REPORT

Digital safety & security in Africa

APRIL 2024

American Friends Service Committee

Table of contents

Researcher: Joanne Kanini

Abbreviations

ACME	Africa Center for Media Excellence
COVID-19	Coronavirus Disease 2019
EMA	Ethiopian Media Authority
GSMA	Global System for Mobile Communications
HRDs	Human Rights Defenders
ICT	Information and Communication Technology
KICTANet	Kenya ICT Action Network
LGBTIQ+	Lesbian, Gay, Bisexual, Transgender, Queer/Questioning, and others
NGO	Non-Governmental Organization
OECD	Organization for Economic Co-operation and Development
PROSAK	Protective & Safety Association of Kenya
#KeepItOn	A network advocating against internet shutdowns
ZBC	Zimbabwe Broadcasting Corporation

Executive summary

Under the Mask is a project developed to address the increasing closing of civic space. The onset of the COVID-19 pandemic saw an acceleration in this global trend. Under the Mask highlights and documents increased restrictions on civic space, and shares strategies and activities that communities and activists worldwide use to protect their freedom. The project includes a series of webinars focused on state restrictions, a series of podcasts, reports, and case studies that highlight strategies that are working worldwide. AFSC is conducting a global research project on 'Digital security across international contexts. The project is responding to targeted networks of activists, journalists, and grassroots CSOs reporting on human rights abuses and deteriorating political conditions in risky contexts across the globe. Digital security measures vary significantly across contexts, and while some tools and trainings exist, they are not accessible and adaptable to various needs and contexts.

This research aims to comprehensively analyze digital communication within the African region. It encompasses mapping out organizations involved in digital communication, assessing gaps across different areas, identifying challenges and their impact on civil society and human rights defenders, articulating emerging issues, and informing the agenda for an in-person convening.

Therefore, this research examines the digital communication landscape in Kenya, Nigeria, and Zimbabwe, shedding light on gaps in digital communication, challenges faced by civil society and human rights defenders, the organizations working in this field, and emerging concerns in this sector. Key findings reveal many organizations actively engaged in digital safety and security across these regions, reflecting a growing awareness of the importance of digital security. However, coordination among these entities is limited, suggesting the need for greater collaboration and capacity building. Disparities in digital infrastructure, skills, and access persist, impeding inclusive digital communication. These disparities underscore the urgency of bridging the digital divide and standardizing legal frameworks for digital safety and security.

Challenges faced by civil society and human rights defenders include repressive laws, surveillance, internet shutdowns, and self-censorship, limiting their ability to advocate for human rights in the digital age. Furthermore, emerging concerns center around the lack of comprehensive research on digitalization in Africa, particularly in comparison to advanced economies, highlighting the need for data-driven strategies. The proposal for a Digitalization Gap Index offers a promising solution to measure progress and guide policy decisions.

Recommendations to address these challenges and concerns include enhanced collaboration among organizations, investments in digital infrastructure and skills development, standardized legal frameworks for cybersecurity, and support for civil society and human rights defenders. An in-person convening is proposed to bring together stakeholders to discuss these issues, fostering collaboration and informed strategies for advancing digital

rights and safety in Africa. This research underscores the importance of addressing the digital divide and safeguarding digital rights to ensure inclusive and secure digital communication across the African continent.

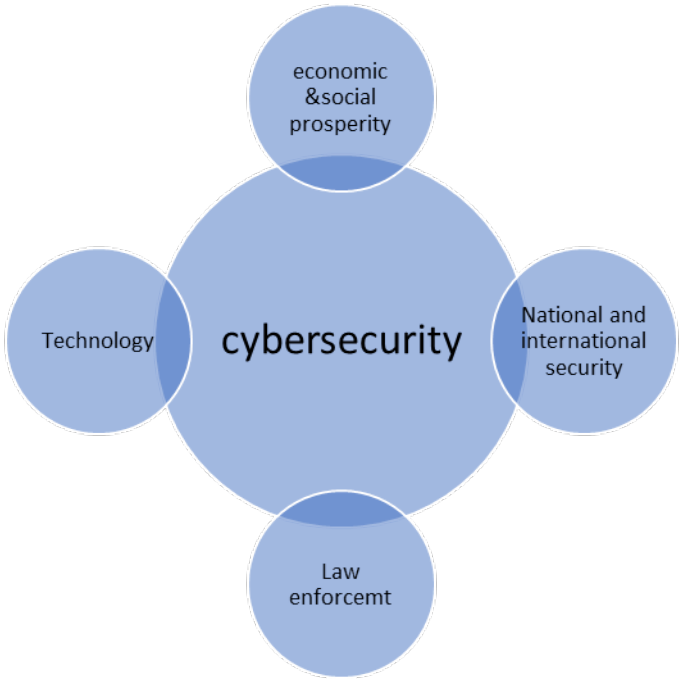
1. Introduction

1.1 Digital Security

Digital security, in its broadest sense, refers to the collective measures required to safeguard valuable online assets, including data and personal identity. Security involves the protection of one's online identity and is of paramount importance in the digital age. In this context, it represents the policies and framework that provide essential and practical guidelines to ensure security without impeding the open and unrestricted use of digital resources.[1]

The Organization for Economic Co-operation and Development (OECD), based in Paris, France, published a policy framework on Digital Security in 2022. The framework is aimed at helping policymakers understand the economic and social dimensions of cybersecurity. According to OECD, digital security is the set of measures taken to manage digital security risks for economic and social prosperity.[2]

Figure 1. Digital security, the economic and social aspect of cybersecurity



[1] Faisal Ahmed Ghauri, "Digital Security Versus Private Information," July 2021, DOI: 10.5281/zenodo.5164002.
[2] OECD (2022), OECD Policy Framework on Digital Security, OECD Publishing, Paris, https://doi.org/10.1787/a69df866-en

The figure above illustrates the diverse dimensions within the realm of cybersecurity.

1. **Tech Protection**: This is about safeguarding computer systems and data from online threats.

2. **Economic Well-being**: Cybersecurity is not just tech; it also helps our economy and society stay safe and work smoothly in the digital world.

3. **Cyber Laws**: This part focuses on enforcing laws against cybercrimes to secure the digital space.

4. **Global Safety**: It is about keeping peace in the online world, both in the country and globally.

1.2. Regional context

According to Hood (2019)[3], Africa's digital security landscape has undergone a notable transformation. Around 15 years ago, the continent faced a historical lag in internet proliferation, characterized by slow and costly internet access. Consequently, cybersecurity received minimal attention during this period. However, Africa has since experienced a remarkable technological leapfrogging phenomenon, propelled by the widespread adoption of mobile technology and services like mobile money, coupled with increased internet penetration. As Africa's digital ecosystem evolves and more individuals gain internet access, the significance of digital security and safety has surged.

In a LinkedIn article by Sentech Africa Tech Week dated March 22, 2023, the importance of cybersecurity in Africa's evolving digital landscape is highlighted.[4] Cybersecurity has become a critical concern with the continent increasingly embracing technology, including the internet, mobile phones, and social media. The article discusses cybersecurity threats, such as phishing attacks, malware, and insider threats, which pose risks to private and public sectors. While acknowledging challenges like the shortage of skilled cybersecurity experts and the need for comprehensive regulatory frameworks, the article emphasizes the importance of investing in cybersecurity education and training to address evolving risks and protect Africa's economic and social development.

1.3. Digital Safety and Security in Selected Countries in Africa

There is rapid growth of digital technology in the continent. This growth has brought challenges such as fake news, recruitment to militia groups, financial and employment

[3] Mukiibi, Hood. (2019). Cyber security in Africa: The boring technology story that matters. XRDS: Crossroads, The ACM Magazine for Students. 26. 56–59. 10.1145/3368077.
[4] Sentech Africa Tech Week. "The Importance of Cybersecurity in Africa's Digital Future." Sentech Africa Tech Week LinkedIn Page. https://www.linkedin.com/pulse/protecting-africas-digital-future-importance-cybersecurity/. Published March 22, 2023.

scams, and hate speech, among others. The onset of COVID-19 made matters worse with increased digital surveillance due to government enforcement of COVID-19 measures and the remote nature of the working environment.

This study will focus on Ethiopia, Kenya, Zimbabwe, and Nigeria. These were chosen as the focal points for this research because they provide a comprehensive and varied perspective on the African continent. These four countries were chosen strategically to encompass various geographical locations, cultural backgrounds, economic contexts, and digital landscapes across Africa. This selection allowed for a comprehensive examination of digital and socioeconomic trends on the continent, providing a deeper understanding of the challenges and opportunities that various African nations face in the modern digital age.

Ethiopia is a vast landlocked country in the Horn of Africa. It has faced significant digital and cybersecurity challenges, making it an interesting case study for examining digital development and security issues in a diverse and geopolitically important region. The country's rich history has also seen instances of ethnic-based conflicts in recent times. The population of Ethiopia is estimated at approximately 116.5 million in 2023.[5] There were 21,147,255 internet users as of December 2021, whereas the internet penetration in the country was 17.7%. At the same time, the internet growth rate was 211,372% between 2000-2021, and Facebook subscribers were 7,535,700 as of April 2021.[6]

Kenya too, was selected as a research focal point due to its reputation for having a relatively advanced digital infrastructure. The country boasts a significant internet penetration rate and a burgeoning technology sector, making it a valuable reference point for comparing digital trends across various African nations. Kenya is located in East Africa and has a population of around 57 million. In 2023, there were 46,870,422 internet users as of December 2021, and the internet penetration was 85.2%. The internet growth rate was 23,335% between 2000 – 2021, while Facebook subscribers were 12,445,700 as of 30th April 2021. [7]

Nigeria is the most populous country and is located in West Africa. Its position as the largest economy on the continent and the governance and resource management challenges it encounters make it an intriguing case study. Nigeria had an estimated population of around 230.8 million in January 2023.[8] There were 154,301,195 internet users as of December 2021, and internet penetration was 73.1%. The internet growth rate was 101,484% between 2000 – 2021, and Facebook Subscribers were 31,860,000 as of 30th April 2022. [9]

On the other hand, Zimbabwe is located in the southern region of Africa and offers insights into the economic challenges many countries face in that part of the continent. Its rich

---

[5] Ethiopia-Country Summary. (2023, August 30). Retrieved from The World Factbook: https://www.cia.gov/the-world-factbook/countries/ethiopia/summaries
[6] Internet Penetration in Africa. (2022). Retrieved August 30, 2023, from https://www.internetworldstats.com/stats1.htm
[7] Internet Penetration in Africa. (2022). Retrieved August 30, 2023, from https://www.internetworldstats.com/stats1.htm
[8] Nigeria-Country Summary. (2023, August 30). Retrieved from The World Factbook: https://www.cia.gov/the-world-factbook/countries/nigeria/summaries/#people-and-society
[9] Internet Penetration in Africa. (2022). Retrieved August 30, 2023, from https://www.internetworldstats.com/stats1.htm

natural resources and financial struggles make it a relevant case study for understanding the complexities of resource-rich but economically challenged nations. It is a landlocked country with abundant minerals such as gold, nickel, and coal among others. [10] With a population of approximately 15.4 million as of January 2023, there were 8,400,000 internet users as of December 2021, and internet penetration was 55.7%. The internet growth rate was 16,700% between 2000 – 2021, and Facebook Subscribers were 1,303 000 as of 30th April, 2022. [11]

[10] Zimbabwe-Country Summary. (2023, August 30). Retrieved from The World Factbook: https://www.cia.gov/the-world-factbook/countries/kenya/summaries
[11] Internet Penetration in Africa. (2022). Retrieved August 30, 2023, from https://www.internetworldstats.com/stats1.htm

2. Literature review

2.1 Mapping out organizations

In the course of the research, a key informant with expertise in digital safety and security in Africa provided valuable insights into key organizations actively addressing these issues across the continent. These organizations play a pivotal role in safeguarding digital advancements and promoting cybersecurity. The African Union Commission (AUC), based in Addis Ababa, Ethiopia, recognizes the importance of digital advancements for Africa's development and champions cybersecurity through the African Union Convention on Cyber Security and Personal Data Protection, known as the Malabo Convention. The Collaboration on International ICT Policy in East and Southern Africa (CIPESA), headquartered in Kampala, Uganda, was acknowledged for its central role in promoting digital rights and internet freedom in East and Southern Africa, engaging with policymakers, civil society, and other stakeholders to ensure a safer digital environment. iHub, located in Nairobi, Kenya, was cited as an innovation hub and hacker space that fosters technological advancements and champions digital safety and security through various programs and workshops. Paradigm Initiative (PIN), based in Lagos, Nigeria, was noted for its advocacy for digital rights and inclusion in Africa, with a focus on building an ICT-enabled support system and advocating for digital rights to improve the livelihoods of underserved youth. Research ICT Africa, situated in Cape Town, South Africa, conducts public-interest research on ICT policy and regulation, with specific projects focusing on cybersecurity and online rights. The Africa Digital Rights Hub (ADRH), described as a not-for-profit "think and action tank," promotes Pan-African research and capacity building on digital rights. BarefootLaw, based in Uganda, utilizes technology to provide free legal services and is an active voice in the space of digital rights and the rule of law in the digital era.

The information provided by the key informant offers valuable insights into the key players addressing digital safety and security in Africa. These organizations, located across the continent, contribute significantly to enhancing digital safety, cybersecurity, and the protection of digital rights, ultimately driving Africa's digital development and security landscape. Their roles encompass advocacy, research, capacity building, and providing essential legal services, each adding a unique dimension to the broader discussion on digital safety and security in Africa. This informant's expertise sheds light on the pivotal contributions of these organizations to the digital landscape, making them invaluable resources for understanding the complexities and challenges of digital safety and security across the African continent.

In the quest to identify organizations actively addressing digital security concerns in Africa, limited information specific to Ethiopia was uncovered through initial desktop research. Consequently, reliance was placed on insights provided by key informants to illuminate this

critical area. Noteworthy among the organizations highlighted were DefendDefenders, a Uganda-based entity committed to safeguarding digital rights and security, and Access Now, a global organization focused on defending and expanding digital rights, which also operates within Africa. Paradigm Initiatives, headquartered in Nigeria, emerged as another prominent player dedicated to enhancing digital rights, inclusion, and security in the country. Consortium of Ethiopian Human Rights Organizations (CEHRO) was identified as an organization focused on promoting human rights, including digital rights and safety, within Ethiopia. Lastly, The Collaboration on International ICT Policy for East and Southern Africa (CIPESA), based in Uganda, operates as a regional center specializing in digital policy and human rights concerns in East and Southern Africa. Although the initial research yielded limited results for Ethiopia, these key informants' contributions shed light on organizations actively striving to address digital safety and security challenges across Africa as a whole, crucially safeguarding digital rights, privacy, and security throughout the continent.

In Kenya, a range of organizations are actively engaged in digital safety and security. The Africa Center for Media Excellence (ACME) is dedicated to making the media a more effective platform for providing information on public affairs, monitoring official power, and fostering public debate. They operate in Kenya, among other East African countries. The Kenya ICT Action Network (KICTANet) serves as a multi-stakeholder think tank for ICT policy and regulation, catalyzing reforms in Kenya's Information and Communication Technology sector. The Association of Media Women in Kenya plays a vital role in advocating for the rights and safety of women in the media industry, including digital safety considerations. The Protective & Safety Association of Kenya (PROSAK) enhances safety measures in Kenya, encompassing digital safety and security aspects. Additionally, the Communications Authority of Kenya (CCK) is a critical regulatory body overseeing telecommunications and broadcasting in Kenya. These organizations mentioned above collectively contribute to advancing digital safety and security in Kenya, addressing critical issues related to digital threats, data privacy, and online safety.

Nigeria also hosts several organizations dedicated to digital safety and security. The Centre for Information Technology and Development (CITAD) focuses on using information and communication technologies (ICTs) to develop and promote good governance. They emphasize freedom of expression and ICT for development. The Fantsuam Foundation is among the pioneering organizations promoting ICT for development in Nigeria. It works with local communities to combat poverty and disadvantage through integrated development programs.

In Zimbabwe, the Digital Society of Africa plays a significant role. The organization works to strengthen the resilience and abilities of frontline activists, human rights defenders, and at-risk groups in the region to recognize and respond to digital threats and attacks independently. Their focus is on enhancing organizational security assessments and audits, digital security training, and raising awareness in the realm of digital safety.

Annexed to this research document is a table (Annex A) that provides a comprehensive list of organizations actively engaged in the field of digital safety and security across various African regions. This table serves as a supplementary resource, offering detailed information about these organizations, including their names, areas of focus, and geographical scope.

2.2 Gaps in digital communication across different regions.

An empirical report on digitalization and digital skills in Africa cited that while mobile connectivity is widespread in Africa, other forms of digital infrastructure like fixed-line internet are less accessible, potentially limiting the scope of digital communication. [12] The report explored key dimensions, including digital entrepreneurship, digital finance, digital public participation, and digital skills. Despite advancements, disparities persist between African nations and developed countries globally, affecting various aspects of the digital landscape. These inequalities impede innovation and growth in digital communication across the continent.

Key indicators like mobile-cellular subscriptions and internet penetration were considerably below global and regional averages.[13] Ethiopia's internet transmission speed was notably sluggish, and its international bandwidth utilization ranked poorly. These shortcomings were compounded by limited investment in critical connectivity infrastructure. Although recent improvements have been made, the digital communication sector in Ethiopia falls far behind the requirements for a modern economy, emphasizing the immediate need for substantial investments and policy reforms.

Odongo and Rono,[14] in their paper examined the digital divide in Kenya, emphasizing unequal access to media technologies. It revealed persistent disparities in digital utilization, driven by factors like location and access to resources such as devices like laptops, computers, software, internet connectivity, etc. Despite Kenya's 50 years of political independence, the digital and cultural divide remained, with urban areas having better access to digital services than rural regions. The paper underscored the urgent need to bridge these gaps to ensure equitable access to digital resources for all Kenyans.

In Nigeria, an examination of the digital divide by Desmond Onyemechi Okocha[15] revealed several critical gaps in digital communication. Firstly, it highlighted a significant disparity in access to information and communication technologies (ICT) between urban and rural areas, driven by factors like poverty, lack of infrastructure, and cultural beliefs. The digital divide was depicted as a deliberate and systemic issue, with those interviewed in this study attributing it to government policies and institutions. Importantly, the study underscored the necessity of closing this divide, as it had far-reaching implications for the economy, education, employment, and political participation. Additionally, the research revealed a lack of awareness among participants regarding government initiatives to bridge the digital gap.

---

[12] Bhorat, H., Signé, L., Asmal, Z., Monnakgotla, J., & Rooney, C. (2023). Digitalization and digital skills gaps in Africa: An empirical profile. Global Economy & Development Report. Brookings Institution. Retrieved from https://www.brookings.edu/wp-content/uploads/2023/05/Bhorat-et.-al-May-2023-Digitalization-and-digital-skills-in-Africa-2.pdf

[13] Adame, Berhan Oumer, Ethiopian Telecom Industry: Gaps and Recommendations Towards a Meaningful Connectivity and a Thriving Digital Eco-System. Available at SSRN: https://ssrn.com/abstract=3885501 or http://dx.doi.org/10.2139/ssrn.3885501

[14] Odongo, Agnes & Rono, Gideon. (2016). Kenya Digital and Cultural Divide. 85-94. 10.1145/2910019.2910077.

[15] Okocha, Desmond & Edafewotu, Endurance. (2022). Bridging the Digital Divide in Nigeria. The Journal of development communication. 33. 45-54.

The effects of this divide were noted, including economic instability, illiteracy, youth unemployment, and political weakness.

In Zimbabwe, a journal article by Teckshawer Tom[16] highlighted the state of digital development and communication, noting significant mobile network coverage, with 84% under 3G and 39% under 4G, suggesting potential for initiatives like e-voting. Despite relatively good mobile network coverage, there were evident gaps in terms of media control and political interference, notably at the state-owned Zimbabwe Broadcasting Corporation (ZBC). These gaps indicated a lack of media independence and a restricted flow of diverse information. Another notable gap was the limited awareness among citizens about government initiatives aimed at bridging the digital divide. This lack of awareness hindered the effectiveness of such programs. Overall, these gaps highlighted challenges in ensuring equitable access to information, promoting media independence, and fostering a robust digital communication environment in Zimbabwe.

2.3 Challenges on digital safety, security, and impact of civil society and human rights defenders across Africa surrounding digital communication.

A report on civil society (CSO) in the digital age in Africa[17] emphasized the critical role civil society plays in a functioning democracy and defined the sector as formal and informal structures that pursue democratic development outside of the state structure. CSO served as a bridge between citizens and stakeholders, facilitating civic engagement and participation. This report highlighted that CSOs faced challenges, including overt and covert actions such as restrictive laws, policies, and regulations, network disruptions, state-sponsored surveillance both online and offline, arrests of activists, monitoring of social media, and online harassment. In Africa, the civic space has been identified as shrinking at a faster rate compared to other continents.

This above report conducted an extensive analysis of the challenges confronted by civil society within the digital landscape, with a focus on Egypt, Sierra Leone, Uganda, and Zambia. It unveiled a troubling pattern where the governments of these countries employed a combination of legal measures and digital threats to constrict the civic space and undermine human rights. The shrinking civic space took various forms, encompassing stringent funding requirements, intimidation of human rights defenders and professionals, physical and online threats, and arbitrary arrests of Human Rights Defenders (HRDs). Additionally, these governments frequently used laws, such as anti-terrorism legislation, to legitimize actions that prioritized national security over civil liberties. The report underscored that in the digital age, threats against civil society evolved into more sophisticated forms as governments harnessed digital technologies for both governance efficiency and the suppression of dissent.

[16] Tom, T. (2023). E-voting, Information Gap, and The Digital Divide in Zimbabwe. Technium Social Sciences Journal, 45(1), 284–305. https://doi.org/10.47577/tssj.v45i1.9167

[17] Dube, H., Simiyu, M. A., & Ilori, T. (2020). Civil Society in the Digital Age in Africa: Identifying Threats and Mounting Pushbacks. Centre for Human Rights, University of Pretoria, and Collaboration on International ICT Policy in East and Southern Africa (CIPESA). ISBN: 978-1-920538-84-2

Ethiopia faced significant challenges related to digital safety and security, according to a press release by United Nations. [18] Internet shutdowns by the government disrupted communication and information access during periods of unrest. The rise of hate speech and disinformation on social media platforms posed threats to social cohesion and peace, exacerbating inter-ethnic tensions. The drafting of legislation to address hate speech raised concerns about potential restrictions on freedom of expression. Access to information remained limited due to a lack of electronic databases and unresponsive government ministries. Surveillance practices, often without judicial oversight, encroached on individuals' privacy and digital security. Despite these challenges, civil society organizations and human rights defenders played crucial roles in reporting violations and advocating for digital rights, emphasizing the need for a balanced approach to addressing these complex issues.

A 2022 report on human rights in Ethiopia shed light on the Ethiopian government's infringements on the rights of HRDs, civil society, and journalists[19]. \While independent media remained active, there were pervasive reports of harassment, intimidation, and restrictions on journalists critical of the government, particularly concerning its handling of the northern conflict and humanitarian crisis. The Ethiopian Media Authority (EMA) imposed limitations on freedom of expression for members of the press, and regional news agencies and social media influencers often propagated biased messages, leading to "echo chambers." Echo chambers are social environments or situations in which individuals are primarily exposed to and interact with information, ideas, beliefs, or people that reinforce and amplify their existing views, opinions, and perspectives. Within an echo chamber, individuals are often shielded from diverse or opposing viewpoints and are more likely to encounter information that aligns with their existing beliefs. These *echo chambers* sometimes downplayed or discredited reports of abuses against rival ethnic groups. Furthermore, criminal sanctions for blasphemy or religious ridicule existed in the legal framework. National security grounds were used to charge journalists, with some facing severe penalties such as the death penalty before subsequent releases. The government also restricted internet access, blocked social media sites and disrupted telecommunications, particularly in conflict-affected areas, limiting the ability of media and human rights organizations to report and verify information. Such actions collectively illustrate how the Ethiopian government curtailed digital communication and restricted the activities of HRDs, civil society actors, and journalists, hindering their efforts to advocate for human rights and free expression.

[18] Kaye, D. (2019, December 9). United Nations Special Rapporteur on the right to freedom of opinion and expression: Visit to Ethiopia, 2-9 December 2019 - End of mission statement [Press release]. Retrieved from https://www.ohchr.org/en/press-releases/2019/12/united-nations-special-rapporteur-right-freedom-opinion-and-expressiondavid

[19] Bureau of Democracy, Human Rights, and Labor. (2022). 2022 Country Reports on Human Rights Practices: Ethiopia. Retrieved from https://www.state.gov/reports/2022-country-reports-on-human-rights-practices/Ethiopia

In Kenya, a perception survey report by Defenders Coalition revealed that (HRDs)[20] in Kenya face significant challenges in terms of digital safety and security. HRDs demonstrated a high level of awareness regarding communication surveillance and the potential threats it posed to their work. They identified various sources of surveillance, including hackers, intelligence services, and telecommunication providers, with a perception that corporates and security forces were actively seeking access to their information. Many HRDs believed they had already been subjected to communication surveillance, such as phone tapping and hacking of their online accounts. Despite their awareness, there were gaps between their knowledge and actual practices in safeguarding their digital communications. Concerns also extended to issues like the Data Protection Act, the security of data collected during the COVID-19 pandemic, and biometric data collection, reflecting the complex landscape of digital rights in Kenya. This report underscored the importance of HRDs' efforts to protect themselves against surveillance while advocating for stronger digital privacy protections.

Additionally, the Kenya 2022 Human Rights report [21] highlighted restrictions on free expression, media censorship, and threats against journalists, suggesting a hostile environment for free speech.[22] The human rights report revealed that the Kenyan government employed various tactics to infringe on the rights of human rights defenders (HRDs), civil society, and journalists in the realm of digital communication. These tactics included pressure and intimidation of journalists to avoid critical reporting, firings based on political leanings, restrictive interpretations of laws, and the imposition of heavy fines. Additionally, the government's declaration of LGBTQ+ content as illegal and the monitoring of online platforms for hate speech further limit the freedom of expression and digital communication. Concerns also arose from reports of government surveillance, including interception of communications data and the use of various surveillance technologies. While Kenya has introduced data protection regulations, the overall environment appears to pose challenges for HRDs, civil society organizations, and journalists in their digital advocacy and communication efforts.

In Nigeria, the 2022 Human Rights report[23] revealed that the government employed a range of tactics to infringe on the rights of human rights defenders (HRDs), civil society, and journalists, particularly in the context of digital communication. The government exercised significant control over television and radio programming, limiting diversity of content, and

[20]Defenders Coalition. (2022). *2022 General Elections Report by Human Rights Defenders in Kenya.* Retrieved from https://defenderscoalition.org/2022-general-elections-report-by-human-rights-defenders-in-kenya/
[21] U.S. Department of State. (2022). *Country Reports on Human Rights Practices 2022: Kenya.* Retrieved from https://www.state.gov/reports/2022-country-reports-on-human-rights-practices/kenya
[22] Bureau of Democracy, Human Rights, and Labor. (2022). 2022 Country Reports on Human Rights Practices: Kenya. Retrieved from https://www.state.gov/reports/2022-country-reports-on-human-rights-practices/kenya
[23] Bureau of Democracy, Human Rights, and Labor. (2022). 2022 Country Reports on Human Rights Practices: Nigeria. Retrieved from https://www.state.gov/reports/2022-country-reports-on-human-rights-practices/Nigeria

prohibited local television stations from transmitting foreign programming, restricting the flow of global perspectives. Regulatory oversight, exemplified by temporary closures and fines was used to clamp down on media outlets, especially when they engaged with critical or sensitive subjects such as terrorism and banditry. The suspension of Twitter's activities in the country and its subsequent negotiation to unblock the platform illustrated the government's attempts to control online discourse. Journalists practiced self-censorship due to concerns about government intimidation and legal repercussions, inhibiting free reporting both offline and in the digital realm. The criminalization of defamation and blasphemy laws had led to the arrest of individuals, stifling criticism of both religion and government officials. Internet freedom was also at risk, with reports of website shutdowns and requests to block online content related to national security or terrorist organizations. Additionally, broad cybercrime laws had been utilized to arrest bloggers, journalists, and critics, further curbing online activism and digital communication. These actions collectively impeded the work of HRDs, civil society actors, and journalists striving to utilize digital platforms for advocacy and information dissemination in Nigeria.

In Zimbabwe, a 2022 human rights report [24] highlighted that the government-maintained censorship through media registration and accreditation laws, providing extensive powers to control media and suppress free speech. Fear of retaliation, whether in the form of legal action, harassment, or physical harm, made journalists practice self-censorship. Additionally, there were enforcements of libel, slander, and defamation laws, occasionally leading to arrests, posed a threat to freedom of expression. The government's broad legal powers, such as the Official Secrets Act, were used to restrict the publication of information critical of government policies or officials, potentially stifling dissent. In terms of internet freedom, the Interception of Communications Act allowed the government to monitor all communications, including internet transmissions, contributing to a regulated online environment to curb dissent. Internet disruptions during opposition rallies were also noted, suggesting potential throttling of online services during critical events. These actions collectively illustrate the Zimbabwean government's efforts to control and restrict digital communication, thereby impeding the work of HRDs, civil society organizations, and journalists in advocating for human rights and free expression.

2.4 Articulate emerging issues and concerns of digital communication.

The emerging issues in digital communication in Africa[25], as highlighted in a report on digitalization and digital skills in Africa encompassed the lack of extensive research on digitalization in the region, particularly in contrast to advanced economies. The continent's youthful population, expected to contribute significantly to the global workforce, underscores the importance of studying how digitalization affects labor markets and employment prospects. The report introduced a framework to measure digitalization across

[24] U.S. Department of State. (2022). *Country Reports on Human Rights Practices 2022: Zimbabwe*. Retrieved from https://www.state.gov/reports/2022-country-reports-on-human-rights-practices/zimbabwe/

[25] Bhorat, H., Signé, L., Asmal, Z., Monnakgotla, J., & Rooney, C. (2023). Digitalization and Digital Skills Gaps in Africa: An Empirical Profile. Brookings Institution | Global Economy and Development.

various dimensions and proposes the creation of a Digitalization Gap Index to assess Africa's progress relative to other regions. Moreover, it emphasized the necessity for a comprehensive measurement of digital skills and suggested policy reflections to address the challenges and opportunities presented by digitalization in Africa, indicating the need for strategic interventions to promote digital skills and infrastructure development.

According to the Global System for Mobile Communications (GSMC), a non-profit industry organization, in a 2022 report[26] in Sub-Saharan African nations, including countries like South Africa, Nigeria and Kenya, transition into a post-pandemic recovery phase, mobile connectivity is defined as the 'new normal' by bolstering economies' resilience and promoting inclusive development. While 3G will remain dominant, constituting over half of total connections by 2025, a significant shift is evident as 3G adoption declines for the first time. The rise of 4G is anticipated, accounting for about one-third of mobile connections by 2025, up from under one-fifth in 2021. Growing 5G activities, such as spectrum auctions and local use case development, underscore the region's potential for digital transformation.

[26] GSMA. (2022). The Mobile Economy Sub-Sahara Africa 2022.

3. Research design and methodology

This section outlines the approach taken to comprehensively explore this multifaceted subject, highlighting the methods employed and limitations encountered during the research process

3.1 Methodology

Desk Research

Desk research formed the backbone of this inquiry. It entailed an extensive exploration of existing literature, encompassing academic articles, reports, papers, and blogs. This approach allowed for the systematic collection of information that had been previously documented, facilitating an understanding of the evolution and current state of digital safety and security in Africa. Additionally, this method was well-suited to the study's focus on recent developments, as it enabled the identification of trends and shifts in the digital security landscape over time.

Questionnaires

In addition to desk research, questionnaires were distributed as a crucial method of data collection. These questionnaires yielded valuable insights and perspectives from experts, practitioners, and key stakeholders in the field of digital safety and security. The responses collected enriched the research findings, providing a more comprehensive understanding of the subject.

Data Accuracy

To enhance the accuracy and reliability of the collected data, a rigorous process of cross-referencing and verification was employed.

Limitations

While conducting this research, some limitations were encountered:

1. Inaccessible Sources: Some government websites and sources were not accessible for analysis. There was no permission to access certain government websites, limiting the ability to gather data from these sources.
2. Internet Barriers: Some information was challenging to access due to restrictions on certain websites or because of safety concerns. In some cases, internet security software warned against exploring certain websites due to potential risks.

3. Limited Country Coverage: The research focused on specific countries in Africa, providing insights into the digital safety and security situation in the eastern, western, southern, and northern regions of the continent. However, this selection did not capture the entire continent's perspective.
4. Reliance on International Sources: In some cases, local information about digital safety and security was limited. As a result, there was a need to rely on reports and data from international organizations operating in those countries.

4. Summary of findings

4.1 Mapping Organizations in Digital Communication

The literature review revealed a significant gap in research related to mapping organizations in digital communication across different regions, especially within the African context. While various reports and articles discussed the role of civil society organizations, human rights defenders, and media outlets in the digital realm, there was adequate comprehensive studies detailing the landscape of these organizations and their specific activities related to digital communication.

Across Kenya, Nigeria, and Zimbabwe, numerous organizations are actively dedicated to the field of digital safety and security.

4.2 Assessing Gaps in Digital Communication Across Different Regions

The review highlighted substantial disparities in digital communication across Africa. These disparities encompassed issues of infrastructure, access, and technological development. While mobile connectivity was identified as a significant driver of digital inclusion in Africa, challenges related to fixed-line internet access, broadband expansion, and digital skills development persisted. The lack of standardized legal cybersecurity frameworks and strategies, as exemplified in Ethiopia, further underscored the existing gaps in digital communication.

A significant disparity compared to developed nations becomes evident in the realm of online services and e-participation. This gap underscores the pressing necessity for the continued development and expansion of digital platforms that facilitate improved communication between governments and citizens. The comprehensive literature review further highlights that while Africa has indeed made noteworthy advancements in the sphere of digital communication, it still grapples with enduring gaps in critical areas such as digital entrepreneurship, digital finance, public participation, and digital skills. These disparities primarily arise from unequal access to essential resources, educational opportunities, and robust infrastructure across the continent.

4.3 Challenges on digital safety, security, and impact of civil society and human rights defenders across Africa surrounding digital communication.

The literature review uncovered several crucial insights into the state of civil society in Africa within the context of digital communication. Firstly, civil society serves as a linchpin for championing democracy, human rights, and civic engagement across the continent, but it grapples with multifaceted challenges encompassing state-backed digital threats, constraining legislation and pervasive surveillance, both online and offline. Secondly, African nations often employ restrictive laws, particularly those tied to national security and counterterrorism, to curb civil society activities, thereby impinging upon fundamental rights, notably freedom of expression and peaceful assembly. These legal constraints pose formidable impediments to the effective functioning of civil society. Thirdly, the literature underscores the paramount significance of digital security for civil society entities and human rights defenders, accentuating the imperative for comprehensive training to adeptly mitigate online risks. Lastly, it underscores the critical role of regional and international collaboration in tackling the predicaments confronting civil society. The international community's advocacy for human rights and the protection of civil society's interests looms large in the African context.

Furthermore, the review unearths notable trends related to digital privacy and security. First, a conspicuous deficiency in privacy awareness prevails among individuals, including activists and defenders, who frequently divulge personal information on social media platforms without adequate safeguards. Second, cyber threats, notably phishing attacks, loom as substantial hazards to human rights defenders in the region, with malevolent actors exploiting personal data gleaned from social media profiles. Third, certain African governments engage in online surveillance, infringing upon citizens' digital privacy rights. The exploitation of personal data, encompassing sensitive categories like health status, religious and political affiliations, interests, and activities, engenders concerns regarding targeting, blackmail, and manipulative tactics.

The literature underscores the multifaceted challenges inherent in digital communication across Africa, including censorship, surveillance, and restrictions on freedom of expression. Human rights defenders, civil society actors, and journalists grapple with threats, intimidation, and legal encumbrances as they employ digital platforms for advocacy. While efforts to address these challenges are perceptible, encompassing the promotion of digital rights and the advocacy for security measures, there remains an acute and ongoing need for fortified digital safety and security practices to safeguard both individuals and organizations in the digital age.

4.4 Articulating Emerging Issues and Concerns

The findings from the literature review on digital communication in Africa are noteworthy. Firstly, research gaps persist in understanding the impact of digitalization in the region, particularly compared to more advanced economies, highlighting the need for more extensive

studies. The concept of a "Digitalization Gap" is introduced to measure digitalization comprehensively, emphasizing Africa's youthful population and its role in the global workforce. This underscores the importance of digital skills and infrastructure development to fully harness digitalization's benefits. Moreover, the Global System for Mobile Communications defines mobile connectivity as the 'new normal' in Sub-Saharan Africa, with a notable shift from 3G to 4G and growing activities in 5G development, indicating the region's digital transformation potential. Additionally, data on internet penetration rates and secure servers in countries like Ethiopia, Kenya, Nigeria, and Zimbabwe highlight the significance of digital security measures in supporting the expanding online presence. In summary, these findings underscore the need for comprehensive research, digital skill development, and the pivotal role of mobile connectivity in Africa's digital evolution.

5. Analysis, discussion and implications

5.1 Mapping Organizations in Digital Communication

The implications drawn from this observation are multifaceted. Firstly, the existence of numerous organizations dedicated to digital safety and security across Kenya, Nigeria, and Zimbabwe signifies a recognition of the growing importance of digital security in these regions. However, the lack of comprehensive synergy among these organizations suggests potential inefficiencies and redundancies in their efforts. There may be a need for greater collaboration and coordination to maximize the impact of their work.

Secondly, the absence of local organizations working in the realm of digital safety and security in some countries highlights a significant gap in addressing digital threats and ensuring online safety. As Africa's digital landscape continues to evolve rapidly, the urgency of bolstering digital security and safety measures becomes even more apparent. Efforts should be made to encourage the establishment of such organizations in underserved regions to better protect individuals and entities in the digital sphere. Moreover, the limited understanding of the dimensions of digital security and safety among these organizations underscores the need for education and awareness in this relatively new field. The COVID-19 pandemic forced many organizations to transition online, prompting a belated realization of the critical importance of digital safety and security. To effectively address digital threats, these organizations should invest in building their capacity and expertise in this domain. Furthermore, the fact that some governments are the primary entities dealing with digital safety and security raises concerns about potential conflicts of interest and the potential for digital rights and human rights violations. There is a need for a more balanced and independent approach to digital security and safety that safeguards individual rights while also addressing legitimate security concerns.

5.2 Gaps in digital communication across Africa

There are significant disparities in digital communication across various regions in Africa. These disparities manifest in several critical dimensions, each presenting distinct challenges. Firstly, there is a pronounced inequality in digital infrastructure and access. While mobile connectivity has played a pivotal role in fostering digital inclusion, it remains unevenly distributed, with rural areas bearing the brunt of limited access. Moreover, the persistence of challenges related to fixed-line internet access and the expansion of broadband services further hinder comprehensive digital inclusion.

Secondly, a substantial technological development gap becomes apparent, particularly when compared to more advanced economies. This discrepancy is especially evident in the realm of online services and e-participation, where the capacity of governments to engage with their citizens digitally falls short of optimal standards. This shortfall underscores the immediate necessity for the continued development and expansion of digital platforms to facilitate more effective and inclusive communication between governments and their constituents.

Thirdly, the literature highlights a pervasive deficiency in digital skills across the African landscape. Some regions still lack access to even the most basic digital devices, revealing a glaring digital skills gap. The abrupt transition to online activities during the COVID-19 pandemic underscored the magnitude of this gap, impacting education, employment opportunities, and overall digital literacy.

Lastly, underlying these disparities is a core issue of inequality in access to essential resources, educational opportunities, and robust digital infrastructure. These disparities contribute significantly to the fragmented nature of the digital landscape across the continent.

Lack of favorable comprehensive policies in the continent to address the shrinking civic spaces, based on restrictive laws, policies, and regulations, network disruptions, online hate speech of different groups e.g., LGBTQ+ communities, state-sponsored surveillance both online and offline.

Implications stemming from these findings are substantial. Addressing the substantial digital divide is imperative, given its far-reaching consequences. Bridging this divide is not just about providing access; it's about enabling equal opportunities in education, employment, and participation in the digital economy. Furthermore, there is a clear need for standardized legal cybersecurity frameworks and strategies to ensure digital security and privacy for all citizens. In parallel, initiatives to enhance digital literacy should be prioritized, particularly in underserved regions, to empower individuals with the skills necessary to navigate the digital world safely and effectively.

Expanding digital platforms and services to reach all citizens is essential to narrow the gap in online services and e-participation. Such efforts will foster better engagement and communication between governments and their constituents. As digital access expands, ensuring digital safety and security must also be elevated as a priority. This is crucial, as the digital threats faced by individuals and organizations may rise with the increasing prevalence of digital communication.

5.3 Challenges on digital safety, security, and impact of civil society and human rights defenders across Africa surrounding digital communication.

Governments across various African countries employ a combination of legal measures and digital surveillance to limit civic space, curtail freedom of expression, and restrict the activities of civil society and HRDs. This includes repressive laws, network disruptions, and

state-sponsored surveillance both online and offline. These restrictive measures hinder the ability of civil society and HRDs to advocate for human rights and democratic development. The digital age has witnessed the evolution of surveillance tactics, making it more challenging for activists to operate securely and without fear of government interference.

Several African nations, including Ethiopia, have faced issues related to digital safety and security due to the lack of standardized legal cybersecurity frameworks and strategies. Anti-terrorism and cybercrime legislation are sometimes used to justify actions that prioritize national security over civil liberties. The absence of clear legal safeguards can lead to violations of digital rights and privacy. It also poses challenges for civil society organizations and HRDs in their efforts to challenge repressive laws and advocate for digital rights.

Internet shutdowns and disruptions, as observed in Ethiopia, are often used by governments during periods of unrest or conflict. These actions not only limit citizens' access to information but also increase cybersecurity vulnerabilities, leaving systems exposed to cyberattacks. Such shutdowns have adverse consequences for both digital safety and security. They hinder the ability of civil society and HRDs to communicate and organize, making it challenging to report human rights violations and advocate for change.

In Kenya and Nigeria, journalists and media outlets often choose to censor themselves because they are afraid of government pressure and threats. These governments have strict rules and can impose fines on the media, which makes journalists cautious about what they say or write. This self-censorship limits the variety of stories and viewpoints in the media. When media organizations are too careful, they can't do their important job of keeping an eye on the government and reporting on it critically. This affects how open and honest the government is with the public and how well people can talk about important issues in their countries. Concerns about privacy and surveillance technologies, such as those used in Zimbabwe, highlight the need for data protection measures and transparency regarding monitoring methods. The absence of data protection and surveillance oversight can lead to violations of citizens' privacy rights. It also raises concerns about the potential misuse of surveillance technologies for political purposes.

International organizations and coalitions, such as the #KeepItOn network, play a crucial role in advocating for digital rights and challenging internet shutdowns and censorship. International advocacy efforts are essential in raising awareness about digital rights violations and pressuring governments to uphold these rights. They contribute to a global dialogue on the importance of digital safety, security, and freedom of expression.

Many educational institutions across the continent face challenges in integrating digital literacy into their curricula, leaving a generation of students unprepared for a digital future. Moreover, the training approaches used often have a Western orientation, resulting in poor adoption of digital literacy in many African communities. Cultural hesitation is another significant barrier, as some communities perceive the digital world as a threat to traditional values and norms, leading to reluctance in engaging with or adopting digital tools. This resistance is further compounded by issues of misinformation and disinformation, especially in areas with limited digital literacy, where the spread of false or misleading information can have severe real-world consequences, affecting public health, politics, and inter-community

relations. The increasing connectivity also brings about challenges such as online exploitation, including cases of fraud, scams, and predatory behavior targeting unsuspecting individuals. Additionally, the rise of social media, while having positive aspects, brings negative ramifications such as cyberbullying and the dissemination of harmful content, impacting mental health. In societies deeply rooted in community, digital exclusion or online ostracization can be particularly detrimental to individuals' psychological well-being.

5.4 Articulate emerging issues and concerns of digital communication.

There is a significant lack of extensive research on digitalization in Africa compared to advanced economies is a significant concern. This knowledge gap hinders a comprehensive understanding of the impact and potential of digitalization on the continent. The absence of research may limit Africa's ability to harness the full benefits of digitalization. Without adequate data and insights, policymakers, businesses, and civil society organizations may struggle to make informed decisions and develop effective strategies.

The youthful population in Africa presents both opportunities and challenges. While the youth can contribute significantly to the global workforce, there is a need to understand how digitalization influences labor markets and employment opportunities. Focusing on digital skills development and employment strategies tailored to the youth is crucial. Failure to do so may result in high youth unemployment and missed opportunities for economic growth.

The proposal by Brookings Institution [27], to create a Digitalization Gap Index, highlights the importance of measuring digitalization comprehensively across various dimensions. Such an index can provide valuable insights into Africa's progress relative to other regions. Developing the Digitalization Gap Index can guide policymakers in identifying areas that require attention and investment. It can also facilitate international comparisons and collaborations to bridge digital divides effectively.

5.5 Inform the agenda for in-person convening.

The research highlights several critical issues related to digital communication in Africa, including the digital divide, digital skills, equitable access to resources, challenges faced by civil society organizations and human rights defenders, and the importance of cybersecurity and digital safety measures. An in-person convening provides a platform for stakeholders, including government officials, civil society representatives, activists, and experts, to come together, discuss these issues, and develop collaborative strategies and solutions. It allows for more in-depth discussions, networking opportunities, and the exchange of best practices, which can lead to more effective and targeted interventions to address the identified challenges, joint advocacy spaces and promote digital rights and safety in the region

[27] Bhorat, H., Signé, L., Asmal, Z., Monnakgotla, J., & Rooney, C. (2023). Digitalization and Digital Skills Gaps in Africa: An Empirical Profile. Brookings Institution | Global Economy and Development.

6. Conclusion and recommendations

In conclusion, addressing the complex landscape of digital communication in Africa requires practical recommendations that can be effectively applied. The findings emphasize the need for comprehensive actions to bridge digital divides, protect digital rights and foster an inclusive digital environment.

6.1 Recommendations

Here are the succinct recommendations based on the research objectives:

1. Comprehensive Mapping

Initiate a comprehensive mapping project to catalog organizations involved in digital communication across Africa, fostering collaboration and transparency.

2. Infrastructure and Skills

Advocate for the prioritization of infrastructure development, digital skills training, and digital literacy programs to ensure equitable access to the digital economy.

3. Legal Frameworks and Rights

COS, HRDs etc. advocate to the government and RECs e.g., AU, to Establish standardized legal cybersecurity frameworks and legislation to protect digital rights, privacy, and freedom of expression. Develop clear and specific legislation that defines the boundaries of national security actions in the digital realm. Ensure that the law explicitly outlines the circumstances under which certain measures, such as surveillance or data access, can be employed. By advocating for such legal frameworks, civil society organizations (CSOs), human rights defenders (HRDs), and other stakeholders aim to create an environment that protects digital rights, privacy, and freedom of expression. Clear and specific legislation can set boundaries for government actions in the digital space, preventing overreach and safeguarding the civic space for individuals and organizations to freely express themselves and engage in online activities without undue interference.

Localize Solutions:

- While global best practices are beneficial, solutions should be localized. This includes using local languages, understanding regional digital behaviours, and recognizing the socio-political realities of specific African regions or countries.

Promote Research:

4. Digital Inclusion

Develop policies that ensure equal access to digital resources, including subsidies for internet access in underserved areas.

Capacity building, strategic advocacy, and policy level advocacy engagement on opening of the civic space.

5. Data Security Education

Promote data security and privacy awareness through educational campaigns, focusing on safeguarding personal information online.

6. Public-Private Collaboration

Foster public-private partnerships to accelerate digital infrastructure development and enhance digital services.

7. Continual Monitoring

Monitor the progress of digital communication initiatives, conducting research to adapt strategies to evolving challenges.

9. Research and Data Collection

Prioritize research on digitalization's impact, collaborating with stakeholders to facilitate data collection and analysis. Encourage research on digital threats specific to the African context, which can inform strategies and interventions

10. Digitalization Gap Index

Develop a Digitalization Gap Index to measure progress and identify areas for targeted interventions.

11. Internet Penetration and Security

Promote policies that enhance internet penetration while ensuring data security and privacy.

12. Support Digital Transformation

Foster an environment conducive to digital entrepreneurship, providing incentives, funding, and mentorship for startups.

13. Bridging the Digital Divide

Develop strategies to bridge the digital divide, with a focus on infrastructure, subsidies, and digital literacy programs.

14. International Collaboration

Collaborate with international partners to share best practices, leverage resources, and address common digital challenges.

15. Policy Reflections

Conduct regular policy reflections to adapt digital policies to emerging issues while safeguarding digital rights.

16. Provide guidelines for what states shall do and provide norm on the use of digital platforms and digital engagements.

6.2 Agenda for in-person convening.

Convening an in-person meeting is highly recommended to discuss the recommendations stemming from the analysis of emerging issues and concerns in digital communication in Africa. Such a gathering would bring together key stakeholders, including government officials, policymakers, industry leaders, experts, and representatives from civil society organizations, providing an opportunity for meaningful engagement and collaboration. Face-to-face interactions allow for in-depth discussions, collaborative problem-solving, and the formation of crucial partnerships and alliances necessary for implementing the recommendations effectively. Additionally, these events serve to raise public awareness, foster trust among participants, and enhance accountability for achieving the goals related to digitalization in the region. While logistical considerations and safety measures must be taken into account, an in-person convening holds the potential to drive positive change in Africa's digital landscape.

6.3 Future Research Direction

While this research offers valuable insights into the current state of digital safety and security in Africa, it also highlights areas for future exploration. One promising avenue for future research pertains to the intersection of digital security and national security. Governments, in

the name of national security, often engage in censorship and surveillance, targeting activists and journalists. Investigating the delicate balance between safeguarding national interests and protecting human rights is an imperative area for further study. Understanding the mechanisms and implications of cyberespionage by governments, particularly in the African context, is vital for upholding democratic values and individual freedoms.

ANNEX A

Region	Name of Organization	What it does	**Scope of work** and specific focus area in the field of digital ommunication	Countries involved	Resource	Title
All over Africa	Smart Africa-	Smart Africa is an alliance of 38 African countries, international organizations and global private sector players tasked with Africa's digital agenda.	Policy, Access, e-Government, Private Sector/Entrepreneurship and Sustainable Development.	36 countries	https://smartafrica.org/who-we-are/	The beginning of a new era
All over Africa	African Declaration on Internet Rights and Freedoms	Pan-African initiative to promote human rights standards and principles of openness in Internet policy formulation and implementation on the continent		Has other Orgs as members	https://africaninternetrights.org/en/about#about-initiative	ABOUT THE INITIATIVE
Northern Africa	Web we Want	A global initiative of the World Wide Web Foundation		Egypt, Morocco		
East Africa (Uganda)	Africa Center for Media Excellence (ACME)	Main goal is to make the media a more effective platform for the provision of information on public affairs, a tool for monitoring official power, and a forum for vibrant public debate.		Uganda, Ghana, Kenya, South Sudan	https://acme-ug.org/about-acme/	About ACME
East Africa	Africa Center for Open Governance	\Aim to address the structural causes of the crisis of governance in East Africa.		East Africa		https://africog.org/
Northern Africa, Eastern Africa	Article 19	Works across the region in partnership with other national and regional organizations and mechanisms to safeguard freedom of expression and information, and to create solidarity networks aimed at achieving this goal.				https://www.article19.org/regional-office/eastern-africa/
East Africa	Association for Progressive Communications (APC)	A membership-based network of organizations and activists, founded in 1990, to empower individuals, organizations and social movements to	1. Digital empowerment 2. Social justice advocacy	The APC network has 62 organizational members and 41		

Region	Name of Organization	What it does	**Scope of work** and specific focus area in the field of digital ommunication	Countries involved	Resource	Title
		use information and communications technologies (ICTs) to build strategic communities to contribute to equitable human development, social justice, participatory political processes and environmental sustainability.	3. Internet governance 4. Gender equality promotion 5. Global ICT collaboration	associates active in 74 countries.		
WEST AFRICA	Centre for Information Technology and Developme nt (CITAD)	Organization that is committed to the use of information and communication technologies (ICTs) for development and promotion of good governance	Freedom of expression ICT for development (ICT4D)	Nigeria		
West Africa	Fantsuam Foundation	Organization that works with local communities to fight poverty and disadvantage through integrated development programmes. They were among the first orgs to promote ICT for development.	Access to information Community networks Environment and ICTs FLOSS Gender and ICTs	Nigeria		https://www.apc.org/en/member/fantsuam-foundation
East Africa	Internationa l Association of Women in Radio and Television - Kenya (IAWRT-K)	Global non-profit professional organization of women working in electronic media, technology and allied media.	Capacity building Digital security Gender and ICTs Media and ICTs	Kenya-Chapter		https://www.apc.org/en/member/international-association-women-radio-and-television-kenya-iawrt-k
East Africa	Zaina Foundation	Empowers women in technology through capacity building and workshops on digital security and privacy	Digital security and Internet rights	Tanzania		https://zainafoundationtz.org/
West Africa	Association des Utilisateurs des TIC, (ICT Users Association)	Promotes and protects human rights and fundamental freedoms in the digital age	Access to information Digital security Freedom of expression Gender and ICTs ICT for development (ICT4D) ICT policy Internet			https://asutic.org/home/

Region	Name of Organization	What it does	**Scope of work** and specific focus area in the field of digital ommunication	Countries involved	Resource	Title
			rights Privacy Transparency and ICTs			
North Africa	Social Media Exchange (SMEX)	Lebanese NGO that works to advance self-regulating information societies in the Middle East and North Africa (MENA)	Access to information Capacity building Cultural and linguistic diversity Digital security Freedom of expression Internet rights ICT for development (ICT4D) ICT policy Internet governance Media and ICTs Strategic use of the internet	Any Arab speaking countries in Africa	https://smex.org/who-we-are/	Who we are
East Africa	Kenya ICT Action Network (KICTANet)	A multi-stakeholder Think Tank for ICT policy and regulation. The Think Tank is a catalyst for reform in the Information and Communication Technology sector	Access to information Accessibility Activism Capacity building Community networks Digital security Free internet Freedom of expression Gender and ICTs ICT policy Internet governance Internet rights Media and ICTs	Kenya	https://www.kictanet.or.ke/	
West Africa	Media Awareness and Justice Initiative	An independent media initiative that supports independent media projects and development of innovative information and communications technologies (ICTs) for community use, and promotes participatory citizen journalism initiatives to increase transparency and accountability.	Media and ICTs	Nigeria	https://www.apc.org/en/member/media-awareness-and-justice-initiative	Media Awareness and Justice Initiative
East Africa	Policy	Feminist collective of technologists, data scientists, creatives and academics working at the	Capacity building Gender and ICTs Internet rights	Uganda	https://www.apc.org/en/member/pollicy	Policy

Region	Name of Organization	What it does	**Scope of work** and specific focus area in the field of digital ommunication	Countries involved	Resource	Title
		intersection of data, design and technology to craft better life experiences by harnessing improved data.	Internet governance			
Central Africa	Promotion of Technologies that Guarantee Environment and Quality of Life	Promote individual and collective initiatives to promote rural development, protect the environment and improve the well-being of communities	Access to information	Cameroon	https://www.apc.org/en/member/protege-qv	Protege-qv
Central Africa	Rudi International		focus on capacity building, advocacy and research in ICT	DRC	https://rudiinternational.org/	Rudi International FOR A BETTER FUTURE OF AFRICA!
Southern Africa	Zenzeleni Networks NPC	It offers quality, high-speed internet comparable to the country's most developed urban centres.	Access to information Community networks Low-cost technology Mobile networks Wireless technology	South Africa	https://www.apc.org/en/member/zenzeleni-networks-npc	Zenzeleni Networks
East Africa	Women of Uganda Network (WOUGNET)	Promote and support the use of ICTs by women and women's organizations	Gender and ICTs	Uganda	https://www.apc.org/en/member/women-uganda-network-wougnet-1	WOUGNET
East Africa	Unwanted Witness	Create secure uncensored online platforms to promote human rights through writing, informing and educating citizens who also utilize the platforms for strengthening free expression and demanding accountability.	Access to information Activism Capacity building Freedom of expression Internet rights Media and ICTs	Uganda	https://www.apc.org/en/member/unwanted-witness	Unwanted Witness
East and Southern Africa	Collaboration on Internet ICT Policy in East and	Works to promote effective and inclusive ICT policy and practice for improved governance, livelihoods, and human rights in Africa	Data Governance Internet Freedom Civic Participation	Uganda	https://cipesa.org/	

Region	Name of Organization	What it does	**Scope of work** and specific focus area in the field of digital ommunication	Countries involved	Resource	Title
	Southern Africa		Digital Resilience Digital Inclusion			
Southern Africa	Digital Society of Africa	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.	Organizational Security Assessments & Audits, Digital Security Trainings and Awareness Raising	Zimbabwe	https://digitalsociety.africa/	Digital Society of Africa
West Africa	Gambia Cyber Security Alliance	Increase awareness and the understanding of Gambians about cyber security, cyber threats, espionage and empowering them to be safer and more secure online	Cyber security, Online safety	Gambia	https://www.gamcyberalliance.org/	welcome to Gambia cyber security alliance
West Africa	African Centre for Coordination and Research in Cybersecurity	The centre acts to promote cybersecurity and the investigation of cybercrime.	Building capacities and supporting established cybersecurity agencies in African countries Collaborating with African governments, policymakers, law enforcement and security experts towards creating effective frameworks for assessing and mitigating cyberthreats and promoting cybersecurity in the regions Providing highly specialized technical and research capabilities for cybersecurity promotion in the region	Togo	hhttps://www.un.org/africarenewal/magazine/september-2022/togo-and-un-sign-mou-establish-african-cybersecurity-centre	Togo and UN sign MoU to establish the African Cybersecurity Centre
West Africa	Cyber Security Incident	CSIRT-GHANA is an organization dedicated to creating a cyber-secured	Their scope includes fostering digital literacy,	Ghana	http://www.csirtghana.org/	Who we are

Region	Name of Organization	What it does	**Scope of work** and specific focus area in the field of digital ommunication	Countries involved	Resource	Title
	Response Team Ghana	community by Educating individuals about cybercrimes and utilizing information technologies to enhance social well-being	providing adaptable safety strategies, and addressing emerging cyber threats to ensure a safer digital environment.			
West Africa	Liberia cyber-crime Prevention, and Mitigation Agency (LCCPMA)	A Non-Governmental Agency focused on delivering cyber security and digital forensics education to the people and government of Liberia	Cyber Security Education Digital Forensics Training Policy Formulation Training and Awareness Technical Assistance Development of Standards and Strategies Cyber Crime Assessments Cyber Defensive Capabilities	Liberia	https://thegfce.org/partners/liberia-cyber-crime-prevention-and-mitigation-agency-lccpma/#:~:text=LCCPMA's%20Mission%20is%20to%20enhance,formulations%2C%20training%2C%20and%20awareness.	Partner Profile Page
All over	Safer Internet Day	Safer Internet Day is an annual global event that raises awareness about emerging online issues and promotes safe internet usage. It involves the collaboration of Safer Internet Centres and Committees worldwide to provide educational campaigns, resources, and support for a better and safer online experience.	Organizing awareness campaigns, Providing educational resources, Running helplines for assistance, Collaboration with youth, International promotion and coordination Showcasing local, national, and international events		https://www.saferinternetday.org/in-your-country/liberia	About Safer Internet Day

Region	Name of Organization	What it does	**Scope of work** and specific focus area in the field of digital ommunication	Countries involved	Resource	Title
			Facilitating multilingual resources Exchange of ideas within internet safety community Supporting Safer Internet Day initiatives globally.			
West Africa	West Africa Civil Society Institute (WACSI)	Established by the Open Society Initiative for West Africa (OSIWA) in 2005, aims to reinforce civil society capacities in the West African sub-region.	From March 20 to 22, 2023, four civil society organizations (CSOs) gathered in Yaoundé for a training on Digital Security and Safety. The initiative, organized by the West Africa Civil Society Institute (WACSI) in collaboration with TechSoup and Hivemind, took place simultaneously in Cameroon, Liberia, and Côte d'Ivoire. Participants engaged in a participatory learning experience covering topics such as cybersecurity, secure communications, and risk assessment. The training aimed to equip CSOs with the knowledge and strategies to safeguard their digital assets and enhance their digital security efforts.	Ghana	https://wacsi.org/who-we-are/	

Region	Name of Organization	What it does	**Scope of work** and specific focus area in the field of digital ommunication	Countries involved	Resource	Title
East Africa	Encrypt Uganda	Encrypt Uganda empowers human rights defenders, activists, journalists, and bloggers in Uganda with knowledge and skills in digital safety and security to protect against threats like surveillance, censorship, hacking, and data loss. Through security awareness training, Encrypt enhances the trainees' digital security knowledge and skills to defend themselves against potential attacks and risks in the digital era.	Empowering human rights defenders, activists, journalists, and bloggers. Educating about digital safety and security. Addressing threats like surveillance, censorship, hacking, and data loss. Providing digital security awareness training.	Uganda	https://encryptuganda.net/index.php/digital-security/#	Digital awareness training
East Africa	DIG/SEC initiative	Founded with the purpose of enhancing the capacity of at-risk Grassroots journalists, activists, and other HRDs to overcome digital security and safety challenges they face daily while doing their work.	Capacity enhancement Skills building Mentorship Tech support Timely response Community empowerment	Uganda	https://www.digisecinitiative.org/	DIG/SEC initiative
East and the Horn of Africa region	Safe Sisters	The program combines self-study, tool practice, mentorship, workshops, peer sharing, and small grants to equip cohorts of women with the skills and support needed to navigate issues such as cyber-harassment, hacking, and online bullying. Safe Sisters aims to create a community of women technologists within civil society who can provide appropriate advice and assistance to HRDs facing complex digital threats.	Protection and security management, advocacy research in communication	East and Horn of Africa	https://defenddefenders.org/our-work/technology-and-digital-safety-3/safesisters/	What is safe sisters?
East and Southern Africa	CIPESA-Collaboration on	CIPESA focuses on leveraging ICT for good governance and human	Advocate for online rights	Uganda	https://cipesa.org/about-us/about-cipesa/	about CIPESA

Region	Name of Organization	What it does	**Scope of work** and specific focus area in the field of digital ommunication	Countries involved	Resource	Title
	International ICT Policy for East and Southern Africa	rights. Their scope of work related to digital security and safety includes advocating for online rights, promoting equal access, raising awareness on threats to free speech, and building digital security skills.	Promote equal access to information and ICT Raise awareness on threats to free speech Build digital security skills Engage in multi-stakeholder conversations on internet rights			
East Africa	HIVOS (INGO)	Digital defenders partnership (DPP) managed by HIVOS aims at bolstering the safety of human rights defenders facing digital threats and enhancing digital emergency response networks.	Enhance safety measures for human rights defenders under digital threats. Strengthen digital emergency response networks. Address shrinking online privacy and freedom through rights-based approaches. Provide emergency response and sustainable protection funding. Build capacity of rapid responders and local protection networks. Contribute to long-term organizational safety with Digital Integrity Fellowships. Develop resources for handling digital security attacks.	Kenya?? Tanzania, but DPP works worldwide	https://hivos.org/program/digital-defenders-partnership/	digital defenders partnerships

Region	Name of Organization	What it does	**Scope of work** and specific focus area in the field of digital ommunication	Countries involved	Resource	Title
			Collaborate with organizations like CiviCERT and Rarenet. Allocate annual budget of €3.5 million for strategic initiatives (2020-2023). Partner with Ministries of Foreign Affairs, SIDA, US State Department, and others. Collaborate with Media Defence, Front Line Defenders, Virtual Road, and more.			
East Africa	Tanzania Computer Emergency Response Team	Team with the responsibility of coordinating response to cyber security incidents at the national level and cooperate with regional and international entities involved with the management of cyber security incidents	network security	Tanzania	https://www.tzcert.go.tz/about-us/tz-cert-profile/	TCERT profile
Eastern Africa	Safety comm South Sudan	This is an online community/platform that provides tools, methodologies and resources on online safety		South Sudan	https://web.facebook.com/SafetyCommSS/?_rdc=1&_rdr&wtsid=rdr_0qFJcpe0lb7PcAkac	SafetyComm South Sudan
East Africa	Tech For Developme nt -T4D	An international tech consultancy and capacity building firm based in Nairobi Kenya.	Conducts trainings on digital safety and security	Kenya	https://comms.southsudanngoforum.org/t/fundamentals-of-digital-safety-and-cyber-security/43430	

Region	Name of Organization	What it does	**Scope of work** and specific focus area in the field of digital ommunication	Countries involved	Resource	Title
Eastern Africa	Digital Shelter		Digital safety trainings, promoting digital rights/inclusion security management, internet freedom and privacy rights			
East Africa	Epuka Ugaidi	Epuka Ugaidi is non-governmental, youth-based civil society organization based in Nairobi, established in 2015 at the peak of radicalization and recruitment into the outlawed Al-Shabaab terrorist organization.	Starting off as an online engagement platform to counter violent extremist narratives used to target online audiences, Epuka Ugaidi has since managed to incorporate both virtual and physical approaches in preventing and countering violent extremism	Kenya	https://www.epukaugaidi.com/	Fight Against radicalization

7. References

Faisal Ahmed Ghauri, "Digital Security Versus Private Information," July 2021, DOI: 10.5281/zenodo.5164002.

OECD (2022), OECD Policy Framework on Digital Security, OECD Publishing, Paris, https://doi.org/10.1787/a69df866-en

Mukiibi, Hood. (2019). Cyber security in Africa: The boring technology story that matters. XRDS: Crossroads, The ACM Magazine for Students. 26. 56-59. 10.1145/3368077.

Sentech Africa Tech Week. "The Importance of Cybersecurity in Africa's Digital Future." Sentech Africa Tech Week LinkedIn Page. https://www.linkedin.com/pulse/protecting-africas-digital-future-importance-cybersecurity/. Published March 22, 2023.

Ethiopia-Country Summary. (2023, August 30). Retrieved from The World Factbook: https://www.cia.gov/the-world-factbook/countries/ethiopia/summaries

Internet Penetration in Africa. (2022). Retrieved August 30, 2023, from https://www.internetworldstats.com/stats1.htm

Kenya-Country Summary. (2023, August 30). Retrieved from The World Factbook: https://www.cia.gov/the-world-factbook/countries/kenya/summaries

Internet Penetration in Africa. (2022). Retrieved August 30, 2023, from https://www.internetworldstats.com/stats1.htm

Nigeria-Country Summary. (2023, August 30). Retrieved from The World Factbook: https://www.cia.gov/the-world-factbook/countries/nigeria/summaries/#people-and-society

Internet Penetration in Africa. (2022). Retrieved August 30, 2023, from https://www.internetworldstats.com/stats1.htm

Zimbabwe-Country Summary. (2023, August 30). Retrieved from The World Factbook: https://www.cia.gov/the-world-factbook/countries/kenya/summaries

Internet Penetration in Africa. (2022). Retrieved August 30, 2023, from https://www.internetworldstats.com/stats1.htm

Bhorat, H., Signé, L., Asmal, Z., Monnakgotla, J., & Rooney, C. (2023). Digitalization and digital skills gaps in Africa: An empirical profile. Global Economy & Development Report. Brookings Institution. Retrieved from https://www.brookings.edu/wp-content/uploads/2023/05/Bhorat-et.-al-May-2023-Digitalization-and-digital-skills-in-Africa-2.pdf

Adame, Berhan Oumer, Ethiopian Telecom Industry: Gaps and Recommendations Towards a Meaningful Connectivity and a Thriving Digital Eco-System. Available at SSRN: https://ssrn.com/abstract=3885501 or http://dx.doi.org/10.2139/ssrn.3885501

Odongo, Agnes & Rono, Gideon. (2016). Kenya Digital and Cultural Divide. 85-94. 10.1145/2910019.2910077.

Okocha, Desmond & Edafewotu, Endurance. (2022). Bridging the Digital Divide in Nigeria. The Journal of Development Communication. 33. 45-54.

Tom, T. (2023). E-voting, Information Gap, and The Digital Divide in Zimbabwe. Technium Social Sciences Journal, 45(1), 284–305. https://doi.org/10.47577/tssj.v45i1.9167

Dube, H., Simiyu, M. A., & Ilori, T. (2020). Civil Society in the Digital Age in Africa: Identifying Threats and Mounting Pushbacks. Centre for Human Rights, University of Pretoria, and Collaboration on International ICT Policy in East and Southern Africa (CIPESA). ISBN: 978-1-920538-84-2.

Kaye, D. (2019, December 9). United Nations Special Rapporteur on the right to freedom of opinion and expression: Visit to Ethiopia, 2-9 December 2019 - End of mission statement [Press release]. Retrieved from https://www.ohchr.org/en/press-releases/2019/12/united-nations-special-rapporteur-right-freedom-opinion-and-expressiondavid

Bureau of Democracy, Human Rights, and Labor. (2022). 2022 Country Reports on Human Rights Practices: Ethiopia. Retrieved from https://www.state.gov/reports/2022-country-reports-on-human-rights-practices/Ethiopia

Bureau of Democracy, Human Rights, and Labor. (2022). 2022 Country Reports on Human Rights Practices: Kenya. Retrieved from https://www.state.gov/reports/2022-country-reports-on-human-rights-practices/kenya

Bureau of Democracy, Human Rights, and Labor. (2022). 2022 Country Reports on Human Rights Practices: Nigeria. Retrieved from https://www.state.gov/reports/2022-country-reports-on-human-rights-practices/Nigeria

Bureau of Democracy, Human Rights, and Labor. (2022). 2022 Country Reports on Human Rights Practices: Zimbabwe. Retrieved from https://www.state.gov/reports/2022-country-reports-on-human-rights-practices/Zimbabwe

Bhorat, H., Signé, L., Asmal, Z., Monnakgotla, J., & Rooney, C. (2023). Digitalization and Digital Skills Gaps in Africa: An Empirical Profile. Brookings Institution | Global Economy and Development.

GSMA. (2022). The Mobile Economy Sub-Sahara Africa 2022.

Digital & Connectivity Indicators. (2023, July). Retrieved from Statista: https://www.statista.com/outlook/co/digital-connectivity-indicators/ethiopia#server-security

Please note these points are very important in background ifnormation

International Frameworks and Conventions:

The Budapest Convention: Formally known as the Convention on Cybercrime, this is the first international treaty designed to address Internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations.

General Data Protection Regulation (GDPR): A European Union (EU) directive that provides guidelines for the collection and processing of personal information of individuals within the EU. It has set the benchmark for data protection globally.

The International Telecommunication Union (ITU): An agency of the United Nations, ITU, has numerous initiatives and guidelines on global cybersecurity.

Regional Frameworks and Conventions:

The African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention): Adopted by the African Union (AU) in 2014, this convention is a comprehensive continent-wide response to data protection, privacy rights, and cybersecurity. While it's a significant milestone, it requires more countries to ratify for it to come into force.

SADC Model Law on Computer Crime and Cybercrime: Developed by the Southern African Development Community (SADC), this provides a harmonized legal framework for combating cybercrime for its member states