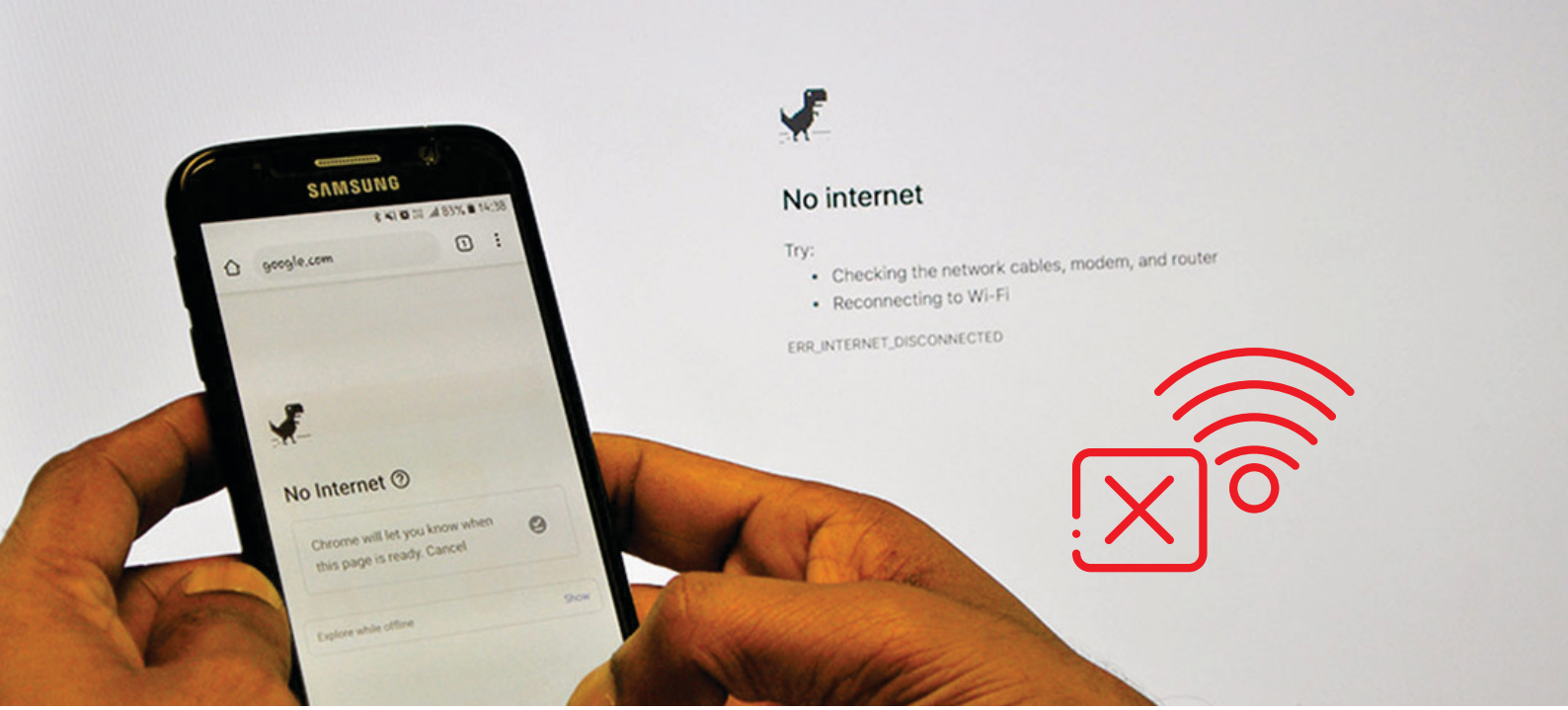
Whenever you are going on a mission, assess the possible risks and take along a first aid kit and all the basics in reasonable quantities based on your health, your journey, the climatic conditions, financial needs, etc, to cater for your physical security.

x. Always have a trusted contact

In risky endeavours like human rights activism, you need to prepare for the risk of arrest, kidnapping or attacks on your data. As a mitigating measure, you need to have one or more trusted colleagues with whom you can share your information, your destination, at which time you are expected to be there, when you are expected to be back, and what should be done in case of emergency.

xi. Emergency numbers and tracking

Keep contacts for the police, ambulance service, fire service, hospital, etc in a safe place. Download and install applications that can track your device when you are in trouble.



CHAPTER 04

INTERNET SHUTDOWNS

Article 19 of the Universal Declaration of Human Rights guarantees everyone the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

However, in recent years, there has been an increased tendency of African states resorting to the disruption of access to information online. This has turned the internet into a more volatile space, and incidences of challenges posed to activists, human rights defenders, dissidents, and journalists are reportedly on the rise.

Authoritarian regimes have resorted to using digital tools and tactics such as internet shutdowns, online censorship and digital surveillance to clamp down on free expression. According to Access Now, in

2022, at least 35 countries shut down the internet at least 187 times.[152] So far this is the highest number ever recorded in a single year. In 2023, by September, at least 12 internet shutdowns had occurred in sub-Saharan Africa, stifling freedom of expression and limiting access to information, particularly during elections and public protest periods,[153] at a cost of $200 million. Globally internet shutdowns resulted in a total cost of $10 billion in 2022.[154]

Further, a Paradigm Initiative 2019 report[155] revealed that a number of African governments have been shutting down the internet for political reasons, passing stringent regulations on online content, and/or employing the use of targeted spyware attacks against human rights defenders. The 2023 PIN Londa report highlighted that five of the 26 countries reported on, shut down the internet.[156] The report added that the export of Chinese and Russian models of so-called "rule of law" tactics towards control of the internet has seen tightening government control and digital rights violations through legislation that is ostensibly written to promote law and order in African societies.

The shutdowns have had adverse economic impacts in the countries in question. A Deloitte study[157] reveals that for a highly connected country, the per day impact of a temporary shutdown of the internet and all of its services would be on average $23.6 million per 10 million population. In 2023 internet shutdowns continue to be costly, with a country like Ethiopia losing an estimated $1.59 billion.[158] However, the overall cost of internet shutdowns during 2023 was down by 67% compared to 2022, but up by 45% in comparison with 2021. Shutdown durations were up by 18% compared to 2022, and a significant 71.5% up in comparison to 2021.[159]

The per day impact of a temporary shutdown of the internet and all of its services would be on average

$23.6 Million

per 10 million population

152. https://www.accessnow.org/press-release/keepiton-internet-shutdowns-2022-africa/
153. https://rsf.org/en/how-internet-shutdowns-undermine-journalism-sub-saharan-africa
154. https://technext24.com/2022/12/14/internet-shutdowns-cost-sub-saharan-africa/
155. http://paradigmhq.org/download/dra19/
156. https://paradigmhq.org/londa/
157. https://www2.deloitte.com/global/en/pages/technology-media-and-telecommunications/articles/the-economic-impact-of-disruptions-to-internet-connectivity-report-for-facebook.html
158. https://www.forbes.com/sites/emmawoollacott/2024/01/04/government-internet-shutdowns-bring-huge-economic-costs/?sh=557e1b654e44
159. https://www.forbes.com/sites/emmawoollacott/2024/01/04/government-internet-shutdowns-bring-huge-economic-costs/?sh=557e1b654e44

Despite this move by various states to clamp down on digital spaces and in the process limiting the work of those on the frontlines of human/digital rights advocacy, a number of internet anonymity and circumvention tools such as VPNs and web based proxies offer hope to human rights actors, digital rights defenders, journalists, and whistleblowers.

4.1 Circumventing Internet Shutdowns and Censorship

i. Virtual Private Network (VPN)

As already discussed in chapter II under digital safety, a VPN is a method for connecting your internet connected device securely to the network of an organisation elsewhere on the internet. When you use a VPN, all of your internet communications are packaged together, encrypted, and then relayed to that organisation, where they are decrypted, unpacked, and then sent on to their destination. To the organisation's network, or any other computer on the wider internet, it looks like your computer's request is coming from inside that organisation, not from your location.

VPNs are used by individuals to bypass local censorship, or defeat local surveillance.

ii. Tor Browser

Tor[160] is free and open-source software for enabling anonymous communication. The name is derived from the acronym for the original software project *"The Onion Router"*. Tor has built-in features that safeguard you from web tracking, surveillance, and finger printing.

iii. DuckDuckGo

An internet search engine that emphasises protecting searchers' privacy and avoiding the filter bubble of personalised search results. DuckDuckGo[161] distinguishes itself from other search engines by not profiling its users and by showing all users the same search results for a given search term.

160. https://www.torproject.org/download/
161. https://duckduckgo.com/

iv. Changing Domain Name System (DNS) Settings

When experiencing DNS poisoning/spoofing,[162] often inflicted by internet service providers, changing the DNS settings can aid in circumventing DNS censorship. Governments are sometimes at the forefront of advancing DNS poisoning in order to limit the content that its citizens have access to.

4.2 Measuring Internet Shutdowns and Censorship

i. The Open Observatory of Network Interference (OONI)

OONI is a free software project that aims to empower decentralised efforts in increasing transparency of internet censorship around the world. OONI develops free and open source software[163] called OONI Probe to detect:

- Blocking of instant messaging apps (WhatsApp, Facebook Messenger and Telegram);
- Blocking of censorship circumvention tools (such as Tor and Psiphon);
- Presence of systems (middleboxes) in your network that might be responsible for censorship and/or surveillance; and
- Speed and performance of your network.

By running OONI Probe,[164] you can collect data that can potentially serve as evidence of internet censorship since it shows how, when, where and by whom it is implemented. Information on internet censorship trends can be found on OONI's censorship findings platform.[165]

ii. Internet Outage and Detection Analysis (IODA)

IODA monitors the internet and detects internet connectivity outages in real time on an interactive internet outages dashboard[166] which allows users to track internet outages globally.

iii. Measurement Lab (M-Lab)

M-Lab[167] provides for open, verifiable measurement of global network performance. Through M-Lab, users can measure the performance of their internet to check internet speed. This helps detect throttling of internet speeds.

162. https://www.fortinet.com/resources/cyberglossary/dns-poisoning
163. https://github.com/ooni/probe
164. https://ooni.org/install/
165. https://explorer.ooni.org/findings
166. https://ioda.inetintel.cc.gatech.edu/dashboard
167. https://speed.measurementlab.net/#/

4.3
Advocacy Against Internet Shutdowns in Africa

i. NetBlocks Cost of Shutdown Tool (COST)

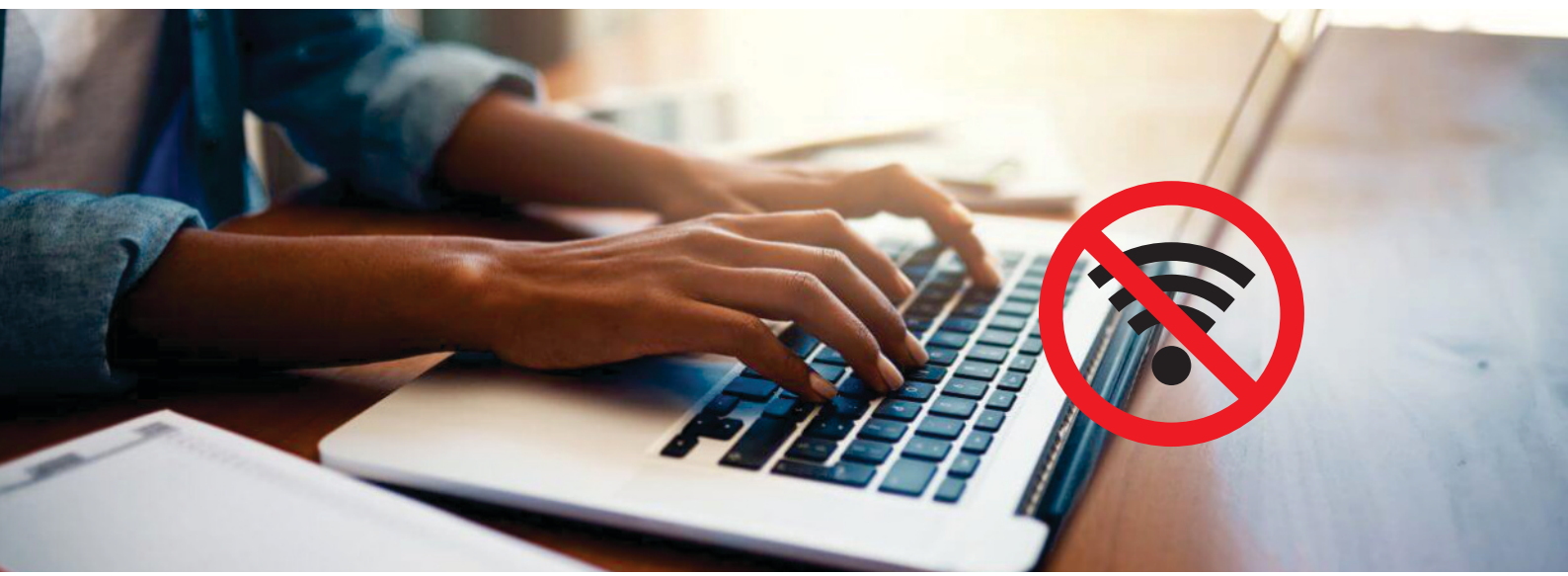
A data driven online tool[168] for measuring the cost of internet shutdowns, and convincing governments to keep the internet on. The tool enables anyone – including journalists, researchers, advocates, policy makers, businesses, and many others – to quickly and easily estimate the economic costs of internet shutdowns, mobile data blackouts and social media restrictions using thousands of regional indicators from the World Bank, ITU, Eurostat and US Census. Netblocks[169] is a global internet monitoring site which provides analysis and reports of internet slowdown, shutdown and internet

ii. #KeepItOn Campaign

This global campaign[170] spearheaded by AccessNow seeks to urge governments the world over not to shut down the internet and allow the free flow of information.

iii. Internet Shutdown Game

The Association for Progressive Communications developed an internet shutdown interactive game[171] which sheds light on various kinds of internet shutdowns and ways to counteract them. The game is targeted at human rights advocates, the general public and legal professionals.



168. https://netblocks.org/cost/
169. https://netblocks.org/reports
170. https://www.accessnow.org/campaign/keepiton/
171. https://shutdowngame.apc.org/

GLOSSARY

Add-on – A piece of software that modifies other software by changing how it works or what it can do. Often add-ons can add privacy or security features to web browsers or email software. Some add-ons are malware, so be careful to install only those that are reputable and from official sources.

Anonymity – The condition of being anonymous.

Anti-virus – Anti-virus software used to prevent, detect, and remove malware, including computer viruses, worms, and Trojan horses. Some examples of anti-virus software are McAfee, Avast, AVG, and Kaspersky.

Censorship – Internet censorship is the control or suppression of what can be accessed, published, or viewed on the internet, enacted by regulators, and/or governments.

Circumvention – The use of various methods and tools to bypass internet censorship.

Cryptography – The art of designing secret codes that let you exchange messages with a recipient without others being able to understand the message.

Digital hygiene – Refers to steps like organising the files on your PC, locking down your social media accounts, introducing new apps or technologies to make your digital life easier or more secure.

Digital rights – Digital rights are basically human rights in the internet era.

Encryption – A process that takes a message and makes it unreadable except to a person who knows how to "decrypt" it back into a readable form.

Encryption Key – An encryption key is a piece of information that is used to convert a message into an unreadable form. In some cases, you need the same encryption key to decode the message. In others, the encryption key and decryption key are different.

Firewall – A tool that protects a computer from unwanted connections to or from local networks and the internet. A firewall might have rules that forbid outgoing email, or connections to certain websites. Firewalls can be used as a first line of defence to protect a device from unexpected interference. They can also be used to prevent users from accessing the internet in certain ways.

File Transfer Protocol (FTP) – A standard network protocol used for the transfer of files from one host to another over a Transmission Control Protocol-based network, such as the internet.

Internet shutdown – An internet shutdown is an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable for a specific population or within a location, often to exert control over the flow of information.

IP address – An Internet Protocol address is what uniquely identifies connected devices on the internet.

Malware – Malicious software: programmes that are designed to conduct unwanted actions on your device. Computer viruses are malware. So are programmes that steal passwords, secretly record you, or delete your data.

Operating System (OS) – A programme that runs all the other programmes on a computer or device. Windows, Linux, Android, HarmonyOS and Apple's OS X and iOS are all examples of operating systems.

Password manager – A tool that creates and stores passwords so that you can use many different passwords on different sites and services without having to memorise them.

Passphrase – A passphrase is longer than a password, which is usually a single word.

PC (personal computer) – A multi-purpose computer.

PGP – Pretty Good Privacy was one of the first popular implementations of public key cryptography to help activists and others protect their communications.

Proxy – A server application or appliance that acts as an intermediary for requests from clients seeking resources from servers that provide those resources. A proxy server thus functions on behalf of the client when requesting service, potentially masking the true origin of the request to the resource server.

Security question – Password related questions to which only you are supposed to know the answers.

Software – A generic term for applications, scripts and programmes that run on a device.

TCP (Transmission Control Protocol) – A communications standard that enables application programmes and computing devices to exchange messages over a network.

Telnet (teletype network) – Telnet is a client/server application protocol that provides access to virtual terminals of remote systems on local area networks or the internet.

Tor – Free and open-source software for enabling anonymous communication. The name is derived from an acronym for the original software project name "The Onion Router".

Two Factor Authentication – 2FA is a way to let users identify themselves to a service provider by requiring a combination of two different authentication methods. These may be something that the user knows (like a password or PIN), something that the user possesses (like a hardware token or mobile phone), or something that is attached to or inseparable from the user (like their fingerprints).

URL (Uniform Resource Locator) – The address of a web page.

UDP (User Datagram Protocol) – A communication protocol used across the internet for especially time-sensitive transmissions such as video playback or DNS lookups.

Virtual Private Network – A VPN is used to connect to the internet via an encrypted tunnel. Your ISP, or anyone sniffing on the free Wi-Fi you are using to access the web, can only see your connection to the VPN service, while the website you are visiting will only record a connection from the VPN servers. Different options of VPNs are available, depending on what you need.[172]

Virus – A PC virus is a piece of code with the capability of copying itself and typically has a detrimental effect, such as corrupting a computer system or destroying data.

172. https://ssd.eff.org/module/choosing-vpn-thats-right-you

Web-based proxy – A website that lets its users access other, blocked or censored websites. Generally, the web proxy will let you type a web address (or URL) onto a web page, and then redisplay that web address on the proxy page. It is easier to use than most other censorship-circumventing services.

PARADIGM INITIATIVE

About Paradigm Initiative

Paradigm Initiative works to connect underserved young Africans with digital opportunities, and ensures protection of their rights.

@ParadigmHQ