United Nations
Interregional Crime and Justice
Research Institute

ACCESS TO JUSTICE IN THE DIGITAL AGE:

Empowering victims of cybercrime in Africa

ACCESS TO JUSTICE IN THE DIGITAL AGE:

Empowering victims of cybercrime in Africa

Disclaimer

Acknowledgements

This report is the product of an initiative led by the United Nations Interregional Crime and Justice Research Institute (UNICRI). It was written by Tina Power, Associate Director at ALT Advisory and UNICRI Consultant, under the guidance of Odhran McCarthy and Ottavia Galuzzi. UNICRI wishes to extend its gratitude to all the key stakeholders and partners who gave their time to be interviewed for the purposes of this research. Particular thanks and appreciation are due to the International Criminal Police Organization (INTERPOL) for facilitating many of the interviews. UNICRI also wishes to thank Kieran Jones for his editorial support and Antonella Bologna for the graphic design.

FOREWORD

Digital transformations are reshaping societies across the globe, opening new avenues not only economic in nature but also for peace, prosperity and the realization of human rights. Yet, these advances are accompanied by growing vulnerabilities as cyberthreats and online harms continue to escalate. This tension is most pronounced when rapid digital adoption outpaces the development of legal safeguards and institutional capacities. There are many parts of the world where people—especially women and girls—face increasing exposure to cybercrime without access justice or appropriate protections.

In our recent report *SDG 16 Through a Digital Lens*, UNICRI explored the intricate interplay between digitalization and the pursuit of peace, justice and strong institutions. It emphasizes the need to ensure that digital transformations advance the 2030 Agenda for Sustainable Development rather than hinder it. Using Namibia, Sierra Leone, South Africa and Uganda as case studies, *Access to Justice in the Digital Age: Empowering Victims of Cybercrime in Africa* builds on this foundation by taking a closer look at the specific—and growing—impact of cybercrime on SDG 16 across Africa.

By examining how digital threats undermine access to justice, equality before the law and the protection of fundamental rights, this report deepens our understanding of the evolving risks of the digital era and how to respond to them. Based on our conclusions, we present evidence-based recommendations to improve legal protections and enhance institutional capacity to respond to cybercrime while supporting victims. Although the research was conducted in four countries, the recommendations are broadly applicable across Africa as well as other parts of the world.

As part of UNICRI's broader workstream on cybercrime and online harms, this study reflects our ongoing mission to develop inclusive, rights-based and victim-centred approaches to countering cyberthreats. We remain committed to working with Member States, regional bodies and partners across sectors to ensure that justice systems respond to cybercrime with fairness, accessibility and empathy at their core.

Leif Villadsen

Acting Director
UNICRI

TABLE OF CONTENTS

List of acronyms and abbreviations

African Charter:	African Charter on Human and Peoples' Rights
Budapest Convention:	Council of Europe Convention on Cybercrime
COE:	Council of Europe
DPCI:	South Africa Directorate for Priority Crime Investigation
GBV:	Gender-based violence
ICTs:	Information and communications technologies
ITU:	International Telecommunication Union
Malabo Convention:	African Union Convention on Cyber Security and Personal Data Protection
Maputo Protocol:	Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa
MICT:	Namibian Ministry of Information and Communication Technology
NamPol:	Namibian Police Force
NC3:	Sierra Leone National Cybersecurity Coordination Center
NCII:	Non-consensual dissemination of intimate images
SADC:	Southern African Development Community
SAPS:	South African Police Service
SLP:	Sierra Leone Police
SOP:	Standard operating procedure
UNDP:	United Nations Development Programme
UPF:	Uganda Police Force

EXECUTIVE SUMMARY

Africa's digital transformation is advancing rapidly, bringing immense socio-economic opportunities. Concerningly, it is also exposing individuals—particularly women and girls—to increasing cyberthreats and online harms. The rise of cybercrime presents complex challenges as many victims struggle to access justice due to fragmented legal frameworks, underreporting and limited institutional capacity. As Internet penetration and digital adoption continue across the continent—and the gap between technological advances and legal protections becomes more evident—urgent and coordinated responses are needed at national and regional levels.

This report examines these challenges in Namibia, Sierra Leone, South Africa and Uganda, highlighting key trends and providing evidence-based recommendations to strengthen legal protections and improve access to justice. Drawing on case studies, stakeholder interviews and a comparative analysis of cybercrime laws, it explores the systemic barriers that hinder effective responses to online harms and cyberthreats.

Key findings reveal that:

A significant data gap in cybercrime statistics prevents policymakers from fully understanding the scope and impact of these threats, leading to inadequate response measures.

This data gap is often fuelled by **underreporting,** which is influenced by a range of factors including stigma, fear of retaliation and limited knowledge of legal rights and reporting mechanisms.

Women are disproportionately affected by cyberstalking, online harassment, cyberbullying and the non-consensual sharing of intimate images. Too often, this goes underreported due to stigma, fear and lack of trust in justice mechanisms. The lack of gender-sensitive approaches in law enforcement further exacerbates this issue.

Law enforcement and judicial bodies face **capacity constraints** investigating and prosecuting cybercrimes, including a lack of technical expertise, insufficient resources and weak cross-border cooperation.

Legal frameworks remain **inconsistent** and in some cases **unenforceable**, creating loopholes that limit accountability for cybercriminals.

Awareness campaigns and digital literacy initiatives exist but require **expansion, standardization** and **stronger engagement** with vulnerable communities.

The rapid evolution of digital threats requires adaptive and forward-looking policy interventions. These efforts need to be responsive, empowering and should ultimately contribute towards strengthening access to justice. To address the present trends and challenges, the report proposes the following evidence-based recommendations:

Adopt gender-transformative approaches, which address both the immediate needs of victims and interrogate and respond to systemic inequalities, to ensure safer digital spaces for women, as well as marginalized groups.

Ratify and domesticate international treaties such as the African Union Convention on Cyber Security and Personal Data Protection and the Council of Europe Convention on Cybercrime. This would strengthen legal frameworks, enhance international cooperation and affirm robust and rights-respecting responses to cybercrimes.

Develop an updated, victim-centred continental model law on cybercrime to guide national legislation and ensure harmonization across jurisdictions. This should be accompanied by legislative audits to assess the current frameworks and pathways to justice for victims of cybercrimes.

Establish clear and accessible reporting mechanisms to build trust and encourage victims to seek justice. These mechanisms should be victim-friendly and empowering.

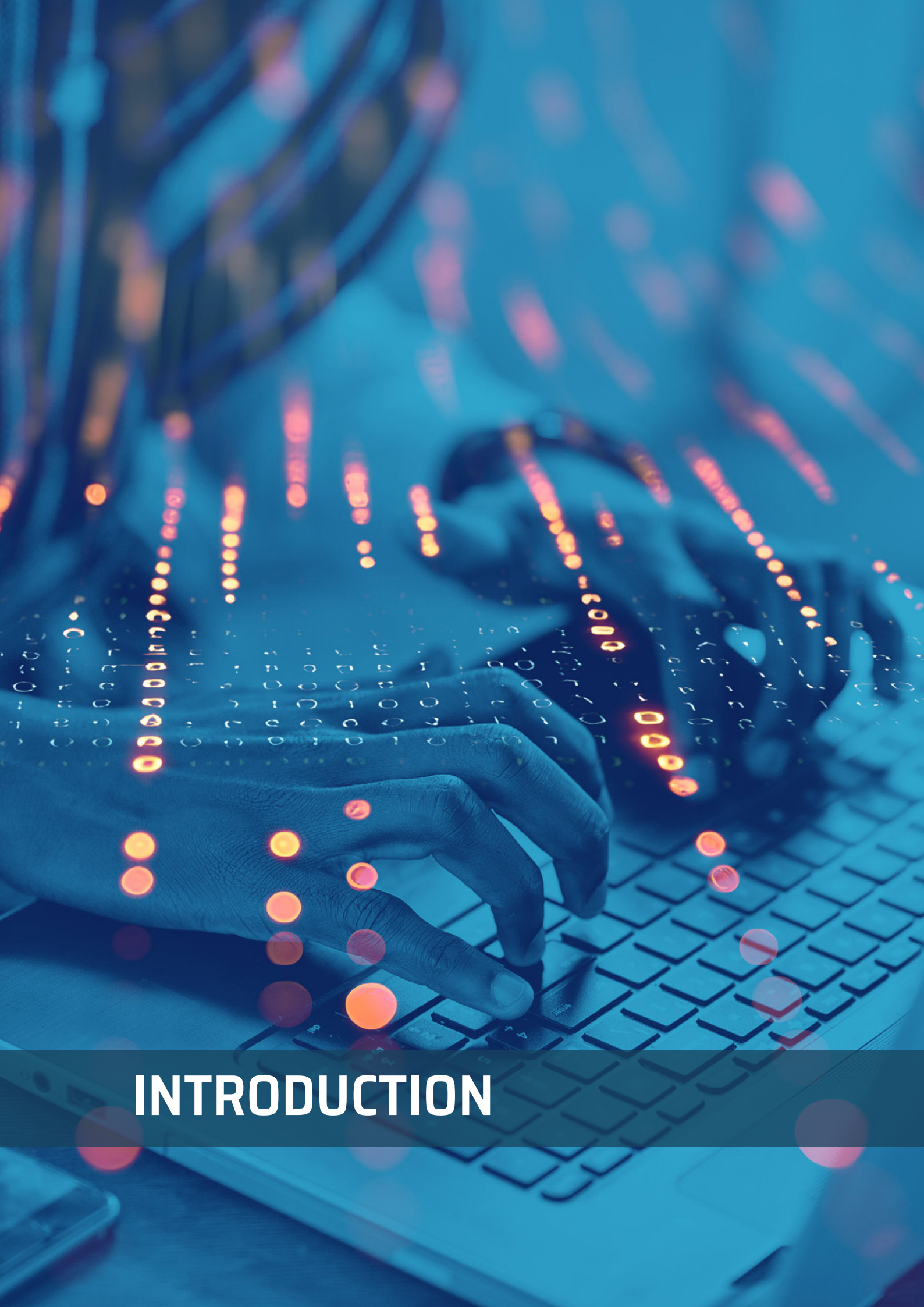
Create standardized cybercrime coding systems to improve data collection, which in turn can better inform policy decisions. Both internal and public-facing coding systems should be clear and accessible.

Implement standard operating procedures for law enforcement to ensure victim-centred approaches and consistent responses. They could be enriched through international learning exchanges in which countries share experiences and lessons with each other.

Provide comprehensive training for justice sector stakeholders to enhance their ability to investigate, prosecute and adjudicate cybercrimes. Joint training that brings together various justice sector stakeholders can help ensure a holistic understanding of the cybercrime justice cycle.

Launch "Know Your Rights" campaigns to raise awareness about legal protections and reporting mechanisms. They should empower people to navigate various online spaces safely and equip them with the skills to report and respond to cybercrimes.

Strengthening legal protections, enhancing institutional capacity and promoting digital literacy are crucial to ensure the benefits of digital transformation are not undermined by the growing risks of cybercrime. By implementing these recommendations, governments, civil society and other stakeholders can build more resilient justice systems that uphold rights, protect victims and foster inclusive and secure digital environments across Africa.



INTRODUCTION

In recent decades, African states have increasingly turned to digital technologies as a catalyst for social and economic development and the realization of fundamental rights.[1] While this expanding digital landscape holds transformative potential, it is accompanied by parallel risks and harms that threaten to undermine these advances.[2] Those who make use of digital technologies and engage in the online world are increasingly at risk of an array of cybercrimes and online harms.[3] Women in particular face online abuse that is part of the continuum of multiple, recurring and interrelated forms of gender-based violence (GBV).[4]

Despite the clear need for robust responses, many African governments, law enforcement agencies and judicial bodies continue to struggle with the rapidly evolving nature of cybercrimes. In many cases, this challenge is compounded by the absence of comprehensive and harmonized laws and policies.[5] The uncertainty surrounding legal frameworks, alongside the lack of awareness among victims about their rights and available remedies, has resulted in limited access to justice. Considering this, there is an urgent need to strengthen local response mechanisms so victims not only know their rights but also have the tools and support to navigate the justice system. This report aims to examine these issues and propose evidence-based recommendations to empower victims, foster inclusive justice systems and promote resilience in the face of digital threats across Africa.

The report will explore the **prevalence of cybercrimes** and the **challenges faced by victims in accessing justice** and the **legal, capacity and educational frameworks** needed to address them. It presents an analysis of current practices and the way forward for more effective, inclusive and victim-centred responses to cybercrime. Though it has a focus on **Namibia**, **Sierra Leone**, **South Africa** and **Uganda**, the report aims to be broadly applicable across the African continent.

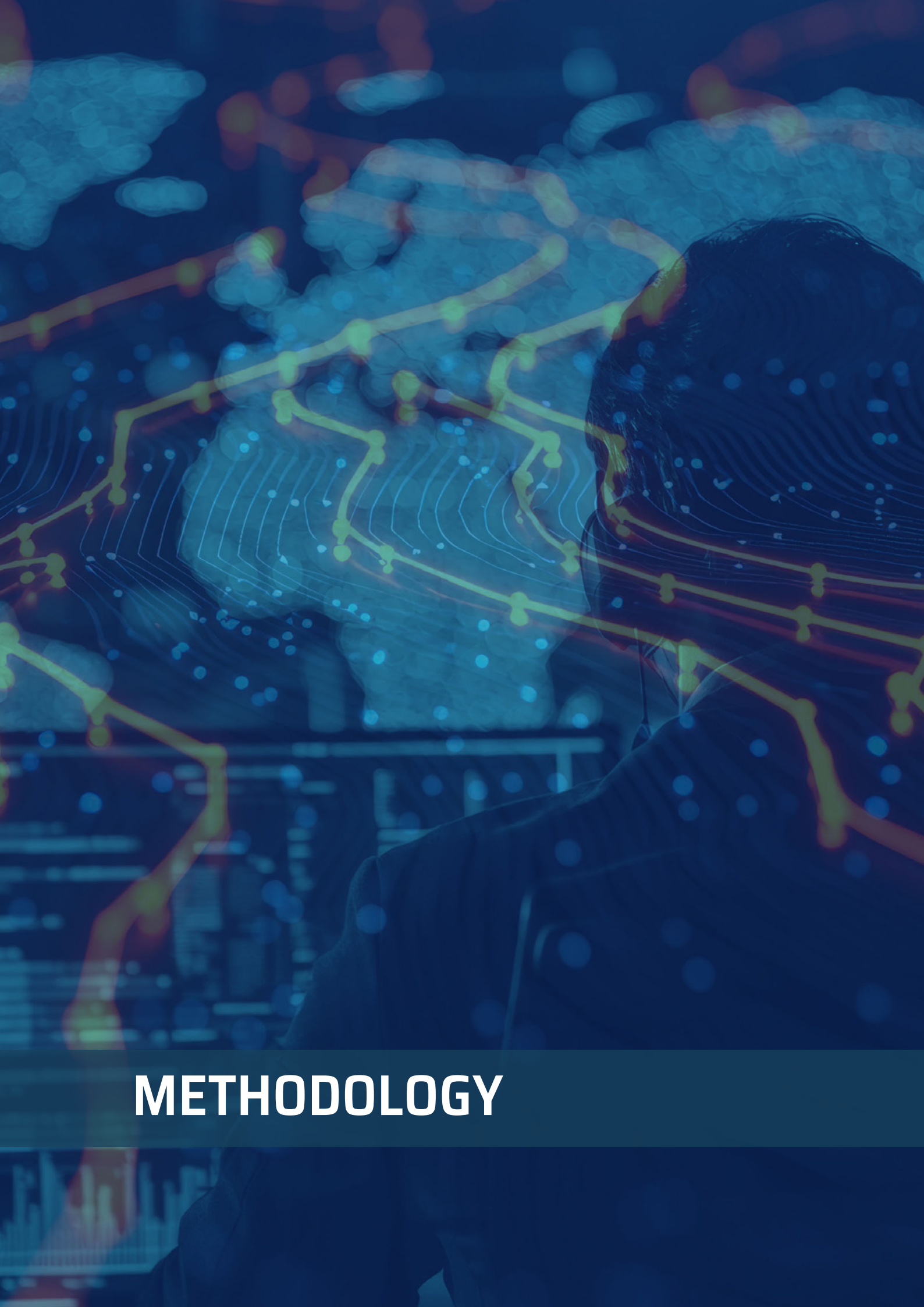
1 African Union, "The Digital Transformation Strategy for Africa (2020-2030)", accessible at: https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf.

2 United Nations General Assembly, "Countering the use of information and communications technologies for criminal purposes", A/RES/74/247, 2020, accessible at: https://documents.un.org/doc/undoc/gen/n19/440/28/pdf/n1944028.pdf.

3 INTERPOL, "African Cyberthreat Assessment Report 2024", accessible at: https://www.interpol.int/content/download/21048/file/24COM005030-AJFOC_Africa%20Cyberthreat%20Assessment%20Report_2024_complet_EN%20v4.pdf.

4 UN Human Rights Council, "Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective", A/HRC/38/47, 2018, accessible at: https://digitallibrary.un.org/record/1641160?ln=en&v=pdf.

5 African Union, "African Union Convention on Cyber Security and Personal Data Protection", 2014, accessible at: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.



METHODOLOGY

Grounded in action-oriented research, this study investigates the individual and systemic barriers preventing victims of cybercrime from accessing justice. It aims to develop knowledge, encourage collaboration and provide implementable recommendations that can open pathways to access justice. In doing so, a **mixed methods approach** was applied, combining qualitative and quantitative research techniques. Data collection included open-source research and interviews with key stakeholders during in-person visits to the four selected countries. The **qualitative** research comprised comprehensive desk research and a situational analysis of digital, socio-economic, legal and policy landscapes. A detailed desktop review was conducted, analyzing existing literature, reports, legal frameworks and case law to document current practices and identify barriers and bottlenecks preventing access to justice for victims of cybercrime. The **quantitative** component, detailed below, involved conducting interviews with key informants to collect in-depth and nuanced perspectives to supplement and contextualize the findings.

Country selection

Four countries across East, West and Southern Africa—**Namibia**, **Sierra Leone**, **South Africa**, and **Uganda**—were strategically selected to provide a representative yet manageable sample for analysis.

The countries initially shortlisted participated in the Voluntary National Reviews at the High-Level Political Forum on Sustainable Development 2024, during which SDG 16—promoting peace, justice and strong institutions—was under review.[6] This list was narrowed down based on the following criteria:

- engagement with digital transformation
- interest and willingness by government and civil society organizations to address cybercrimes
- signatory status on relevant regional legal instruments
- existing legal frameworks

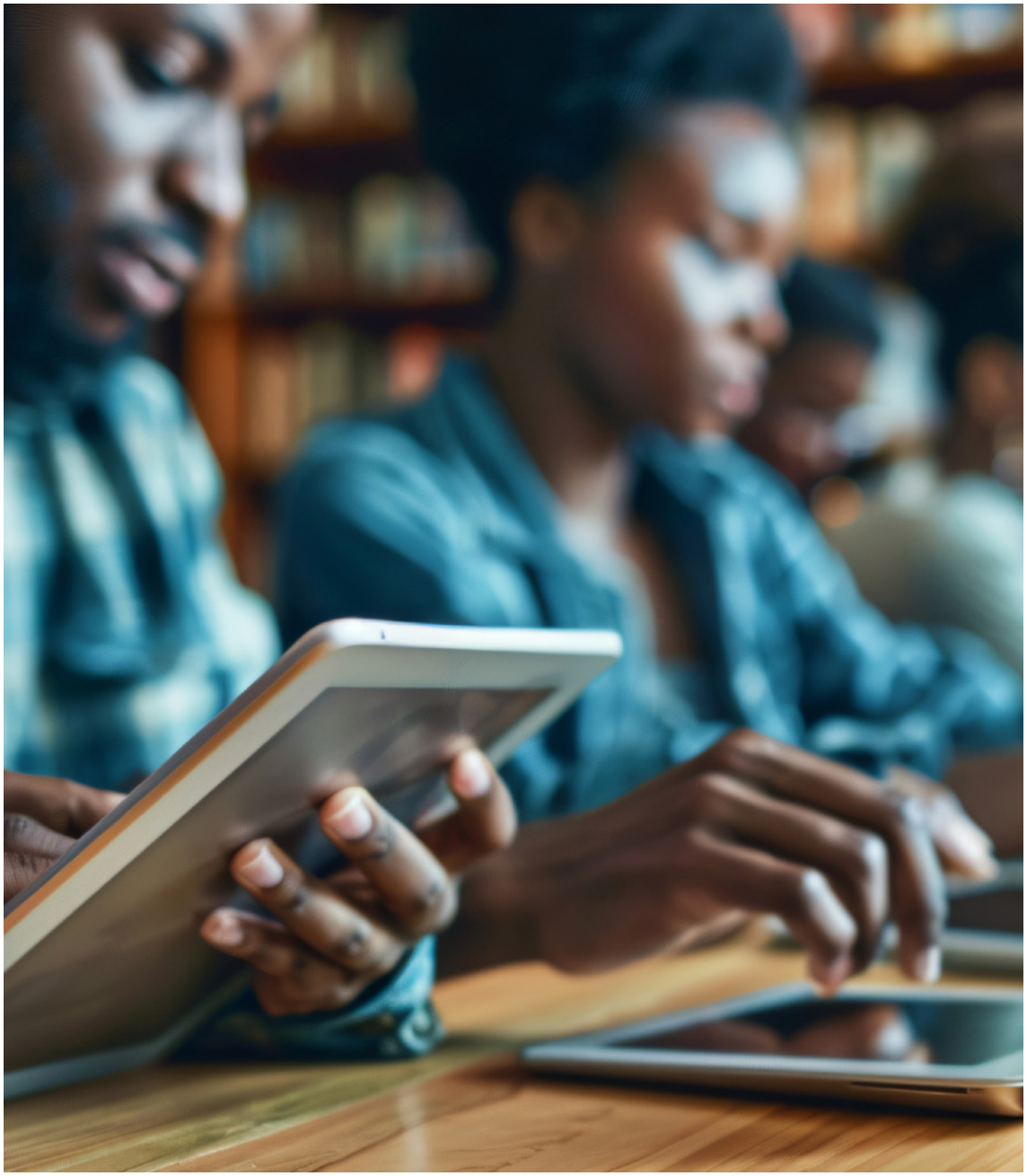
Consideration was also given to regional representation; political and socio-economic climate; the status of law enforcement agencies and judicial bodies; and the availability of academic, policy and other resources to inform the study.

6 Member States participating in the Voluntary National Reviews for the 2030 Agenda for Sustainable Development during the 2024 High-Level Political Forum: Chad; the Republic of Congo; Egypt; Eritrea; Guinea; Guinea-Bissau; Kenya; Libya; Mauritania; Namibia; Sierra Leone; South Africa; South Sudan; Uganda; and Zimbabwe.

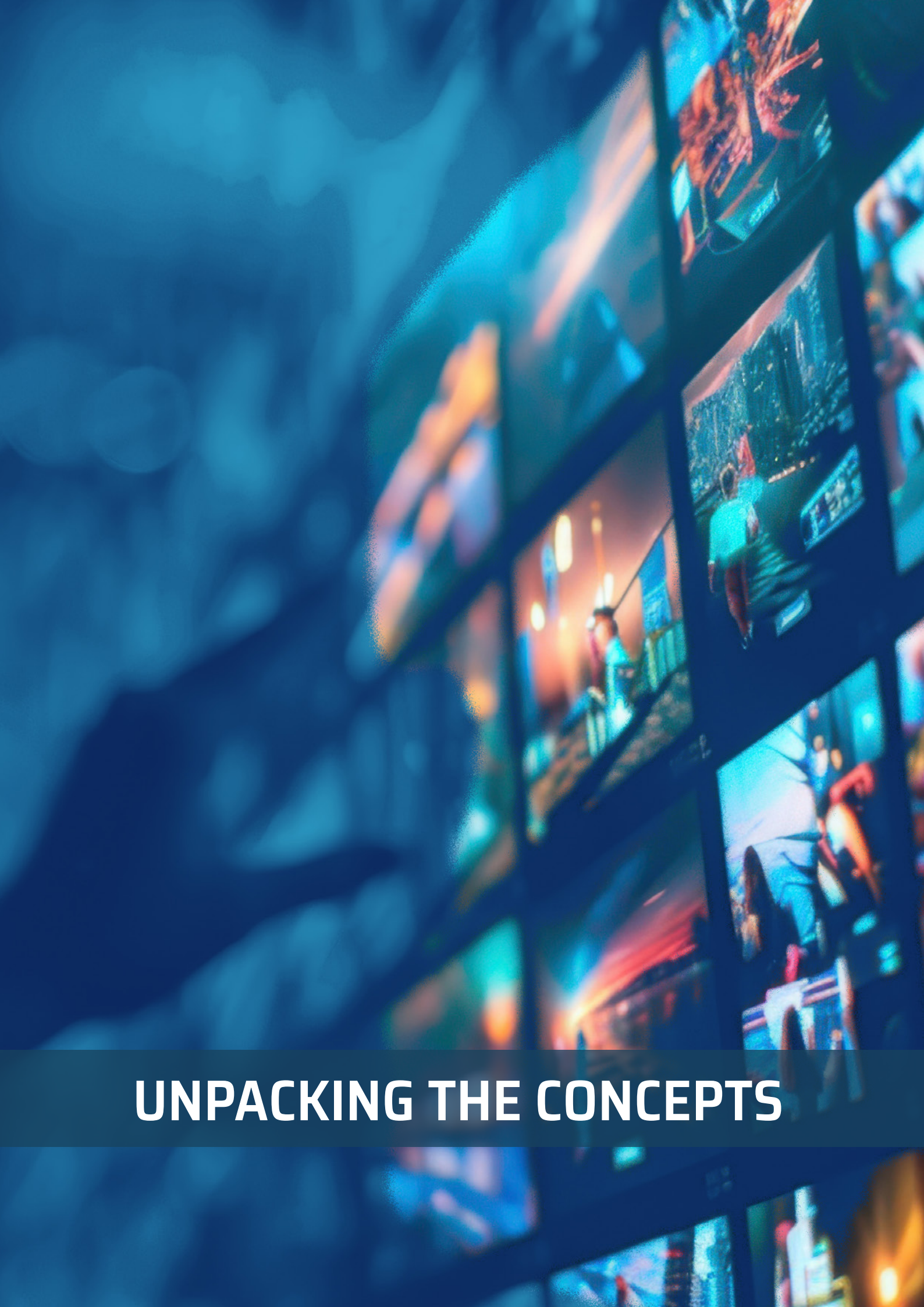
Country visits and key informant interviews

To ensure a comprehensive and contextually grounded analysis, the research included brief in-person visits to the four selected countries to conduct interviews with key informants. They allowed direct interaction with diverse stakeholders, including policymakers, law enforcement officials, legal professionals and civil society representatives, enriching the findings with localized perspectives and lived experiences.

Overall, **40 key informants were interviewed**. Consideration was given to their expertise, roles, availability and willingness to participate, and gender representation. These engagements provided valuable insights into the practical realities of advancing access to justice in the selected countries, as well as the challenges and opportunities. The diversity of stakeholders gave a broad spectrum of perspectives, which led to a nuanced and holistic understanding of specific issues in each country.



“Access to justice for victims of cybercrime requires more than legal frameworks—it demands local insight, stakeholder collaboration, and context-sensitive solutions.”



UNPACKING THE CONCEPTS

To help interpret this study's findings and recommendations, this section unpacks its central concepts, namely **victims**, **access to justice** and **cybercrime**.

Victims

Within the criminal justice system, the term victim refers to a person who has been **subjected to a crime**. It is also a legal status that **affords certain rights** under the law.[7] For the purposes of this report, victims are defined as individuals or groups who have suffered harm or experienced a substantial impairment of their fundamental rights due to acts or omissions in violation of the law.[8] However, it is necessary to note that different crimes affect individuals differently, and those who have experienced harm relate to their experiences in varied ways. This includes how they define their experience; for some, victim is the preferred term whereas others prefer survivor. This report uses the term victim for consistency, but its usage is not intended to impose a fixed definition or response on those who have experienced cybercrime. This is particularly relevant to cybercrimes of a personal nature causing an egregious affront to a person's dignity and privacy. Instead, the report acknowledges and respects the **diverse ways in which individuals process and frame their experiences, recognizing the importance of maintaining dignity and agency when advancing access to justice.**

Access to justice

Access to justice is key to enabling people to have their voices heard, exercise their rights and hold decision makers accountable.[9] In its narrowest sense, access to justice speaks to **legal rights, processes and procedures**,[10] and is often understood as the ability to bring a legal issue to court to seek and obtain a just resolution.[11] From a victim's perspective, it means **compassionate treatment, respect for their dignity** and **access to the mechanisms of justice and prompt redress**.[12] This relies on functioning systems that are structured and administered to provide fair, accessible, efficient and appropriate procedures through which they can resolve harms and enjoy their rights. It further encompasses "the equity with which those

7 United Nations General Assembly, "Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power", Resolution 40/34, 1985, accessible at: https://www.ohchr.org/en/instruments-mechanisms/instruments/declaration-basic-principles-justice-victims-crime-and-abuse.

8 Ibid.

9 United Nations website, "Access to Justice", accessible at: https://www.un.org/ruleoflaw/thematic-areas/access-to-justice-and-rule-of-law-institutions/access-to-justice/?form=MG0AV3.

10 Mathias Nyenti, "Access to justice in the South African social security system: Towards a conceptual approach", De Jure, 2013, accessible at: https://www.saflii.org/za/journals/DEJURE/2013/44.pdf.

11 Organisation for Economic Co-operation and Development, "Equal Access to Justice for Inclusive Growth", 2019, accessible at: https://www.oecd.org/en/publications/equal-access-to-justice-for-inclusive-growth_597f5b7f-en.html.

12 United Nations General Assembly, "Declaration of Basic Principles of Justice".

from differing backgrounds are able to gain from the justice delivery system and enjoy equality before the law".[13]

For victims of cybercrime to meaningfully access justice, suitable legal pathways with several interconnected factors in place need to be established[14]:

- **Conducive legal frameworks:** A conducive legal framework is essential to enable access to justice and safeguarding people's rights,[15] as well as enhancing the justice system's responsiveness to online harms and cybercrimes. At a minimum, laws should be clear, consistent, accessible and compliant with the rule of law and human rights standards.[16] They must strike a balance between flexibility and stability, allowing for adaptation to emerging technologies while maintaining the necessary consistency and reliability of the legislative framework.[17] Laws must also be grounded in equality and non-discrimination in both content and practice, and be proportionate to and effective in addressing cybercrimes. Cybercrime legislation also requires clarity on evidence and criminal procedures unique to this form of criminal activity.[18]

- **Rights awareness**: These pathways require people to know their rights and the remedies available to them.[19] First, online crimes need to be recognized as real crimes.[20] Unlike visible crimes such as burglary or assault, cybercrime is often perceived as intangible. This makes it harder to identify its impact or acknowledge certain actions as criminal offences. Second, people need to know where to report or to whom they should report Third, victims must also know their legal options and how they should be treated during the justice process. Finally, rights awareness also plays a preventive role, equipping individuals with the knowledge and skills to protect themselves against cybercrime.[21] Educational initiatives promoting digital literacy and cybersecurity are essential to build this awareness. Such efforts empower individuals to recognize cybercrimes, seek justice when affected and adopt measures to protect themselves. Access to justice for cybercrime victims depends on bridging the knowledge gap and

13 Kholeka Gcaleka, "Access to Justice: Emerging issues and challenges in Justice Administration in Africa", Annual Conference of the African Bar Association, 2023, accessible at: https://www.pprotect.org/sites/default/files/speeches/Paper%20on%20Access%20to%20Justice%20African%20Bar%20Association%2010%20August%202023.pdf.

14 Organisation for Economic Co-operation and Development, "Recommendation of the Council on Access to Justice and People-Centred Justice Systems", 2023, accessible at: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0498.

15 Southern African Litigation Centre, "Goal 16 of the Sustainable Development Goals: Perspectives from Judges and Lawyers in Southern Africa on Promoting Rule of Law and Equal Access to Justice", 2016, accessible at: https://www.southernafricalitigationcentre.org/wp-content/uploads/2017/08/GOAL-16-Book.pdf.

16 Organization for Security and Co-operation in Europe Office for Democratic Institutions and Human Rights, "Guiding Principles of Democratic Lawmaking and Better Laws", 2023, accessible at: https://www.osce.org/files/f/documents/c/a/552682.pdf.

17 Ibid.

18 United Nation Office on Drugs and Crime website, "The role of cybercrime law", accessible at: https://sherloc.unodc.org/cld/en/education/tertiary/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html.

19 United Nations General Assembly, "Declaration of Basic Principles of Justice".

20 INTERPOL website, "New campaign will raise awareness of the top cyberthreats and how to stay safe", 2020, accessible at: https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-reminds-public-that-OnlineCrimeIsRealCrime.

21 Ibid.

ensuring that everyone understands their rights and the resources available to them.

- **Institutional capacity:** This comprises several operational aspects focusing on the ability of institutions to enable access to justice:
  - **Victim-centred approach:** From reporting a crime through to investigation, prosecution and enforcement, a victim-centred approach protects dignity and guards against further victimization. Appropriate safeguards need to be in place to ensure that victims do not experience shame or stigma when reporting crimes.
  - **Viable reporting mechanisms**: Viable reporting mechanisms—particularly in law enforcement—need to be both rights-protecting and capable of addressing the specific crime reported. This means law enforcement officials respecting and protecting everyone's human rights[22] and having the required legal and technical capacity to identify, refer and investigate crimes appropriately.
  - **Independent resolution mechanisms:** For the purposes of this study, the focus is on the judiciary as the appropriate resolution forum. This requires judicial independence so courts can adjudicate disputes impartially and without fear or favour.[23] Adequate resources and training are needed to adjudicate and enforce the law effectively.
  - **Skilled prosecutors:** Prosecutors play an important role in enabling access to justice and require appropriate and ongoing training.[24]
  - **Support structures:** Victims should have access to free, comprehensive psycho-social support and should be informed of the availability of other forms of relevant support.[25]

Access to justice for all requires **appropriate legal frameworks** and **awareness of rights and remedies**. It also depends on a **well-equipped criminal justice system** that respects, protects and promotes human rights while being technically skilled to handle complaints, investigations, prosecutions and judgments.

22 United Nations General Assembly, "Code of Conduct for Law Enforcement Officials", Resolution 34/169, 1979, accessible at: https://www.ohchr.org/en/instruments-mechanisms/instruments/code-conduct-law-enforcement-officials.

23 United Nations General Assembly, "Basic Principles on the Independence of the Judiciary", Resolution 40/32, 1985, accessible at: https://www.ohchr.org/en/instruments-mechanisms/instruments/basic-principles-independence-judiciary.

24 Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, "Guidelines on the Role of Prosecutors", 1990, accessible at: https://www.ohchr.org/en/instruments-mechanisms/instruments/guidelines-role-prosecutors.

25 United Nations General Assembly, "Declaration of Basic Principles of Justice".

Cybercrime

While there is no universal definition of cybercrime, by drawing on existing and emerging laws and frameworks it is understood to include a **range of offences** including: illegal and unauthorized access to and interception of data, systems and devices; misuse of devices; fraud; theft; and offences relating to online child sexual abuse.[26] The recently adopted United Nations Convention against Cybercrime considers an array of offences as cybercrimes. It includes but is not limited to illegal access to, interception of and interference with electronic data; the misuse of devices; information and communications technology system-related theft or fraud; online child sexual abuse or child sexual exploitation material; and non-consensual dissemination of intimate images (NCII).[27]

Cybercrimes can be "cyber-dependent" such as hacking or spreading malware, which rely on computers or networks to be carried out; or "cyber-enabled" like fraud and cyberstalking, which use information technology or digital spaces as tools to act and commit traditional crimes.[28] Cybercrimes can also vary in scope and impact, with some targeting individuals—whether known or unknown to the perpetrator—and others affecting small businesses and civil society organizations or crippling major corporations, governments and critical infrastructure.[29]

Online harms—technology-facilitated or wholly digital violence—are often linked with cybercrimes, but they are distinguishable from commonly considered examples like fraud, theft and hacking. Online harms include online harassment and cyberbullying; non-consensual intimate image (NCII) abuse; violent content;[30] hate speech; and incitement to violence.[31] They are often manifestations of offline forms of hate, violence and discrimination. In some cases these harms fall within the purview of criminal conduct; in others, they do not amount to criminal activity but may warrant other forms of legal protection for victims.[32] Due to the disproportionate gendered impact of online harms, they are also often referred to

26 INTERPOL, "National Cybercrime Strategy Guidebook", 2021, accessible at: https://www.interpol.int/content/download/16455/file/Cyber_Strategy_Guidebook.pdf; Council of Europe (COE), "Convention on Cybercrime Budapest", 2001, accessible at: https://rm.coe.int/1680081561; African Union, " African Union Convention on Cyber Security and Personal Data Protection"; United Nations General Assembly, "United Nations Convention against Cybercrime", A/RES/79/243, 2024, accessible at: https://documents.un.org/doc/undoc/gen/n24/426/74/pdf/n2442674.pdf; Media Defence, "Summary Modules on Digital Rights and Freedom of Expression Online in sub-Saharan Africa: Cybercrimes", 2024, accessible at: https://www.mediadefence.org/ereader/publications/introductory-modules-on-digital-rights-and-freedom-of-expression-online/module-7-cybercrimes/.

27 United Nations General Assembly, "United Nations Convention against Cybercrime".

28 Rabalo and others, "Cyber Victimisation, Restorative Justice and VictimOffender Panels", Asian Journal of Criminology, 2023, accessible at: https://pmc.ncbi.nlm.nih.gov/articles/PMC9936482/pdf/11417_2023_Article_9396.pdf.

29 Ibid.

30 In this report, "violent content" refers to a wide range of material depicting, among others, terrorism, violent extremism, murder and suicide.

31 African Commission on Human and Peoples' Rights, "Resolution on the Protection of Women Against Digital Violence in Africa", ACHPR/Res. 522, 2022, accessible at: https://achpr.au.int/en/adopted-resolutions/522-resolution-protection-women-against-digital-violence-africa-achpr; COE, "The relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in addressing online and technology-facilitated violence against women", 2021, accessible at: https://rm.coe.int/the-relevance-of-the-ic-and-the-budapest-convention-on-cybercrime-in-a/1680a5eba3.

32 UK Government, "A Summary – Online Harms White Paper", accessible at: https://www.gov.uk/government/consultations/online-harms-white-paper.

as “technology-facilitated gender-based violence”, “online gender-based violence” or “technology-facilitated violence against women”.[33]

For the purposes of this report—which has a particular focus on individuals as victims—cybercrimes are understood to encompass a broad range of unlawful activities using digital means or information and communications technologies (ICTs) to carry out criminal activities. These activities include fraud and online scams; ransomware; digital extortion; privacy and data protection violations, including cyberstalking and doxxing; online hate speech and violent content; NCII; online harassment; online sexual exploitation; and cyberbullying, among others.

At an individual level, cybercrime manifests in two primary ways: financial and personal harm. **Financial harm** can be both cyber-dependent and cyber-enabled and causes financial loss to the victim. Attacks can be made on information systems or through fraud and forgery.[34] It includes activities such as stealing payment card information, gaining access to bank accounts to initiate unauthorized transactions and extortion or impersonation for unlawful financial gain.[35]

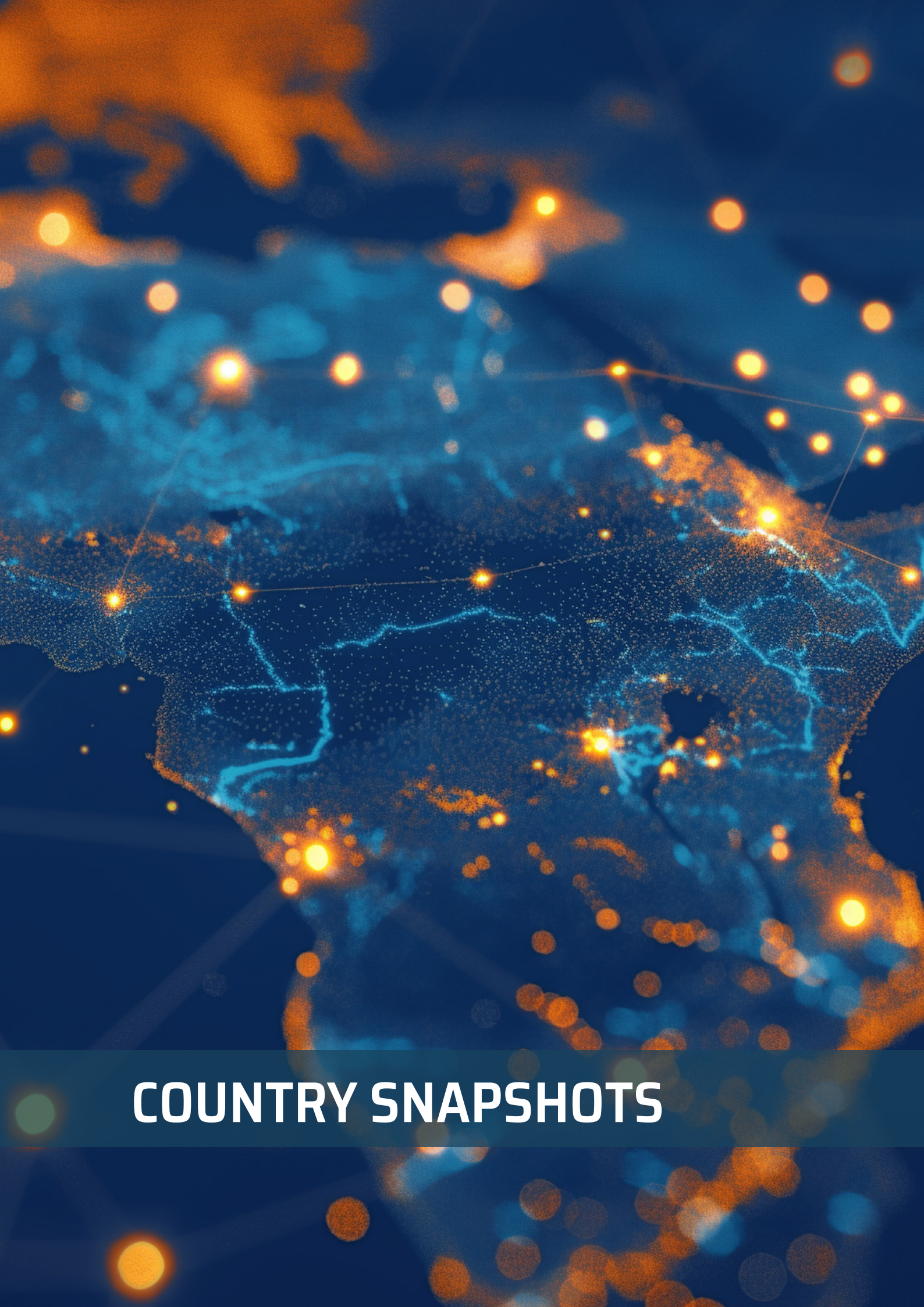
Cybercrimes that cause **personal harm** impact the victim’s safety and security (both physical and psychological), dignity, privacy, freedom of expression and other rights. Examples of this include but are not limited to NCII, online harassment, cyberstalking and online hate speech and incitement.[36] These personal harms are more commonly associated with online harms as an overarching term.

33 UN Human Rights Council, “Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective”.

34 European Commission website, “Cybercrime”, 2024, accessible at: https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en?form=MG0AV3.

35 Global South Dialogue on Economic Crime website, “Cybersecurity and Financial Crimes”, 2024, accessible at: https://gsdec.network/8374/cybersecurity-and-financial-crimes/.

36 Media Defence, “Digital Attacks and Online Gender-based Violence”, 2024, accessible at: https://www.mediadefence.org/ereader/wp-content/uploads/sites/2/2024/06/Module-2-Digital-attacks-and-OGBV-2024.pdf.



COUNTRY SNAPSHOTS

The intersection of access to justice and digital transformation is shaped by the selected countries' socio-economic and political landscapes, which influence how effectively cybercrime victims can seek and obtain justice. Presently, Namibia, Sierra Leone, South Africa and Uganda have diverse economic, political and social contexts and are at different stages of their digital transformation journey.

Namibia

With a population of 3 million people, Namibia is one of the least densely populated countries in the world.[37] Despite being classified as an upper-middle income country due to its abundant natural resources, it faces significant economic challenges. These include high levels of income inequality, unemployment and poverty, particularly in rural areas.[38] Its Internet penetration rate is 53 per cent.[39] It has a relatively stable political environment, save for tensions regarding the credibility of the November 2024 elections.[40] Namibians enjoy their constitutional rights to freedom of expression and access to information,[41] but there are concerns about privacy and data protection.[42] Namibia has signaled its strong political will to address this and is on the brink of adopting cybercrime legislation. The Namibian Ministry of Information and Communication Technology's (MICT) focus on enhancing access to information, coupled with the ratification of the African Union Convention on Cyber Security and Personal Data Protection (the **Malabo Convention**), may improve awareness of access to justice avenues.[43] Namibia is presently ranked as an "**evolving**" country in the International Telecommunication Union *Global Cybersecurity Index* (ITU Index) for 2024, "demonstrating a **basic cybersecurity commitment** to government-driven actions that encompass evaluating, establishing or implementing certain generally accepted cybersecurity measures".[44]

37 Namibia Statistics Agency website, accessible at: https://nsa.org.na/.

38 Ibid.

39 Datareportal website, "Digital 2023: Namibia", 2023, accessible at: https://datareportal.com/reports/digital-2023-namibia#:~:text=The%20state%20of%20digital%20in%20Namibia%20in%202023&text=There%20were%201.37%20million%20internet,percent%20of%20the%20total%20population.

40 Frederico Links, "Namibia's 'shambolic' poll leaves citizens shaken and traumatised to the core", Daily Maverick, 2024, accessible at: https://www.dailymaverick.co.za/article/2024-12-11-namibia-poll-leaves-citizens-shaken-traumatised-to-the-core/; Nyasha Nyaungwa, "Namibia's top court dismisses opposition election challenge", Reuters, 2025, accessible at: https://www.reuters.com/world/africa/namibias-top-court-dismisses-opposition-election-challenge-2025-02-28/.

41 African Declaration on Internet Rights and Freedoms Coalition, "The struggle for the realisation of the right to freedom of expression in Southern Africa", 2020, accessible at: https://ippr.org.na/wp-content/uploads/2021/02/Report20201203.pdf.

42 Freedom House website, "Namibia", 2024, accessible at: https://freedomhouse.org/country/namibia/freedom-world/2024.

43 COE website, "Octopus Cybercrime Community: Namibia", accessible at: https://www.coe.int/en/web/octopus/-/namibia; Datareportal website, "Digital 2023: Namibia"; Data Protection Africa website, "Namibia", accessible at: https://dataprotection.africa/namibia/.

44 ITU, "Global Cybersecurity Index 2024, 5th Edition", 2024, accessible at: https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf.

Sierra Leone

Sierra Leone, with a population of 9 million, has low economic growth and a significant portion of the population living below the poverty line.[45] The country faces widespread corruption,[46] inadequate infrastructure and high unemployment rates.[47] Sierra Leona has an Internet penetration rate of 30.4 per cent.[48] Freedom House records that while Sierra Leone is on an upward democratic trajectory, there appear to be challenges regarding political rights and civil liberties.[49] The country struggles with issues related to freedom of expression and press, with some restrictions on media operations.[50] However, the adoption of domestic laws and recent policy developments on cybercrime reflect a growing political will to address the increasing challenges relating to cybercrimes. Sierra Leone ranks higher in the ITU Index than Namibia, categorized as "establishing" with stronger indicators of cybersecurity commitment.[51] Unfortunately, concerns about judicial independence and inadequate court resources pose significant challenges to accessing justice.[52]

South Africa

South Africa has a population of 63.02 million people,[53] and currently has the largest economy in Africa. However, it continues to face high levels of unemployment and inequality.[54] It has an Internet penetration rate of 74.7 per cent.[55] South Africa's government does not impose restrictions on Internet access or social media. In 2024, for the first time in its democratic history, South African elections did not

45 World Bank Group website, "The World Bank in Sierra Leone", 2024, accessible at: https://www.worldbank.org/en/country/sierraleone/overview; United Nations Population Fund, "World Population Dashboard: Sierra Leone", 2024, accessible at: https://www.unfpa.org/data/world-population/SL.

46 Freedom House website, "Sierra Leone", 2024, accessible at: https://freedomhouse.org/country/sierra-leone/freedom-world/2024; Transparency International, "Overview of corruption and anti-corruption in Sierra Leone", 2023, accessible at: https://knowledgehub.transparency.org/helpdesk/overview-of-corruption-and-anti-corruption-in-sierra-leone-1.

47 Bertelsmann Stiftung's Transformation Index, "Sierra Leone Country Report", 2024, accessible at: https://bti-project.org/fileadmin/api/content/en/downloads/reports/country_report_2024_SLE.pdf; ISS African Futures, "Sierra Leone", 2024, accessible at: https://futures.issafrica.org/geographic/countries/sierra-leone/.

48 Datareportal website, "Digital 2024: Sierra Leone", 2024, accessible at: https://datareportal.com/reports/digital-2024-sierra-leone#:~:text=There%20were%202.70%20million%20internet,percent%20of%20the%20total%20population.

49 Freedom House website, "Sierra Leone".

50 Ibid.

51 ITU, "Global Cybersecurity Index 2024, 5th Edition".

52 COE website, "Octopus Cybercrime Community: Namibia"; Datareportal website, "Digital 2024: Sierra Leone"; Freedom House website, "Sierra Leone"; Data Protection Africa website, "Sierra Leone", accessible at: https://dataprotection.africa/sierra-leone/.

53 Statistics South Africa, Republic of South Africa, "2024 Mid-year population estimates", 2024, accessible at: https://www.statssa.gov.za/?p=17440#:~:text=South%20Africa's%20mid%2Dyear%20population,by%20Statistics%20South%20Africa%20today.

54 Statista website, "Socioeconomic Indicators – South Africa", 2024, accessible at: https://www.statista.com/outlook/co/socioeconomic-indicators/south-africa#:~:text=The%20gini%20coefficient%20in%20South,to%208.41m%20in%202024; Freedom House website, "South Africa", 2024, accessible at: https://freedomhouse.org/country/south-africa/freedom-world/2024.

55 Datareportal website, "Digital 2024: South Africa", 2024, accessible at: https://datareportal.com/reports/digital-2024southafrica#:~:text=South%20Africa's%20internet%20penetration%20rate,January%202023%20and%20January%202024.

result in an outright majority. This development has led to the formulation of the Government of National Unity,[56] a coalition government consisting of 11 political parties.[57] While it is too early to accurately judge the coalition's performance, Freedom House notes concerns about the lingering effects of the corruption characterized by previous administrations.[58] South Africa has a comprehensive legislative framework against cybercrimes, and having signed the Malabo Convention, the legal landscape and relatively strong judiciary suggest a potentially enabling environment. However, it appears that cybercrimes are on the rise and preliminary research indicates that significant challenges persist, particularly for victims and notably regarding online GBV.[59] In this study, South Africa ranks the highest on the ITU Index as an "**advancing**" country demonstrating "a **strong cybersecurity commitment** to coordinated and government-driven actions that encompass evaluating, establishing or implementing certain generally accepted cybersecurity measures".[60]

Uganda

Uganda has a population of 49.9 million people[61] and has seen positive economic growth in recent years, with its per capita GDP almost reaching lower-middle income status. However, much of the population lives in conditions of material deprivation. The country experiences high poverty levels, with income and wealth inequality on the rise.[62] Internet penetration is an area of concern, with Uganda having a low rate of 27 per cent.[63] In recent years, the civic and political space in Uganda has shrunk due to the implementation of strict laws, the suppression of opposition voices and attacks on independent civil society organizations.[64] According to Freedom House, journalists face intimidation for criticizing authorities, particularly in election years. This severely impacts freedom of expression and the right to access information

56 South African Government News Agency, "GNU: A new era for SA", 2024, accessible at: https://www.sanews.gov.za/features-south-africa/gnu-new-era-sa.

57 Ibid.

58 Freedom House website, "South Africa".

59 Data Protection Africa website, "South Africa", accessible at: https://dataprotection.africa/south-africa/; COE website, "Octopus Cybercrime Community: South Africa", accessible at: https://www.coe.int/en/web/octopus/-/south-africa; Datareportal website, "Digital 2024: South Africa"; Paradigm Initiative, "Digital Rights and Inclusion in Africa Report", 2023, accessible at: https://paradigmhq.org/wp-content/uploads/2024/04/Londa-2023-1-1.pdf; Media Defence, "Violence Against Women Journalists in Sub-Saharan Africa", 2024, accessible at: https://www.mediadefence.org/ereader/wp-content/uploads/sites/2/2024/06/Module-1-Violence-against-women-journalists-in-SSA-2024.pdf; Media Defence, "Digital Attacks and Online Gender-based Violence".

60 ITU, "Global Cybersecurity Index 2024, 5th Edition".

61 United Nations Population Fund website, "World Population Dashboard: Uganda", 2024, accessible at: https://www.unfpa.org/data/world-population/UG.

62 Bertelsmann Stiftung's Transformation Index, "Uganda Country Report 2024", accessible at: https://bti-project.org/en/reports/country-report/UGA.

63 Datareportal website, "Digital 2024: Uganda", accessible at: https://datareportal.com/reports/digital-2024-uganda#:~:text=There%20were%2013.30%20million%20internet%20users%20in%20Uganda%20in%20January,January%202023%20and%20January%202024.

64 Bertelsmann Stiftung's Transformation Index, "Uganda Country Report 2024".

in the country.[65] Further, there are instances of the government blocking certain social media platforms and regularly cutting off access to the Internet, particularly during election periods.[66] Concerns persist over judicial independence and resource restraints, both of which significantly hinder access to justice for cybercrime victims, and especially within the context of rising online GBV.[67] Uganda's existing cybercrime legislation has been critiqued as outdated and limited in scope, and it is not a signatory of the Malabo Convention. However, a new national cybersecurity strategy has been introduced and the government appears to be interested in engaging on questions of cybercrimes.[68] Similarly to Sierra Leone, Uganda is ranked as an "**establishing**" country in the ITU Index.[69]

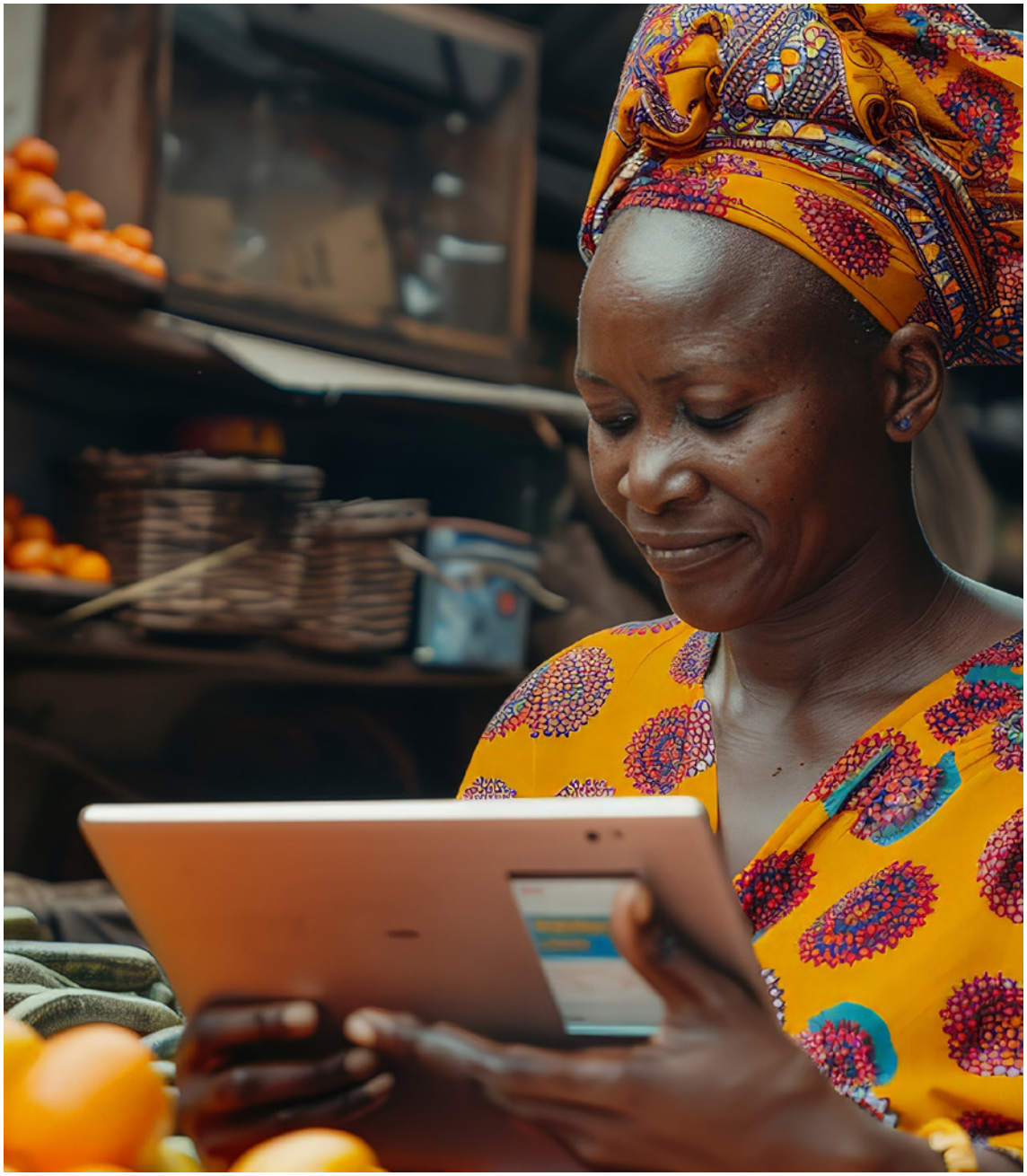
65 Freedom House website, "Uganda", 2024, accessible at: https://freedomhouse.org/country/uganda/freedom-world/2024.

66 Freedom House website, "Freedom on the Net 2023: Uganda", 2023, accessible at: https://freedomhouse.org/country/uganda/freedom-net/2023.

67 Kakande and others, "Amplified Abuse: Report on Online Violence Against Women in the 2021 Uganda General Election", Pollicy, 2021, accessible at: https://pollicy.org/wp-content/uploads/2022/08/Amplified-Abuse-Report-on-online-violence-Against-women-in-the-2021-general-elections.pdf; Media Defence, "Violence Against Women Journalists"; Media Defence, "Digital attacks and Online Gender-Based Violence'".

68 Republic of Uganda, "National Cybersecurity Strategy", 2022, accessible at: https://ega.ee/wp-content/uploads/2022/08/Ugandan-national-cybersecurity-strategy.pdf; COE website, "Octopus Cybercrime Community: Uganda", accessible at: https://www.coe.int/en/web/octopus/-/ugan-1; Datareportal website, "Digital 2024: Uganda", 2024, accessible at: https://datareportal.com/reports/digital-2024-uganda; Freedom House website, "Uganda"; Data Protection Africa website, "Uganda", accessible at: https://dataprotection.africa/uganda/.

69 ITU, "Global Cybersecurity Index 2024, 5th Edition".



“From advanced legislative frameworks to fragile civic spaces, the selected countries reflect the complex realities of building digital justice across Africa.”

PREVALENCE OF CYBERCRIME

Regional overview

Cybercrime is surging across Africa, emerging as one of the continent's most pressing and fast-evolving threats. The African cybercrime landscape remains highly dynamic, with attacks rapidly increasing in sophistication and scale.[70] It ranks as the continent with the highest cybersecurity exposure score per country, with 75 per cent of nations in the "high" or "very high" exposure categories.[71] In a review of four cybersecurity indexes[72] across 193 countries and spanning five geographical regions, **Africa is recorded as having the highest exposure to cyberthreats**.[73] Compromised critical infrastructure, ransomware and business email compromise are among the common cyberthreats directed at governments and businesses across the continent.[74]

At the individual level, cybercriminals have increasingly targeted victims in Africa through online scams, leveraging email, social media and messaging platforms as key entry points. Phishing attacks, sextortion, mobile money and financial scams appear to be prominent methods.[75] During Operation Serengeti—a two-month joint operation between INTERPOL and AFRIPOL—more than 35,000 victims of cybercrimes were identified across 19 countries.[76]

Key trends at the domestic level

Limited data and underreporting

Before highlighting trends in common cybercrimes, it should be noted that limited data collection and regular underreporting make it difficult to assess the prevalence of cybercrimes accurately.

Lack of data

Three out of the four select countries—Namibia, Sierra Leone and South Africa—do not appear to have official statistics relating to cybercrimes. The dearth of official

70 INTERPOL, "African Cyberthreat Assessment Report"; Access Partnership and the Centre for Human Rights, "Elevating Africa's Cyber Resilience: Unveiling Regional Challenges and Charting AI Solutions", 2024, accessible at: https://www.chr.up.ac.za/images/researchunits/dgdr/documents/resources/Cisco-AP-UP_Elevating-Africas-Cyber-Resilience.pdf.

71 Yijie Weng, Jianhao Wu, "Fortifying the Global Data Fortress: A Multidimensional Examination of Cyber Security Indexes and Data Protection Measures across 193 Nations", International Journal of Frontiers in Engineering Technology, 2024, accessible at: https://francis-press.com/papers/15225.

72 This study reviewed four prominent indices: the Cybersecurity Exposure Index, Global Cyber Security Index, National Cyber Security Index, and Digital Development Level.

73 Weng, Wu, "Fortifying the Global Data Fortress".

74 INTERPOL, "African Cyberthreat Assessment Report".

75 Ibid.

76 INTERPOL website, "Empowering law enforcement and partners to disrupt cybercrime networks", 2024, accessible at: https://www.interpol.int/en/News-and-Events/News/2024/Major-cybercrime-operation-nets-1-006-suspects.

statistics stems from a lack of enabling legislation, or challenges in implementing it when it does exist.

Namibia's lack of enabling legislation is the primary cause of its absence of statistics. Despite indications that there were 2.7 million instances of cybercrime in 2022 in Namibia,[77] there is no verifiable data to support this. Further, this figure does not align with Namibia's general trends of reported criminal cases, given that in 2021/22 reported criminal cases totaled 98,640,[78] rising to 110,551 in the 2023/24 financial year.[79] The Head of the Cybercrimes Unit at the Namibian Police Force (NamPol) explained that the lack of enabling legislation led to cybercrimes being categorized with more traditional crimes, making accurate data collection difficult.[80] For example, financial cybercrimes appear to fall under categories relating to fraud or theft and certain personal crimes such as NCII would likely fall under domestic violence. There are additional data capturing challenges regarding online child sexual exploitation and abuse: only one case was recorded in national statistics for 2017–2019 despite law enforcement officials from the Gender-Based Violence Protection Units and Cybercrime Unit reporting awareness of others.[81] MICT noted similar challenges with data collection.[82]

Sierra Leone, despite having enabling legislation and annual reporting on cybersecurity efforts by the Sierra Leone Police (SLP), does not have formalized and publicly accessible cybercrime data.[83] There is also no centralized system that captures data on reported cybercrimes, making it difficult for both the SLP and Sierra Leone's National Cybersecurity Coordination Center (NC3) to fully assess their prevalence.[84] Further, it is difficult to assess the exact number of reported cybercrimes as some are grouped under other categories of crime; for example, cyberfraud is grouped under economic offences.[85]

Similarly, **South Africa** does not have formalized data on cybercrimes. Additional challenges arise when members of the South African Police Service (SAPS) cannot categorize and code cybercrimes correctly.[86] However, this is anticipated to improve

77 Veripuami Kangumine, "Namibia experiences over two million cyber attacks per year", The Namibian, 2024, accessible at: https://www.namibian.com.na/namibia-experiences-over-two-million-cyber-attacks-per-year/#:~:text=Manifestos%202024,Namibia%20experiences%20over%20two%20million%20cyber%20attacks%20per%20year,Cybersecurity%20Conference%20underway%20in%20Windhoek.&text=The%20government%20says%202%2C7,attacks%20on%20a%20daily%20basis.

78 Future News Media, "Windhoek ranks 7th in Africa for high crime rates", 2024, accessible at: https://futuremedianews.com.na/2024/07/18/windhoek-ranks-7th-in-africa-for-high-crime-rates/.

79 Future News Media, "NamPol records over 110 000 criminal cases", 2024, accessible at: https://futuremedianews.com.na/2024/07/22/nampol-records-over-110-000-criminal-cases/.

80 Interview with Detective Chief Inspector Ratjindua Tjivikua, Head of Cybercrimes, NamPol, 9 October 2024.

81 ECPAT, INTERPOL, UNICEF, "Disrupting Harm in Namibia: Evidence on online child sexual exploitation and abuse", Global Partnership to End Violence Against Children, 2022, accessible at: https://safeonline.global/wp-content/uploads/2023/12/DH_Namibia_2_1.pdf.

82 Interview with staff at MICT, 9 October 2024.

83 Sierra Leone Police, "General Annual Crime Statistics Report: 2023", 2023, accessible at: http://www.police.gov.sl/wp-content/uploads/2024/02/Sierra-Leone-Police-Crime-Statistics-Report-2023.pdf.

84 Interviews with staff at NC3, 4–5 November 2024.

85 SLP, "General Annual Crime Statistics Report: 2023".

86 Ibid.

in the short to medium term. The Cybercrime Investigation Component of the Directorate for Priority Crime Investigation (DPIC) in South Africa explained that in addition to the cybercrimes legislation Standard Operating Procedures (SOPs), the SAPS has released new case codes for cybercrimes which should enable better categorization and data capture.[87]

Despite having the most accessible data on cybercrimes, **Uganda** has had problems categorizing certain offences when preparing a charge sheet. This leads to charges being made under the incorrect law, which can impact the investigation and management of the case.[88]

Underreporting

Underreporting of cybercrimes, caused by various social, economic and technical factors, was listed as a key challenge across all countries. Stakeholders observed that victims are ill-informed about online harms and cybercrime, and do not know their legal rights and the avenues available for seeking justice. Stigma and fears of re-victimization were also noted as key barriers in reporting.

Underreporting in **Namibia** is driven by a lack of knowledge; digital illiteracy; shame; perception of a lack of responsiveness from police; fears of re-victimization; and reputational considerations. LifeLine/ChildLine Namibia explained that people do not know their rights, and as a result are unaware they should report certain conduct to the police.[89] For children, the fear of reporting to an adult adds another layer of complexity. Although a digital reporting portal to address child sexual exploitation was launched in 2018 in partnership with the Internet Watch Foundation, uptake has been limited.[90] This has been attributed to low digital literacy rates, a lack of awareness about the portal and a limited understanding of how to use it.

Shame also plays a critical role in underreporting in Namibia. Interviews with MICT revealed that victims of scams often feel embarrassed and prefer to "move on" rather than inform the police.[91] Additionally, re-victimization concerns coupled with victim blaming are deterrents, particularly for those who have experienced intimate and personal harm.[92] Public perceptions that the police are unresponsive further exacerbate the issue. This perception may be reinforced by the absence of enabling legislation, which restricts the police's capacity to address cybercrimes effectively. From an economic perspective, underreporting is also tied to reputational concerns

87 Interview with staff at the Cybercrime Investigation Component, DPCI, 26 November 2024.

88 Interview with a non-governmental organization working on gender rights in Uganda, 23 October 2024.

89 Interview with a non-governmental organization working on children's rights in Namibia, 10 October 2024.

90 "IWF Namibia Reporting Portal", accessible at: https://report.iwf.org.uk/na/.

91 Interview with staff at MICT, 9 October 2024.

92 Interview with Detective Chief Inspector Ratjindua Tjivikua, Head of Cybercrimes, NamPol, 9 October 2024.

among financial institutions in Namibia. For example, banks may choose not to disclose data breaches or fraud cases to safeguard their public image.[93]

Sierra Leone faces challenges with underreporting of cybercrimes driven by stigma, lack of awareness and distrust in government institutions. The Cyber Investigation and Forensic Unit of the SLP highlights that stigma is particularly acute for crimes such as extortion.[94] Victims often feel ashamed or fear further exposure, leading many to choose to pay ransoms rather than report incidents to police. Their experience with cases involving child sexual abuse material has revealed that young victims, fearful of being identified or judged, are reluctant to come forward despite efforts by law enforcement to provide counselling and support.

A lack of knowledge about reporting mechanisms also contributes to underreporting. Although the Sierra Leone Cyber Security and Crime Act has been in place for several years, the police estimate that 70 per cent of people remain unaware of its provisions or where to report cybercrimes.[95] Confusion between the roles of the Cyber Investigation and Forensic Unit and the Sierra Leone Ministry of Communications and Cybersecurity further complicates matters, leaving victims uncertain about how to seek assistance.[96] Moreover, given the limited number of prosecutions, victims may feel that nothing will happen and do not make a report.[97]

In **South Africa**, the underreporting of cybercrimes is driven by multiple factors, including lack of awareness, systemic challenges in law enforcement, socio-economic divides and entrenched patriarchal norms. The Directorate for Priority Crime Investigation (DPCI) within SAPS has received feedback that many victims are reluctant to report cybercrimes due to unsatisfactory service from law enforcement when their primary concern—recovering financial losses—is often unmet.[98] Victims frequently encounter frustration at police stations, with officers dismissing unauthorized access to a device as non-criminal if no money is stolen. Compounding this issue is a low digital literacy rate, limited access to digital tools and the absence of clear, user-friendly reporting channels. For many, the legislative framework governing cybercrime is inaccessible and difficult to navigate, further discouraging engagement.[99]

93 Ibid.

94 Interview with staff at the Cyber Investigation and Forensic Unit, SLP, 4 November 2024.

95 Ibid

96 Interview with staff at the Sierra Leone Ministry of Communications and Cybersecurity, 4 November 2024.

97 Ibid.

98 Interview with staff at the Cybercrime Investigation Component, DPCI, 26 November 2024.

99 Ibid.

Anecdotal evidence suggests a stark rural-urban divide in reporting efficacy in South Africa. While urban areas may have some level of citizen awareness and capacity within law enforcement, in rural areas reporting is often ineffective or does not occur at all.[100] Socio-economic factors also play a significant role. Victims from middle-class backgrounds may only report incidents to fulfil insurance requirements, while those with fewer resources lack both the knowledge and motivation to engage with the criminal justice system.[101]

Gender dynamics add another layer of complexity. Women and girls, especially victims of sextortion or other gendered cybercrimes, face compounded barriers. For example, young teens subjected to sextortion may avoid reporting due to fear of humiliation or judgment, exacerbated by the lack of safe and confidential reporting mechanisms. Women who are harassed online have been met with dismissive responses, for example that it is "a fight with their boyfriend and not a serious issue".[102] Persisting patriarchal attitudes and cultural stigma around online harms further discourage women from coming forward. Physical spaces for reporting also fail to support victims' needs. Police stations often lack private, confidential environments, particularly in smaller or rural locations, which deters victims from disclosing personal or sensitive information.[103]

In **Uganda**, the underreporting of cybercrimes is primarily influenced by the nature of the crime and societal attitudes. As in other countries, stakeholders consistently identified two broad categories of cybercrimes: financial crimes and sexual crimes. These categories are treated differently by law enforcement in Uganda, with financial crimes receiving swift attention while sexual crimes are often deprioritized or dismissed entirely.[104] This disparity reflects broader societal attitudes, in which victim blaming in cases of online GBV and NCII is rampant.[105] Victims, particularly women, are often told it is their fault, asked why they took intimate photos or advised to "delete the pictures" or "just leave social media".[106] Such responses discourage reporting and deepen the stigma around these crimes, and may impact the available data on cybercrimes in Uganda.

100 Interview with cybercrime lawyer in South Africa, 20 November 2024.

101 Interview with digital rights activist in South Africa, 15 November 2024.

102 Interview with human rights lawyers in South Africa, 25 November 2024.

103 Ibid.

104 Interview with digital rights activist in Uganda, 23 October 2024.

105 Interview with women's rights lawyer in Uganda, 23 October 2024.

106 Interviews with digital rights activist and women's rights lawyers and activists in Uganda, 23–24 October 2024.

A lack of awareness compounds these challenges. Many victims do not perceive certain online harms as crimes or are unclear about where and how to report them. Cultural norms, especially for women, discourage speaking out: fears of judgment, reputational damage and long-term social consequences, such as being labeled "unmarriageable" for survivors of NCII, lead to silence.[107] This lack of support creates a harmful cycle: women see others silenced or ignored when they try to report and are further discouraged from coming forward.

Socio-economic considerations create additional barriers. The Ugandan police have observed that more educated members of society are more likely to report cybercrimes, while those with less education are often unaware that the conduct is a criminal offence.[108] Additionally, victims are often asked to pay the police to prompt an investigation. It appears that police request payment for transportation, data and printing, with an implicit understanding that payment is needed for investigations to ensue.[109] This can deter reporting, particularly among socio-economically marginalized groups.[110]

General trends

Notwithstanding data limitations and underreporting challenges, it is evident that cybercrimes are prevalent across the four countries. **Namibia** and **Sierra Leone** are experiencing an increase in cybercrime activity,[111] while **South Africa** ranks sixth globally for cybercrime density.[112] In 2024 **South Africa** was ranked as number 14 globally of countries worst affected by cybercrime.[113] In **Uganda**, although cybercrimes remain a significant concern, reported cases decreased from 286 in 2022 to 245 in the 2023/24 financial year, in part due to efforts by specialized task forces and building key stakeholders' capacity.[114] While there is limited centralized government or police data, a compilation of studies, reports, cases and insights from interviews with key stakeholders provides a general picture of cybercrimes in the respective countries, categorized into financial and personal harms.

107 Interview with women's rights lawyer in Uganda, 23–24 October 2024.

108 Interview with Inspector General of the Uganda Police Force (UPF), 24 October 2024.

109 Interviews with women's rights lawyers and activists in Uganda, 23–24 October 2024; FIDA-Uganda, "Study on the Adequacy of the Immediate State Response to Survivors of Sexual and Gender-Based Violence in Uganda in Ensuring Access to Justice", 2023, accessible at: https://fidauganda.or.ug/uploads/PISCCA_Immediate_State_Response_SGBV.pdf.

110 Interviews with women's rights lawyers and activists in Uganda, 23–24 October 2024.

111 Global Initiative Against Transnational Organised Crime, "Global Organised Crime Index: Namibia", 2023, accessible at: https://ocindex.net/assets/downloads/2023/english/ocindex_profile_namibia_2023.pdf; Mohamed Wurie Bah, "Sierra Leone's Cybersecurity Odyssey: Progress, Challenges and Future Paths", The Institute for Legal Research and Advocacy for Justice, 2023, accessible at: https://www.ilraj.org/publications/sierra-leones-cybersecurity-odyssey-progress-challenges-and-future-paths/.

112 News24, "CSIR collaborates with SAPS to strengthen cybercrime investigations", 2023, accessible at: https://www.news24.com/tech-and-trends/csir-collaborates-with-saps-to-strengthen-cybercrime-investigations-20230404.

113 University of Oxford website, "World-first "Cybercrime Index" ranks countries by cybercrime threat level", 2024, accessible at: https://www.ox.ac.uk/news/2024-04-10-world-first-cybercrime-index-ranks-countries-cybercrime-threat-level.

114 Financial Intelligence Authority, "Strengthening Cyber Safety and Ransomware Response", 2024, accessible at: https://www.fia.go.ug/strengthening-cyber-safety-and-ransomware-response.

Financial cybercrimes and online harms

Across the four countries, financial cybercrimes share common threads such as the widespread use of phishing, social engineering and impersonation tactics. Mobile money fraud is a significant issue in both Sierra Leone and Uganda, while Namibia and South Africa report growing concerns around digital banking fraud and cryptocurrency scams. Notably, **South Africa** stands out for the increasing sophistication of cybercrime methods, including the use of artificial intelligence, underscoring a divergence in the technological tools employed by cybercriminals.[115]

In **Namibia**, the perception of cyberthreats remains relatively low, contributing to a thriving environment for financial cybercrimes.[116] Common attacks include social engineering, phishing and identity theft.[117] A notable trend is the increasing number of cryptocurrency scams targeting bank clients.[118] Scammers also use platforms like WhatsApp and social media to impersonate trusted figures, such as bank managers, to solicit money.[119] Namibia has been active in combating these crimes, participating in INTERPOL's Operation First Light, which rescued 88 youths forced into scams and targeted phishing, investment fraud, fake shopping sites and impersonation scams.[120]

In **Sierra Leone**, phishing, online fraud and identity theft are widespread.[121] Scammers often exploit social media platforms to deceive individuals, leading to financial losses and identity theft.[122] Sierra Leone in particular appears to have challenges with social media takeovers where criminal actors unlawfully access an individual account and either use it to exploit the individual or to receive money from the individual's contacts.[123]

South Africa stands out for the sophistication and scale of its financial cybercrimes.[124] The country has seen a 45 per cent increase in digital banking fraud in 2023, with banking apps being a primary target.[125] Phishing and social engineering attempts

115 SEACOM, "What cyber threats are likely to entail in 2024", 2024, accessible at: https://seacom.co.za/news/what-cyber-threats-are-likely-to-entail-in-2024.

116 Elmarie Biermann, "A Digital Odyssey: The Convergence of Rapid Digitization, Population Dynamics, and Financial Risk in Namibia", Carnegie Endowment for International Peace, 2024, accessible at: https://carnegie-production-assets.s3.amazonaws.com/static/files/Biermann_Digital_Odyssey_Namibia.pdf.

117 Ibid.

118 Global Initiative Against Transnational Organised Crime, "Global Organised Crime Index: Namibia".

119 Interview with staff at MICT, 9 October 2024; Interview with senior academic in Namibia, 8 October 2024.

120 INTERPOL website, "Operation First Light highlights the extensive reach of scam syndicates", 2024, accessible at: https://www.interpol.int/News-and-Events/News/2024/USD-257-million-seized-in-global-police-crackdown-against-online-scams.

121 Interviews with staff at NC3, 4–5 November 2024; Interview with staff at the Cyber Investigation and Forensic Unit, SLP, 4 November 2024.

122 Interview with human rights lawyer in Sierra Leone, 5 November 2024.

123 Humphrina Pearce, Francis Turay, "The state of Cyber-Bullying in Sierra Leone: Where is the law?", SierraLii, 2023, accessible at: https://sierralii.gov.sl/articles/2023-12-08/Humphrina/the-state-of-cyber-bullying-in-sierra-leone-where-is-the-law.

124 The Banking Association South Africa, "SABRIC Reports Significant Increase in Financial Crime Losses for 2023", 2024, accessible at: https://www.banking.org.za/news/sabric-reports-significant-increase-in-financial-crime-losses-for-2023/.

125 Ibid.

remain common, but cybercriminals in South Africa have increasingly adopted advanced technologies including artificial intelligence, deepfakes and other tools to enhance their attacks. Ransomware is another prominent threat, further highlighting the growing complexity of cybercrime in the country.[126] Notably, South African courts are increasingly faced with cases of cybercrime.[127] In one instance, a judge observed that cybercrimes are a persistent and growing threat, with cybercriminals using phishing and tactics to impersonate or deceive people, and noting the upward trend of business email compromise (BEC).[128]

In **Uganda**, financial cybercrimes predominantly take the form of electronic fraud and obtaining money by false pretenses.[129] In 2023 alone, the financial impact of recorded cybercrimes in Uganda amounted to over 1.5 billion Uganda shillings (approximately US$419,407), though only a fraction of the losses were recovered.[130] A significant concern is mobile money fraud, where criminals exploit the widespread use of mobile money platforms by sending fake payment notifications to deceive victims. The mobile money divisions of MTN Uganda and Airtel, widely used services providers in Uganda, appear to be common targets for cybercriminals;[131] MTN Uganda customers were only recently advised of a new phishing scam.[132] Other common crimes include fraudulent SIM card registrations, online impersonation and unauthorized database access.[133] In response to these concerns, MTN Uganda and the Ugandan Communications Commission launched awareness campaigns. They successfully addressed digital and financial fraud by raising public awareness of the safe use of ICTs, demonstrating the effectiveness of multi-sector collaboration and media engagement.[134]

126 Calif Sausalito, "Cybercrime In South Africa 2024: Deepfakes On The Rise", Cybercrime Magazine, 2024, accessible at: https://cybersecurityventures.com/cybercrime-in-south-africa-2024-deepfakes-on-the-rise/.

127 Southern Africa Legal Information Institute, "Movienet Networks (Pty) Ltd and Another v Motus Ford Culemborg and Others", ZAWCHC 231, 2024, accessible at: https://www.saflii.org/za/cases/ZAWCHC/2024/231.html.

128 Ibid.

129 Interview with staff at UPF, 24 October 2024.

130 Christopher Kiiza, "Shs1.5 Billion Lost In Cyber Attacks In 2023", Business Times Uganda, 2024, accessible at: https://businesstimesug.com/shs1-5-billion-lost-in-cyber-attacks-in-2023/.

131 Joseph Kato, "UCC Warns Public on Mobile Money Pin, ID Fraudsters, Uganda Radio Network, 2022, accessible at: https://www.ugandaradionetwork.net/story/ucc-warns-public-on-mobile-money-pin-id-fraudsters-1; Cynthia Arinda, "Tricks Used by Mobile Money Fraudsters in Uganda", Nexus Media Uganda, 2023, accessible at: https://nexusmedia.ug/tricks-used-by-mobile-money-fraudsters-in-uganda/.

132 Ibid.

133 Republic of Uganda, "National Cybersecurity Strategy".

134 Winnie Wambugu, "Mobile money fraud typologies and mitigation strategies", GSMA, 2024, accessible at: https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/wp-content/uploads/2024/05/Mobile-Money-Fraud-Typologies-and-Mitigation-Strategies-20.05.24.pdf.

Personal cybercrimes and online harms

As with financial harms, all four countries reported different types of personal harm ranging from harassment, cyberbullying and hate speech to sextortion, NCII and doxxing. While not all falling under criminal conduct in these jurisdictions, there are concerning increases illustrating the fast-growing nature of online harms and their repercussions for the offline lives of potential targets and victims.

Harassment and cyberbullying

Harassment and cyberbullying are widespread across Namibia, Sierra Leone, South Africa and Uganda, though the nature and context of these issues vary.

According to NamPol, online harassment and cyberbullying are on the rise in **Namibia**.[135] Similarly, **South Africa** experiences high levels of cyberbullying, cyberstalking and online harassment, often targeting women.[136] In **Sierra Leone**, cyberbullying is reported to have become a significant issue but no comprehensive national statistics are available.[137] However, anecdotal evidence and studies reveal its pervasiveness, particularly among women and girls. A Safe Sister Training study found that 64 per cent of women reported experiencing threats, harassment or violence online.[138] In **Uganda,** harassment is similarly prevalent.[139] Forms of harassment include body shaming, sextortion and the unsolicited sharing of explicit images. One respondent noted "it happens to everyone; I just open my email, and there's an unwanted sexually explicit image".[140]

Vulnerable and marginalized communities are at heightened risk of online harm. For example, members of the LGBTQI+ community are subjected to online violence and harassment. Indigenous persons are also often harassed online in **Namibia**.[141] In **South Africa,** online hate speech and harassment are also being used to incite others to engage in physical violence against foreign nationals.[142] A 2022 case in South Africa illustrated the often-intersectional dimensions of online harassment. Brought by the South African Human Rights Commission, it pertained to a series of social media messages that were argued to be "serious, demeaning and humiliating

135 Interview with Detective Chief Inspector Ratjindua Tjivikua, Head of Cybercrimes, NamPol, 9 October 2024.

136 Eileen Carter, "GBV at the click of a button: even online, misogyny is out of line", South African Human Rights Commission, 2023, accessible at: https://www.sahrc.org.za/index.php/sahrc-media/opinion-pieces/item/3499-opinion-gbv-at-the-click-of-a-button-even-online-misogyny-is-out-of-line.

137 Interview with human rights lawyer in Sierra Leone, 5 November 2024.

138 Pearce, Turay, "The state of cyber-bullying in Sierra Leone".

139 Interviews with digital rights activist and women's rights lawyers and activists in Uganda, 23–24 October 2024.

140 Interviews with digital rights activist and women's rights lawyers and activists in Uganda, 23–24 October 2024.

141 Internet Society, Collaboration on International ICT Policy for East and Southern Africa, "Online Violence Against Women and Girls in Namibia", 2022, accessible at: https://isocnamibia.org/wp-content/uploads/2022/05/Ovaw-Digital.pdf.

142 Global Witness, " 'We need to kill them': Xenophobic hate speech approved by Facebook, TikTok and YouTube", 2023, accessible at: https://globalwitness.org/en/campaigns/digital-threats/we-need-to-kill-them-xenophobic-hate-speech-approved-by-facebook-tiktok-and-youtube/.

comments against women, and black women in particular".[143] The South African Human Rights Commission further argued that the messages in question were also overtly manipulating online harms for financial gain.[144]

Online child sexual exploitation and abuse

Online child sexual exploitation and abuse is a growing concern across all four countries, with distinct patterns emerging. In **Namibia**, a *Disrupting Harm* survey found that 9 per cent of children aged 12–17 who used the Internet had experienced online sexual exploitation in the past year.[145] Reports also indicate increasing trends of sextortion and other forms of online violence against children. **South Africa** faces similar challenges.[146] According to *South African Kids Online*, over half of child participants had encountered sexual images online, and nearly 20 per cent had received unwanted sexual messages or been directed to explicit content.[147]In **Sierra Leone**, the African Committee of Experts on the Rights and Welfare of the Child has expressed concern over the rise of online child sexual exploitation.[148] Although exact data is limited, stakeholders agree on the increasing prevalence of this issue. **Uganda** has also seen a rise in child sexual exploitation, particularly after the COVID-19 pandemic as more children are now online. Without sufficient guidance, children are vulnerable to manipulation by perpetrators posing as friends or allies online.[149]

Non-consensual sharing of intimate images (NCII)

The issue of NCII is becoming increasingly concerning across the four countries, albeit with varying degrees of recognition and response. **Namibia** has reported a rise in NCII and sextortion cases over the past decade, highlighting the evolving nature of online harms.[150] In **Sierra Leone**, police have reported fewer than 10 NCII cases in recent years.[151] However, the country has witnessed a troubling spate of "sex tapes", which often result in public humiliation and victim blaming.[152] That said,

143 Powerlaw Africa, "Mavhidula (on behalf of the South African Human Rights Commission) v Matumba (1/2020)", 2022, accessible at https://powerlaw.africa/2022/03/16/south-african-human-rights-commission-v-matumba/.

144 Interview with media and digital rights activist (also the representative of the *amicus curiae* in the case), 25 November 2024.

145 ECPAT, INTERPOL, UNICEF, "Disrupting Harm in Namibia".

146 Media Monitoring Africa, "Children's Rights Online: Towards A Digital Rights Charter", 2020, accessible at: https://media-monitoringafrica.org/wordpress22/wp-content/uploads/2020/11/1.pdf.

147 Burton and others, "South African Kids Online: A glimpse into children's internet use and online activities", The Centre for Justice and Crime Prevention, 2016, accessible at: http://globalkidsonline.net/wp-content/uploads/2016/06/South-Africa-Kids-Online-Report.pdf.

148 African Committee of Experts on the Rights and Welfare of the Child, "Sierra Leone: Follow-up mission", 2023, accessible at: https://www.acerwc.africa/en/article/press-release/press-release-sierra-leone-mission.

149 Interview with a non-governmental organization working on gender rights in Uganda, 23 October 2024.

150 Interview with Detective Chief Inspector Ratjindua Tjivikua, Head of Cybercrimes, NamPol, 9 October 2024; Interview with gender and digital rights activist in Namibia, 8 October 2024.

151 Interview with staff at the Cyber Investigation and Forensic Unit, SLP, 4 November 2024.

152 Wallace Abdul Faley, "The Law on Pornography and Indecent Material in Sierra Leone: An Investigation into Victims' Rights", 2022, accessible at: https://ssrn.com/abstract=4219154.

there has been a successful criminal conviction for making and sharing a sexually explicit video without consent, which may act as a deterrent for these types of personal harm.[153]

In **South Africa**, the landmark 2024 case *KS v AM* marked the first successful claim for damages related to NCII, setting a legal precedent for survivors.[154] The High Court awarded 3.5 million South African rand (approximately $185,000) in damages to the victim for online harms, including the creation of an imposter social media profile and acts of NCII. It also held that the conduct violated the victim's personality, identity, dignity, privacy and reputation.

Uganda has also grappled with NCII, illustrated by the high-profile case of a female pop singer whose intimate images were shared by a former partner.[155] The backlash against the victim included public vilification and calls for her prosecution, showcasing a deeply entrenched victim-blaming culture. Unfortunately, this is not an isolated incident. Over the past five years, at least eight prominent Ugandan celebrities—including Judith Heard, Fabiola Anita, Martha Kay, Cindy Sanyu, Sanyu Robina Mweruka, Desire Luzinda, Zari Hassan and Maama Fina—have fallen victim to NCII. These incidents are often attributed to ex-boyfriends or individuals seeking to blackmail the victims for financial gain.[156]

Attacks against journalists and human rights defenders

Digital attacks against journalists are on the rise across Africa, with a disturbing trend of targeting women journalists in particular.[157] These attacks often manifest as online GBV, hate speech, doxxing and online harassment, aimed at silencing their voices and undermining press freedom.[158] Although the specific forms and impacts vary across countries, commonalities include the use of online platforms to victimize journalists, often driven by political, societal or gender biases.

153 Abdul Rashid Thomas, "Sierra Leone High Court Judge sentences man to 5 years imprisonment for recording and circulating sexual video", The Sierra Leone Telegraph, 2021, accessible at: https://www.thesierraleonetelegraph.com/sierra-leone-high-court-judge-sentences-man-to-5-years-imprisonment-for-making-and-circulating-sexual-video/?utm_source=chatgpt.com.

154 Republic of South Africa, "KS v AM and SHM", Case No. 2021/28121, 2024, accessible at: https://powerlaw.africa/wp-content/uploads/2024/11/0001-Judgement-KS-v-AM-_28121-of-2021-2024-11-12.pdf.

155 Sarai Chisala-Tempelhoff, Monica Twesiime Kirya, "Gender, law and revenge porn in Sub-Saharan Africa: a review of Malawi and Uganda", Palgrave Communications, 2016, accessible at: https://www.nature.com/articles/palcomms201669.pdf.

156 APC, Wougnet, "Bridging the Digital Gender Gap in Uganda: An Assessment of Women's Rights Online Based on the Principles of the African Declaration of Internet Rights and Freedoms', 2020, accessible at: https://africaninternetrights.org/sites/default/files/Bridging-the-Digital-Gender-Gap-in-Uganda-WOUGNET.pdf.

157 Media Defence, "Digital Attacks and Online Gender-based Violence".

158 S'lindile Khumalo, Murray Hunter, "Londa 2023 Digital Rights and Inclusion in Africa Report: South Africa", Paradigm Initiative, 2023, accessible at: https://paradigmhq.org/wp-content/uploads/2024/06/South-Africa-Country-Report.pdf; Sandra Aceng, "Londa 2023 Digital Rights and Inclusion in Africa Report : Uganda", Paradigm Initiative, 2023, accessible at: https://paradigmhq.org/wp-content/uploads/2024/06/Uganda-Country-Report.pdf.

In **Namibia**, online safety for women has become increasingly challenging, especially for women human rights defenders and journalists.[159] In particular, these women face online harassment, online hate speech and disinformation attacks[160] linked to their gender and profession, contributing to self-censorship and withdrawal from public spaces. Social media platforms—particularly Facebook—have become hotbeds for victimization, including the spread of disinformation targeting prominent figures and journalists.[161] Prominent Namibian public figure Beate Sekerete, also known as Betty Davis, ended up having to claim civil damages for derogatory insults shared about her on a WhatsApp group.[162]

South Africa mirrors these challenges, with persistent efforts to silence journalists, particularly women, through hate speech, doxxing and harassment.[163] NGOs have documented cases where journalists are targeted by police, political parties and the public.[164] Prominent cases, such as journalist Ferial Haffajee's experience with manipulated sexualized images, highlight the growing use of technology to discredit and demean.[165] Similarly, Qaanitah Hunter faced baseless accusations and vitriol from political figures on the social media platform X.[166] The *Brown v Economic Freedom Fighters* case exemplifies the extremity of such attacks.[167] In 2019, a political leader publicly shared journalist Karima Brown's personal phone number, leading to a torrent of abuse including graphic messages with racial and gendered violence as well as death threats. In another case, a South African human rights defender obtained a protection order after facing a series of harassing and threatening social media posts targeting her and her family due to her professional work.[168]

In **Uganda**, women journalists are frequently subjected to online harassment and violence, especially those covering political topics. A recent study on online GBV revealed that these attacks often deter women from engaging fully in their

159 Nashilongo Gervasius, "Londa 2023 Digital Rights and Inclusion in Africa Report: Namibia", Paradigm Initiative, 2023, accessible at: https://paradigmhq.org/wp-content/uploads/2024/06/Namibia-Country-Report.pdf.

160 Ibid.

161 Itai Zviyita, Admire Mare, "Same threats, different platforms? Female journalists' experiences of online gender-based violence in selected newsrooms in Namibia", Journalism 25 (4): 779–799, 2023, accessible at: https://journals.sagepub.com/doi/epub/10.1177/14648849231183815.

162 Centre for Human Rights, University of Pretoria, "Understanding Online Gender-based Violence in Southern Africa", 2022, accessible at: https://www.chr.up.ac.za/images/researchunits/dgdr/documents/resources/FINAL_v_Understanding_oGBV_in_Southern_Africa.pdf.

163 Reid and others, "The women journalists of South Africa's Daily Maverick: Sexualized, Silenced and Labeled Satan", International Center for Journalists, 2024, accessible at: https://www.icfj.org/sites/default/files/2024-05/ICFJ_BigData_SouthAfrica_DailyMaverick.pdf.

164 Amnesty International South Africa, Campaign for Free Expression, Committee to Protect Journalists, Media Monitoring Africa and the South African National Editors' Forum, "Submission for the 41st Session of the Universal Periodic Review Working Group", 2022, accessible at: https://amnesty.org.za/research/universal-periodic-review-freedom-of-expression/.

165 Ferial Haffajee, "Twitter and the rest of social media are a rising threat to media freedom — and I am part of their roadkill", Daily Maverick, 2019, accessible at: https://www.dailymaverick.co.za/article/2019-08-06-twitter-and-the-rest-of-social-media-are-a-rising-threat-to-media-freedom-and-i-am-part-of-their-roadkill/.

166 Media Defence, "Digital Attacks and Online Gender-based Violence".

167 Southern Africa Legal Information Institute, "Brown v Economic Freedom Fighters and Others, ZAGPJHC 166, 2019, accessible at: https://www.saflii.org/za/cases/ZAGPJHC/2019/166.html.

168 Takudzwa Pongweni, "Former Helen Suzman Foundation chief granted court order to halt cyberbully after ZEP challenges", Daily Maverick, 2024, accessible at: https://www.dailymaverick.co.za/article/2024-03-11-former-helen-suzman-foundation-chief-granted-court-order-to-halt-cyberbully-after-zep-challenges/.

profession.[169] The abuse includes vitriol on social media and targeted campaigns to undermine their credibility and professional standing.

Public-facing women, including journalists and human rights defenders, also face heightened risks of harassment and efforts to silence them online and offline in **Sierra Leone**.[170] A recent report found that 62 per cent of female civil society representatives and 50 per cent of female journalists surveyed had experienced online harassment.[171] These incidents reflect a broader pattern of using online platforms to intimidate and silence women in the public sphere.

The gender dynamics

As shown above, all four of the focus countries are experiencing a rise in the prevalence of cybercrime[172] that disproportionately affects women. Although relevant statistics are not always available, engagements with various stakeholders indicated that women experience higher levels of personal cybercrime like cyberstalking, online harassment and cyberbullying because of their gender.

There are many reasons for the disproportionate number of personal cybercrimes committed against women in the focus countries. However, each nation has certain characteristics in common that may be identified as the root causes for this.

All the focus countries' societies are patriarchal, whereby women do not enjoy equal rights and societal norms dictate that they should only fill certain roles. In **Uganda**, various cultural norms, beliefs, practices and attitudes hinder the position of women and girls in society. These norms manifest in different ways including, but not limited to:[173]

- imbalanced power relations between women and men in private and public spheres
- gender stereotyping and male bias
- widespread acceptance of violence as an appropriate method of resolving conflict in intimate relationships
- disparity in the amount and quality of education received by girls.

169 Gerald Walulya, Florence Namasinga Selnes, "'I Thought You Are Beautiful': Uganda Women Journalists' Tales of Mob Violence on Social Media", Digital Journalism 11 (10): 1962–81, 2023, accessible at: https://doi.org/10.1080/21670811.2023.2170899.

170 Sierra Leone Association of Women in Journalism, "Threats Against Public-Facing Women in Sierra Leone", 2022, accessible at: https://internews.org/wp-content/uploads/2022/12/SLAWIJ_Threats-Against-Public-Facing-Women-2022.pdf.

171 Ibid.

172 Media Defence, "Non-Consensual Sharing of Intimate Images", 2024, accessible at: https://www.mediadefence.org/ereader/publications/online-violence-against-journalists/module-2-digital-attacks-and-online-gbv/ncii/.

173 United Nations Development Programme (UNDP) Uganda Country Office, "Gender Equality Strategy 2022-2025", 2022, accessible at: https://www.undp.org/sites/g/files/zskgke326/files/2023-02/UNDP%20UGANDA%20Gender%20Equality%20Strategy%202022-2025.pdf.

These manifestations of patriarchal society are not unique to Uganda. **South Africa** has some of the highest rates of GBV in the world.[174] Further, recent studies have shown that women are 18 per cent less likely to participate in the labour market and 9 per cent more likely to be unemployed.[175] Although **Namibia** has made significant progress in achieving gender equality over the past decade, women still account for more than 70 per cent of those experiencing severe food insecurity in the country.[176] In **Sierra Leone**, only 28 per cent of girls in rural areas attend secondary school, and access to health care is critically constrained for women.[177] In patriarchal societies, there may be more backlash against women who are vocal about their rights, and this behaviour may occur intentionally or subconsciously. Those who wish to maintain the status quo may feel entitled to silence such women, particularly those who are public facing, putting them at a greater risk of cybercrime and online harms.

Further, patriarchal norms may affect women reporting cybercrimes. This is particularly the case when the exposure of the cybercrime in question may have an ostracizing effect on the victim, and NCII presents an illustrative example of this. Patriarchy dictates that women should not be overtly sexual in public spaces; women consensually taking intimate images of themselves contravenes this norm and, therefore, reporting an instance of NCII may result in the woman being shunned in their community.

The circumstances described above are exacerbated by the reality that women in all four focus countries have less access to the Internet and ICT infrastructure and are less digitally literate. This is particularly the case for women living in rural areas. In **South Africa**, women have less access to the Internet and digital financial services than men.[178] Similarly in **Uganda**, only 13 per cent of women use the Internet compared to approximately 24 per cent of men.[179] In **Namibia**, only 47 per cent of women have access to the Internet,[180] while in **Sierra Leone**, only 5.7 per cent of women are Internet users.[181] The digital gender divide is exacerbated by a

174 Lacey George, "Gender-Based Violence Against Women in South Africa", Ballard Brief, 2020, accessible at: https://ballardbrief.byu.edu/issue-briefs/gender-based-violence-against-women-in-south-africa.

175 Inclusive Society Institute, "Understanding gender inequality", 2023, accessible at: https://www.inclusivesociety.org.za/post/understanding-gender-inequality.

176 Kathryn Kendrick, "The Progress of Women's Rights in Namibia", The Borgen Project, 2023, accessible at: https://borgenproject.org/womens-rights-in-namibia/.

177 World Bank, "World Bank Country Gender Action Plan to Help Address Gender Inequalities in Sierra Leone", 2024, accessible at: https://www.worldbank.org/en/news/press-release/2024/10/03/world-bank-country-gender-action-plan-to-help-address-gender-inequalities-in-sierra-leone#:~:text=Sierra%20Leone%20has%20made%20steady,the%20Sub%2DSaharan%20Africa%20average.

178 Tinuade A Ojo, Kamogelo Segone, "Women are being squeezed out of the digital economy", Daily Maverick, 2022, accessible at: https://www.dailymaverick.co.za/opinionista/2022-03-07-women-are-being-squeezed-out-of-the-digital-economy/.

179 Yegnanew A. Shiferaw, "A spatial analysis of the digital gender gap in South Africa: Are there any fundamental differences?", Technological Forecasting and Social Change, vol. 24, 2024, accessible at: https://doi.org/10.1016/j.techfore.2024.123443.

180 DigWatch, "Women and the ICTs in Namibia", 2020, accessible at: https://dig.watch/updates/women-and-icts-namibia.

181 Media Foundation for West Africa, "Women's Rights Online in Sierra Leone: National Policy Gaps & Recommendations", 2024, accessible at: https://www.mfwa.org/wp-content/uploads/2024/02/Advocacy-Paper-on-Women-Rights-Online-reprot-in-Sierra-Leone-August-2023.pdf?form=MG0AV3.

lack of digital literacy educational opportunities and training for women.[182] In Sierra Leone, for example, women and girls have very limited digital literacy skills.[183] The combination of a lack of access to the Internet and technology and digital illiteracy makes women particularly vulnerable to cybercrime. Understanding online platforms and the risks that come with using them is crucial for women to be able to recognize signs of cybercrimes and prevent them from occurring. Women must have the necessary skills to be able to use the Internet safely and responsibly to decrease the risk of cybercrimes occurring.

182 A Ojo, Segone, "Women are being squeezed out of the digital economy".

183 DigWatch, "Women and the ICTs in Namibia".

CONDUCIVE LEGAL FRAMEWORKS

Conducive legal frameworks are important components of enabling access to justice. International and regional law play an important role in guiding domestic standards; equally, domestic frameworks serve as the practical avenues that lead victims to accessing justice. All four countries are at various stages of the legal efforts to respond to cybercrimes, but there are some barriers and bottlenecks that may hinder access to justice. Despite this, they are relatively well placed to engage in law reform to ensure more conducive legal frameworks and compliance with international human rights standards.

Ratification of international and regional instruments

All of the countries are party to the International Covenant on Civil and Political Rights,[184] Convention on the Elimination of All Forms of Discrimination against Women[185] and Convention on the Rights of the Child.[186] These treaties require states to ensure, among others, that no one shall be subjected to torture or cruel, inhuman or degrading treatment;[187] that everyone is equal before the law and gets equal protection of the law;[188] the elimination of discrimination against women;[189] and the protection and promotion the rights of the child.[190] The countries have a duty to uphold the interrelated and essential components of justice systems—justiciability, availability, accessibility, quality, the provision of remedies for victims and accountability—that guarantee access to justice.[191] It is also by now well accepted that "the same rights that apply offline apply online".[192] This applies to children, whose rights must be respected, protected and fulfilled in the digital environment.[193]

184 UN Treaty Body Database, "Ratification Status for CCPR - International Covenant on Civil and Political Rights", accessible at: https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Treaty.aspx?Treaty=CCPR&Lang=en.

185 UN Treaty Body Database, "Ratification Status for CEDAW - Convention on the Elimination of All Forms of Discrimination against Women", accessible at: https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Treaty.aspx?Treaty=CEDAW&Lang=en.

186 UN Treaty Body Database, "Ratification Status for CRC - Convention on the Rights of the Child", accessible at: https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Treaty.aspx?Treaty=CRC&Lang=en.

187 United Nations General Assembly "International Covenant on Civil and Political Rights", Resolution 2200A (XXI), article 7, 1966, accessible at: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

188 Ibid, article 26.

189 United Nations General Assembly, "Convention on the Elimination of All Forms of Discrimination against Women", Resolution 34/180, 1979, accessible at: https://www.ohchr.org/sites/default/files/cedaw.pdf.

190 United Nations General Assembly, "Convention on the Rights of the Child" Resolution 44/25, 1989, accessible at: https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child.

191 UN Committee on the Elimination of Discrimination against Women, "General recommendation No. 33 on women's access to justice", CEDAW/C/GC/33, 2015, accessible at: https://digitallibrary.un.org/record/807253?ln=en&v=pdf.

192 United Nations Human Rights Council, "Resolution adopted by the Human Rights Council on 13 July 2021 47/16: The promotion, protection and enjoyment of human rights on the Internet", A/HRC/RES/47/16, 2021, accessible at: https://digitallibrary.un.org/record/3937534?ln=en.

193 Committee on the Rights of the Child, "General comment No. 25 (2021) on children's rights in relation to the digital environment", 2021, accessible at: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC/C/GC/25&Lang=en.

At the regional level—and giving rise to similar obligations—all of the countries are party to the African Charter on Human and Peoples' Rights (**African Charter**);[194] the African Charter on the Rights and Welfare of the Child;[195] and the Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa (**Maputo Protocol**).[196]

When it comes to cybercrimes, the four countries have different regional and international legal commitments. **Sierra Leone**, **Namibia** and **South Africa** have ratified the Malabo Convention,[197] demonstrating commitment to addressing cybercrime and digital security. **Ugandan** civil society is calling on authorities to ratify the Malabo Convention to affirm the country's commitment to regional and international human rights obligations; establish a trustworthy digital environment; safeguard personal data; and combat cybercrime across the continent.[198] Among the four countries selected for this research, **South Africa** and **Sierra Leone** are the only parties to the Council of Europe Convention on Cybercrime (**Budapest Convention**).[199]

As a member of the Economic Community of West African States, Sierra Leone is also party to the Supplementary Act on Personal Data Protection[200] and the Directive on Fighting Cyber Crime within ECOWAS.[201] As a member of the Southern African Development Community (SADC), Namibia and South Africa are guided by the SADC Cyber Crime Model Law, which presently appears to be under review and modernization.[202] Uganda, as a part of the East African Community, is set to be guided by the Data Governance Policy Framework.[203] It appears the East African Community Legal Framework for Cyber Laws of 2008 remains in draft form.[204]

194 African Commission on Human and Peoples' Rights, "State Parties to the African Charter", accessible here: https://achpr.au.int/en/states.

195 African Committee of Experts on the Rights and Welfare of the Child, "Ratifications Table", accessible at: https://www.acerwc.africa/en/member-states/ratifications.

196 African Union, "List of Countries Which Have Signed, Ratified/Acceded to the Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa", 2023, accessible at: https://au.int/sites/default/files/treaties/37077-sl-PROTOCOL_TO_THE_AFRICAN_CHARTER_ON_HUMAN_AND_PEOPLES_RIGHTS_ON_THE_RIGHTS_OF_WOMEN_IN_AFRICA.pdf.

197 African Union, "List of Countries Which Have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection", 2023, accessible at: https://dataprotection.africa/wp-content/uploads/2305121.pdf.

198 Unwanted Witness, "Ratify the Malabo Convention, a call to Government of Uganda as we mark the Human Rights Day", 2019, accessible at: https://www.unwantedwitness.org/ratify-the-malabo-convention-a-call-to-government-of-uganda-as-we-mark-the-human-rights-day-2019/.

199 COE website, "Chart of signatures and ratifications of Treaty 185", accessible at: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185.

200 Economic Community of West African States, "Supplementary Act A/SA.1/01/10 on Personal Data Protection", 2010, accessible at: https://www.statewatch.org/media/documents/news/2013/mar/ecowas-dp-act.pdf.

201 Economic Community of West African States, "Directive C/DIR. 1/08/11 on Fighting Cyber Crime within ECOWAS", 2011, accessible at: https://ccdcoe.org/uploads/2018/10/ECOWAS-110819-FightingCybercrime.pdf.

202 SADC, "Review and Modernisation of the SADC Cyber Crime Model Law'", 2022, accessible at: https://www.sadc.int/procurement-opportunities/review-and-modernisation-sadc-cyber-crime-model-law.

203 East Africa Community, "EAC set to advance Data Governance and Protection with development of a regional Policy Framework", 2024, accessible at: https://www.eac.int/press-releases/3195-eac-set-to-advance-data-governance-and-protection-with-development-of-a-regional-policy-framework.

204 Edrine Wanyama, "Robust Data Protection Standards Could Spur Regional Economic Integration", Collaboration on International ICT Policy for East and Southern Africa, 2024, accessible at: https://cipesa.org/2024/03/robust-data-protection-standards-could-spur-regional-economic-integration/.

As noted above, in December 2024 the General Assembly of the United Nations adopted the United Nations Convention against Cybercrime.[205] The Convention seeks to provide tools that will enhance international cooperation, law enforcement and technical capacity relating to cybercrime.[206] Should the focus countries ratify this Convention, it is likely to have significant impacts on their international obligations, domestic legislation and measures related to cybercrime. The countries' engagement with the draft and final version of the Convention varied. **Namibia** was present in the final round of treaty negotiations and adoption and appeared supportive.[207] **South Africa** provided submissions at key moments.[208] **Sierra Leone** participated in a day-long debate on evolving cyberspace threats.[209] **Uganda's** participation was noted when it appeared to abstain from voting for the deletion of article 6(2) of the treaty, stating that "nothing in [the] Convention shall be interpreted as permitting suppression of human rights or fundamental freedoms, including the rights related to the freedoms of expression, conscience, opinion, religion or belief, peaceful assembly and association, in accordance and in a manner consistent with applicable international human rights law".[210] The Electronic Frontier Foundation suggests that the abstention of 26 Member States from voting for the deletion of article 6(2) represents a divergent position on a rights-based approach to cybercrimes.[211]

Before turning to the countries' respective domestic frameworks, it is necessary to understand how international and regional legal obligations are incorporated into national law. The domestication of international law varies across the respective countries. **Sierra Leone**, as a dualist system, requires that international agreements and treaties incorporated into national law have domestic effect.[212] **Namibia**'s legal system is characterized as predominantly monist, with certain dualist elements.[213] Namibia, guided by Article 144 of its Constitution, incorporates international agreements into domestic law automatically unless contradicted by the Constitution

205 United Nations General Assembly, "United Nations Convention against Cybercrime".

206 Ibid.

207 Frederico Links, "United Nations Cybercrime Treaty Enables Threatening State Intrusion", Intel Watch, 2024, accessible at: https://intelwatch.org.za/2024/09/11/op-ed-united-nations-cybercrime-treaty-enables-threatening-state-intrusion/.

208 "South Africa's Contribution on the Provisions on International Cooperation, Technical Assistance and Mechanism of Implementation and Final Provisions in Preparation for the 3rd Ad Hoc Meeting Scheduled to Take Place on 29 August to 9 September 2022, New York", accessible at: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_session/Documents/Submissions/South_Africa_AHC3.pdf.

209 United Nations website, "Digital Breakthroughs Must Serve Betterment of People, Planet, Speakers Tell Security Council during Day-Long Debate on Evolving Cyberspace Threats", 2024, accessible at: https://press.un.org/en/2024/sc15738.doc.htm.

210 United Nations General Assembly, "United Nations Convention against Cybercrime".

211 Katitza Rodriguez, "The UN General Assembly and the Fight Against the Cybercrime Treaty", Electronic Frontier Foundation, 2024, accessible at: https://www.eff.org/deeplinks/2024/08/un-general-assembly-and-fight-against-cybercrime-treaty.

212 United Nations website, "Submission of the Republic of Sierra Leone to the United Nations International Law Commission on the use of subsidiary means for the determination of rules of international law in the national courts of Sierra Leone", 2023, accessible at: https://legal.un.org/ilc/sessions/74/pdfs/english/sm_sierra_leone.pdf.

213 Dunia Zongwe, "Researching Namibian Law and the Namibian Legal System", NYU Global Law, 2013, accessible at: https://www.nyulawglobal.org/globalex/namibia1.html#:~:text=On%20balance%2C%20Namibia%20has%20largely,law%20to%20Acts%20of%20Parliament.

or an Act of Parliament.[214] **Uganda**, also a dualist state, theoretically requires treaties to be domesticated through enabling legislation before being relied upon in court.[215] However, in practice Ugandan judges increasingly refer to international human rights treaties even in the absence of implementing legislation.[216] **South Africa** adopts a hybrid approach: customary international law automatically forms part of domestic law unless inconsistent with the Constitution or legislation (monist approach), while treaties must generally be approved by Parliament and enacted into law unless self-executing or of a technical nature (dualist approach).[217]

Overview of domestic legal frameworks

In terms of domestic law, the countries all have legislation that addresses cybercrimes to varying degrees.

Namibia

The **Namibian Constitution** guarantees access to justice as a cornerstone of protecting fundamental rights and freedoms, ensuring administrative justice, resolving criminal charges and determining civil rights and obligations.[218] Article 5 of the Constitution affirms that these rights and freedoms are enforceable by the courts, while Article 25(2) specifically provides that any individual whose fundamental rights have been infringed or threatened has the right to approach a competent court for enforcement or protection.[219]

This is an important and necessary foundation for access to justice; however, in the context of cybercrimes exercising this fundamental right becomes challenging in the absence of dedicated legislation.[220] The **Cybercrime Bill** and the **Data Protection Bill** are in advanced stages of development, but their prolonged drafting processes have left the country without comprehensive legal tools to tackle cybercrimes effectively. The Cybercrime Bill has been under discussion for nearly a decade, with stakeholders citing thorough public participation processes, civil society concerns

214 Yvonne Dausab, "International law vis-à-vis municipal law: An appraisal of Article 144 of the Namibian Constitution from a human rights perspective", 2020, accessible at: https://www.kas.de/documents/252038/253252/dausab.pdf/eca5052a-cf12-2c7e-364a-677fa8ede39b#:~:text=What%20is%20the%20meaning%20of%20Article%20144%3F&text=%5Bu%5Dnless%20otherwise%20provided%20by,of%20the%20law%20of%20Namibia.

215 Jamil Ddamulira Mujuzi, "International human rights law and foreign case law in interpreting Constitutional rights: The Supreme Court of Uganda and the death penalty question", African Human Rights Law Journal, 2009 accessible at: https://www.ahrlj.up.ac.za/images/ahrlj/2009/ahrlj_vol9_no2_2009_jamil_d_mujuzi.pdf.

216 Ibid.

217 Southern African Legal Information Institute, "The Incorporation of Public International Law into Municipal Law and Regional Law against the Background of the Dichotomy between Monism and Dualism", PER 43, 2014, accessible at: https://www.saflii.org/za/journals/PER/2014/43.html.

218 Zoila Hinson, Dianne Hubbard, "Access to justice in Namibia: Proposals for Improving Public Access to Courts", Legal Assistance Centre, 2012, accessible at: https://www.lac.org.na/projects/grap/Pdf/access2justice1_human_right.pdf.

219 Permanent Mission of the Republic of Namibia to the United Nations, "The Constitution of The Republic of Namibia", accessible at: https://www.un.int/namibia/namibia/constitution.

220 Interview with Detective Chief Inspector Ratjindua Tjivikua, Head of Cybercrimes, NamPol, 9 October 2024.

and the death of a key legal drafter as reasons for the delays.[221] The absence of effective cybercrime laws continues to hinder access to justice, leaving victims of cybercrime and technology-facilitated abuse with limited legal recourse.[222]

The Cybercrime Bill aims to address key challenges by protecting critical data, safeguarding privacy and establishing mechanisms for the investigation of offences. It proposes the appointment of a computer security inspector and the creation of a team with defined powers to investigate cybercrimes, as well as the accreditation of security service providers.[223] However, a 2021 draft of the Bill received significant criticism from civil society for granting overly broad powers to officials without sufficient checks and balances.[224] Critics argued that these provisions infringed on the right to privacy and failed to include adequate safeguards against unjustified state surveillance.[225] Stakeholders now emphasize the importance of aligning the Bill with international human rights standards, including insights gained from Namibia's engagement with the United Nations Convention against Cybercrime.[226]

The Data Protection Bill, introduced for public comment in 2022, aims to regulate the processing of personal information and ensure the right to privacy.[227] However, this draft was also criticized for underdeveloped consent provisions and insufficient protections for data subjects.[228] The lack of a robust data protection framework is particularly concerning as it may increase vulnerability to specific types of cybercrime, further highlighting the urgent need for legislative reform. Namibia's 2019 **Electronic Transactions Act** criminalizes certain cybercrimes and includes some provisions to protect vulnerable groups from online GBV and cybercrimes against children.[229] However, it does not comprehensively address cybercrimes, provide viable avenues for justice or adequately address privacy and data security concerns[230]. Furthermore, the Act's scope is limited, and stakeholders argue that the lack of comprehensive cybercrime laws continues to impede access to justice.

221 Interview with Detective Chief Inspector Ratjindua Tjivikua, Head of Cybercrimes, NamPol, 9 October 2024; Interview with staff at MICT, 9 October 2024; See also Frederico Links, "Familiar Flaws – Unpacking Namibia's draft Cybercrime Bill", IPPR, 2022, accessible at: https://ippr.org.na/wp-content/uploads/2022/03/Familiar-Flaws-MHRC-Feb-2022-web-2.pdf.

222 Interview with Detective Chief Inspector Ratjindua Tjivikua, Head of Cybercrimes, NamPol, 9 October 2024.

223 Elmarie Biermann, "A Digital Odyssey".

224 Frederico Links, "United Nations Cybercrime Treaty Enables Threatening State Intrusion".

225 Frederico Links, "Rights watered down in draft privacy and data protection bill in Namibia", Southern Africa Digital Rights, 20–23, 2024, accessible at: https://www.apc.org/sites/default/files/digital_rights_southern_africa_ed2.pdf.

226 Interview with staff at MICT, 9 October 2024.

227 Parliament of the Republic of Namibia, "The Draft Data Protection Bill, 2021", accessible at: https://dataprotection.africa/wp-content/uploads/2022/09/Namibia_DPA-Bill.pdf; Digital Policy Alert, "Namibia: MICT opens public consultation on draft Data Protection Bill including data protection obligations", 2022, accessible at: https://digitalpolicyalert.org/event/7328-mict-opens-public-consultation-on-draft-data-protection-bill-including-data-protection-obligations.

228 Frederico Links, "United Nations Cybercrime Treaty Enables Threatening State Intrusion".

229 Republic of Namibia, "Electronic Transactions Act 4 of 2019", 2019, accessible at: https://www.lac.org.na/laws/annoSTAT/Electronic%20Transactions%20Act%204%20of%202019.pdf.

230 Namibia Media Trust, "Review of Namibia's National Cyber-security Strategy & Awareness Raising Plan 2022-2027", 2021, accessible at: https://www.nmt.africa/uploads/614346b1d2ebb/NMTsubmision-Reviewofnationalcybersecuritystrat(22-27).pdf.

In the interim, Namibia has relied on common law to prosecute cybercrimes such as fraud, but this approach has proven insufficient.[231] Prosecutors face challenges adapting traditional legal frameworks to address cybercrime and to "make something fit where it does not", leading to gaps in justice for victims.[232] The absence of specific legislation has left many, particularly women, journalists, the LGBTQI+ community and other marginalized groups without effective remedies for online harms, including GBV.[233] A digital rights activist described how victims "cannot go to court when the laws do not see this as real violence", leaving many without recourse.[234]

Some stakeholders noted that only high-profile cases, particularly financial cybercrimes, are taken seriously by the police. One individual shared her experience of falling victim to a banking scam, explaining that as an "ordinary person" she received no assistance while politicians and high-ranking officials did.[235] This inconsistent approach to cybercrime justice in Namibia leaves victims feeling unsupported and discouraged from reporting such crimes.

Namibia has taken some positive steps to address some of the challenges outlined above. This includes the launch of the **National Cybersecurity Strategy and Awareness Creation Plan 2022–2027** in March 2023, which aims to safeguard critical information infrastructure, educate Internet users and promote cybersecurity awareness.[236] However, without the finalized Cybercrime Bill Namibia lacks a cohesive legal framework to combat cybercrime effectively. While some stakeholders argue it is better to enact imperfect legislation than to wait indefinitely, others stress the importance of ensuring the Bill provides robust protections to prevent future challenges and rights violations.[237] This legislative vacuum highlights the urgency of passing effective cybercrime and data protection laws to ensure access to justice, protect victims and build a credible legal framework for Namibia's digital future.

231 Interview with Detective Chief Inspector Ratjindua Tjivikua, Head of Cybercrimes, NamPol, 9 October 2024.

232 Interview with Detective Chief Inspector Ratjindua Tjivikua, Head of Cybercrimes, NamPol, 9 October 2024.

233 Gaervasis, "Namibia: Londa Digital Rights and Inclusion Report".

234 Interview with gender and digital rights activist in Namibia, 8 October 2024.

235 Interview with senior academic in Namibia, 8 October 2024; Tracy Tafirenyika, "Minister Agnes Tjongarero loses N$711 200 to scam: Calls for improved cybersecurity measures", The Namibian, 2024, accessible at: https://www.namibian.com.na/minister-agnes-tjongarero-loses-n711-200-to-scam-calls-for-improved-cybersecurity-measures/.

236 Elmarie Biermann, "A Digital Odyssey".

237 Interview with Detective Chief Inspector Ratjindua Tjivikua, Head of Cybercrimes, NamPol, 9 October 2024; Interview with staff at MICT, 9 October 2024.

Sierra Leone

Sierra Leone's Constitution provides a foundation for the recognition and protection of human rights, including access to justice for all without discrimination and the right of all individuals to seek redress through the courts.[238] However, despite these constitutional guarantees there are still challenges due to financial barriers, lack of awareness about rights and systemic inefficiencies.[239] Fortunately, in recent years there have been clear efforts to improve access to justice, particularly in addressing violence against women and girls. For instance, the modernization of the Sexual Offences Model Court in Kailahun District, including solar-powered electricity and ICT facilities, enhances its capacity to serve victims of GBV.[240]

The main cybercrime legislation for Sierra Leone is the **Cybersecurity and Crime Act of 2021**.[241] Drafted to ensure alignment with international standards, including the Budapest Convention, the Act establishes a robust framework to combat cybercrime. It provides for, among others, the prevention of abusive use of computers; the collection of electronic evidence for the effective investigation and prosecution of cybercrime; and the safeguarding of critical national information infrastructure.[242] The Act criminalizes a wide range of both personal and financial cybercrimes. It is a robust legal framework designed to protect individuals, businesses and the state from various forms of cybercrime. It pays particular attention to protecting vulnerable groups. It includes specific measures to safeguard children, women and marginalized communities from cybercrimes.[243] Notable achievements include the establishment of the NC3, which coordinates cybersecurity initiatives and responds to cyber-attacks.[244]

Several stakeholders welcomed the Cybersecurity and Crime Act, noting that while there may be scope for improvement it is an important starting point.[245] Stakeholders further noted that the force and effect of the Act have not yet been fully and regularly tested, given that no cybercrime cases have been finalized through judicial processes.[246] As such, it is difficult to fully assess the utility of the law as an avenue for access to justice. It appears that some proactive steps have been taken to improve the implementation of the Act, including the establishment

238 Constitute Project, "Constitution of the Republic of Sierra Leone", 2008, accessible at: https://www.constituteproject.org/constitution/Sierra_Leone_2008.

239 Institute for Security Studies, "Access to justice: Sierra Leone - A country review of crime and criminal justice", 2009, accessible at: https://issafrica.org/research/monographs/sierra-leone-a-country-review-of-crime-and-criminal-justice-2008.

240 UNDP Sierra Leone, "UNDP Sierra Leone enhances access to justice and promotes human rights", 2024, accessible at: https://www.undp.org/sierra-leone/news/undp-sierra-leone-enhances-access-justice-and-promotes-human-rights.

241 Parliament of Sierra Leone, "Cybersecurity and Crime Act, 2021", 2021, accessible at: https://www.parliament.gov.sl/uploads/acts/THE%20CYBERSECURITY%20AND%20CRIME%20ACT,%202021%20-%20%2025TH%20NOVEMBER,%202021.pdf.

242 COE website, "Octopus Cybercrime Community: Sierra Leone", accessible at: https://www.coe.int/en/web/octopus/-/sierra-leone.

243 Ibid. at sections 47 and 48.

244 Bah, "Sierra Leone's Cybersecurity Odyssey".

245 Interviews with staff at NC3, 4–5 November 2024; Interview with Sierra Leone Financial Intelligence Unit, 5 November 2024.

246 Interviews with staff at NC3, 4–5 November 2024.

of a working group to develop SOPs, address warrant issuance and ensure proper chain-of-custody protocols for electronic evidence.

While the Act has been largely welcomed, some concerns have been raised. Critics argue that the legislation might infringe on freedoms of expression and press. For instance, the Sierra Leone Association of Journalists has emphasized the need to ensure that the law does not impede journalistic activities and the right to free speech.[247] Broad search and seizure powers under the Act, which allow law enforcement to extend searches to additional systems beyond the scope of the original warrant, have been flagged as problematic. There are concerns that these provisions could be misused against journalists, activists and political opponents, eroding gains made in repealing laws that restricted press freedom.[248] Furthermore, the lack of a clear definition for "electronic device" and insufficient safeguards for data protection highlight areas for improvement.

Following recent high-profile arrests, the potential for the Act to be applied in ways that may impact freedom of expression is an additional concern. In 2022, the Criminal Investigation Department announced an investigation into Ibrahim Kemoh Sesay, a former Minister of Transport and Aviation and prominent opposition figure. It was alleged he committed "cyberstalking and cyberbullying" offences after a video surfaced on WhatsApp containing purportedly "inciting and insulting messages" against President Julius Maada Bio.[249] Sesay, a well-known political figure and presidential aspirant, was remanded in custody, prompting discussions about the implications of the law for political discourse.[250] Similarly, a young lawyer named Joy Precious Bayoh was detained overnight by the Criminal Investigation Department following a post on the social media platform X, in which she questioned the legitimacy of President Bio. Authorities cited an ongoing investigation into "incitement and other cyber-related offences".[251] These incidents have sparked debate among civil society groups and media reform advocates, who caution that such applications of the law could have a broader impact on open political engagement and free expression.[252]

Critics argue that the Act is being wielded in ways reminiscent of the repealed criminal libel law, which was historically used to suppress dissent and undermine press freedom. The Media Reform Coordinating Group and other stakeholders have documented instances of the Act being applied against journalists, musicians

247 Jackson Mvunganyi, "Journalist: Sierra Leone Cyber Security law could infringe on press freedom", VOA, 2023, accessible at: https://www.voaafrica.com/a/sierra-leone-cyber-security-law-/7080676.html.

248 Media Foundation for West Africa, "How Sierra Leone is Hiding Behind the Fight Against Cybercrime to Abuse Digital Rights", 2021, accessible at: https://mfwa.org/how-sierra-leon-is-hiding-behind-the-fight-against-cybercrime-to-abuse-digital-rights/.

249 Abdul Rashid Thomas, "Opposition APC presidential aspirant Kemoh Sesay arrested for allegedly insulting president Bio", The Sierra Leone Telegraph, 2022, accessible at: https://www.thesierraleonetelegraph.com/opposition-apc-presidential-aspirant-kemoh-sesay-arrested-for-allegedly-insulting-president-bio/comment-page-1/.

250 Media Foundation for West Africa, "Sierra Leone's new Cybercrime Law begins to bite", 2022, accessible at: https://mfwa.org/country-highlights/sierra-leones-new-cybercrime-law-begins-to-bite/.

251 Alvin Lansana Kargbo, "Arrest Ignites Debate on Cyber Law and Free Speech in Sierra Leone", The Calabash Newspaper, 2024, accessible at: https://thecalabashnewspaper.com/arrest-ignites-debate-on-cyber-law-and-free-speech-in-sierra-leone/.

252 Ibid.

and ordinary citizens for online activities, effectively curbing dissent. They caution that while the Act aims to address legitimate cybercrimes, its vague provisions and broad enforcement powers risk undermining fundamental rights, including freedom of expression and political participation.[253] This misuse could erode public trust in the Act, compromise its intended purpose of promoting cybersecurity and hinder access to justice for genuine victims.

South Africa

South Africa's commitment to access to justice, enshrined in section 34 of its **Constitution**, ensures that everyone has the right to have legal disputes resolved through fair and impartial hearings.[254] The right of access to courts envisages that rights-bearers have access to remedies through the justice system.[255] This principle aligns with the equality guarantees in the Constitution, emphasizing that justice must be accessible to all, including victims of cybercrime.[256]

South Africa's legal framework for addressing cybercrimes is underpinned by the **Cybercrimes Act**. It criminalizes a wide range of cyber-related offences and outlines the powers of law enforcement to investigate, search and seize digital evidence.[257] Drafting the Cybercrimes Act involved extensive consultations with stakeholders, including law enforcement, the judiciary and private sector actors, reflecting a collaborative approach to enhancing access to justice in the digital realm.[258] It has laid the foundation for addressing both financial and personal forms of cybercrime.[259] The Act criminalizes offences including unlawful access; unlawful interception of data; unlawful acts regarding software or hardware tools; unlawful interference with data or computer programs; and cyberfraud.[260] The Act also criminalizes the disclosure of data messages of intimate images, where the intimate image violates or offends the sexual integrity or dignity of the person or amounts to sexual exploitation.[261]

The Act obliges the National Commissioner to establish or designate an office within SAPS as the Point of Contact for the country. This office must immediately assist proceedings or investigations into any of the listed cybercrime offences or

253 Ibid.

254 Republic of South Africa, "Constitution of the Republic of South Africa", 1996, accessible at: https://www.justice.gov.za/constitution/SAConstitution-web-eng.pdf.

255 Sanya Samanti, "International Law, Access to Courts and Non-Retrogression: Law Society v President of the Republic of South Africa", Constitutional Court Review, 2020, accessible at: https://www.saflii.org/za/journals/CCR/2020/8.pdf.

256 Mathias Nyenti, "Access to justice in the South African social security system".

257 Republic of South Africa, "Act No. 19 of 2020: Cybercrimes Act, 2020", 2021, accessible at: https://www.gov.za/sites/default/files/gcis_document/202106/44651gon324.pdf; Michalsons, "Cybercrimes Act in South Africa", 2024, accessible at: https://www.michalsons.com/focus-areas/cybercrime-law-around-the-world/cybercrimes-act-south-africa.

258 Interview with staff at the Cybercrime Investigation Component, DPCI, 26 November 2024.

259 Interview with staff at the Cybercrime Investigation Component, DPCI, 26 November 2024.

260 Republic of South Africa, "Act No. 19 of 2020", chapter 2.

261 Republic of South Africa, "Act No. 19 of 2020", section 11 and 16.

those deemed substantially similar.[262] To date, it does not appear that this Point of Contact has been established.[263] The Act also sets out obligations on electronic communications service providers and financial institutions to report cybercrime offences and to preserve any information that may help in an investigation.[264]

There have been some challenges with the practical implementation of the Cybercrimes Act. In 2022, South African courts set aside search and seizure warrants issued under the Cybercrimes Act due to procedural deficiencies, leading to the return of seized property.[265] There appears to have been swift responses to these challenges, with the 2023 **Standard Operating Procedures** for investigation, search, access and seizure marking an important step in efforts to advance the practical application of the Act.[266] Despite its strengths, the Cybercrimes Act has faced criticism. While the Act provides the technical tools needed to prosecute cybercrimes, its practical effectiveness remains limited. Additionally, victims often find the legislative framework challenging to navigate, and some sections of the Act are not user-friendly or fully operational.[267]

In addition to the Cybercrimes Act, South Africa has a suite of legislation that indirectly bolsters protections against cybercrime by addressing specific areas of concern. For example, the **Electronic Communications and Transactions Act** criminalizes offences such as computer-related extortion while limiting the liability of Internet service providers under certain conditions.[268] The **Protection of Personal Information Act** mandates secure processing of personal data, requiring notification in case of data breaches, thereby playing a preventive role in combating cybercrime.[269] The **Film and Publications Act** prohibits the distribution of private sexual photographs and films in any medium, including the Internet and social media, without the prior consent of the individual, and the distribution of child pornography under any circumstance.[270] The **Financial Intelligence Act** targets fraudulent activities, including cyber-related crimes, through strict record-

262 Republic of South Africa, "Act No. 19 of 2020", section 52.

263 Sizwe Snail ka Mtuze, Melody Musoni, "An overview of cybercrime law in South Africa" International Cybersecurity Law Review vol.4: 299–323, 2023, accessible at: https://link.springer.com/article/10.1365/s43439-023-00089-8.

264 Ibid. at chapter 8.

265 Southern Africa Legal Information Institute, "Buchler v Minister of SAPS N.O. and Others", ZAFSHC 1, 2023, accessible at: https://www.saflii.org/za/cases/ZAFSHC/2023/1.html.

266 Interview with staff at the Cybercrime Investigation Component, DPCI, 26 November 2024; SAPS, "Standard Operating Procedures in terms of Section 26 of the Cybercrimes Act, No 19 of 2020 for the Investigation, Search, Access or Seizure of Articles", 2023, accessible at: https://www.saps.gov.za/resource_centre/notices/downloads/SAPS-CCA-SOP-FINAL-12-09-2023.pdf.

267 Interview with staff at the Cybercrime Investigation Component, DPCI, 26 November 2024.

268 Republic of South Africa, "Electronic Communications and Transactions Act 25 of 2002", accessible at: https://www.gov.za/documents/electronic-communications-and-transactions-act.

269 Republic of South Africa, "Act No. 4 of 2013: Protection of Personal Information Act, 2013", 2012, accessible at: https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf.

270 Republic of South Africa, "Film and Publications Act 65 of 1996", accessible at: https://www.gov.za/documents/films-and-publications-act.

keeping obligations.[271] Additionally, the **Protection from Harassment Act**[272] and the **Domestic Violence Amendment Act**[273] cover both offline and online spaces, supporting vulnerable groups and addressing online harassment and online GBV.[274] Collectively, these laws complement the Cybercrimes Act by offering comprehensive protections, particularly for children and other vulnerable groups, through explicit and indirect safeguards against cyberthreats and personal online harms.

Uganda

Under Uganda's **Constitution**, any person whose rights or freedoms have been infringed or threatened has the right to seek redress in court, including compensation.[275] While the government has expressed its commitment to promoting access to justice and the rule of law, public confidence in the judiciary remains divided. According to a 2024 study, about 51 per cent of Ugandans feel somewhat or very confident in their ability to obtain justice; however, 45 per cent express little to no confidence, citing concerns about inequality and judicial decisions influenced by powerful interests rather than the fair application of the law.[276]

The **Computer Misuse (Amendment) Act 2022** serves as Uganda's primary cybercrime legislation.[277] It criminalizes unlawful access to and abuse and misuse of computers, targeting both financial and personal forms of cybercrime. The Act includes provisions to protect vulnerable groups, such as the prohibition of child pornography, online harassment and cyberstalking. However, concerns persist regarding its vagueness and susceptibility to abuse. Stakeholders have noted that while the Act provides some tools for addressing cybercrimes, its ambiguous language has allowed for selective enforcement that often targets journalists, human rights defenders and political activists.[278] Several stakeholders take the view that the Act disproportionately targets critics of the government while offering limited recourse for victims of cybercrime.[279] The Act also addresses hate speech, the dissemination of malicious or unsolicited information and the "misuse of social

271 Republic of South Africa, "Financial Intelligence Act 38 of 2001", accessible at: https://www.gov.za/documents/financial-intelligence-centre-act.

272 Republic of South Africa, "Protection from Harassment Act 17 of 2011", accessible at: https://www.gov.za/documents/acts/protection-harassment-act-17-2011-05-dec-2011.

273 Republic of South Africa, "Domestic Violence Amendment Act 14 of 2021, accessible at: https://www.gov.za/documents/acts/domestic-violence-amendment-act-14-2021-english-afrikaans-28-jan-2022.

274 Tina Power, "The DVA Act: one step closer to online safety", ALT Advisory, 2022, accessible at: https://altadvisory.africa/2022/02/22/the-dva-act-one-step-closer-to-online-safety/.

275 Uganda Legal Information Institute, "Constitution of the Republic of Uganda", 2018, accessible at: https://ulii.org/akn/ug/act/statute/1995/constitution/eng@2018-01-05#chp_Four__sec_50.

276 Afrobarometer, "Access to justice? As public trust in courts declines, many Ugandans have their doubts", 2024, accessible at: https://www.afrobarometer.org/wp-content/uploads/2024/07/AD821-Access-to-justice-Ugandans-have-their-doubts-Afrobarometer-11july24.pdf.

277 Republic of Uganda, "Computer Misuse (Amendment) Act", 2022, accessible at: https://chapterfouruganda.org/sites/default/files/downloads/The-Computer-Misuse-%28Amendment%29-Act-2022.pdf.

278 Interviews with women's rights lawyers and digital rights activists in Uganda, 23–24 October 2024.

279 Ibid.

media" as content-related cybercrimes, raising significant concerns about freedom of expression.[280]

The United Nations Working Group on Arbitrary Detention found that the arrest and detention of Stella Nyanzi, a Ugandan academic and activist, constituted arbitrary detention.[281] Nyanzi was charged under the Computer Misuse Act for Facebook posts critical of President Yoweri Museveni and the First Lady. In its findings, the Working Group raised concerns about the broad and vague nature of the legislative provisions used in her case, highlighting the potential impact on freedom of expression. It further noted that her detention raised human rights concerns, including issues related to free expression, fair trial rights, the presumption of innocence, personal liberty and protection from cruel, inhuman or degrading treatment. This case has contributed to ongoing discussions about the balance between regulating online speech and safeguarding fundamental freedoms.[282]

In January 2023, the **Ugandan Constitutional Court** declared Section 25 of the Computer Misuse Act null and void, ruling that its vague language violated the right to freedom of expression guaranteed under the Constitution.[283] The Court noted that laws must be clear and precise to prevent arbitrary prosecution.[284] This case emphasized the need for legislative clarity to protect fundamental rights.[285]

The **Anti-Pornography Act** further complicates Uganda's legal response to cybercrimes.[286] The Act has been criticized for victim blaming in cases of NCII, where women whose photos are shared without consent are arrested instead of the perpetrators.[287] In contrast, the **Sexual Offences Bill**, currently under parliamentary consideration, offers hope for a more victim-centred approach.[288] Addressing online GBV is a critical avenue for justice, and the Bill seeks to create a more comprehensive legal framework to protect victims and hold perpetrators accountable.[289]

280 Global Partners Digital, ARTICLE 19 West Africa, "An ever-tightening net: Restrictions on online expression under cybercrime laws and content restrictions in Africa, the Middle East and Türkiye", 2024, accessible at: https://www.gp-digital.org/publication/an-ever-tightening-net-restrictions-on-online-expression-under-cybercrime-laws-and-content-restrictions-in-africa-the-middle-east-and-turkiye/.

281 United Nations Human Rights Council, Working Group on Arbitrary Detention, "Opinions adopted by the Working Group on Arbitrary Detention at its seventy-ninth session, 21-25 August 2017", A/HRC/WGAD/2017/57, 2017, accessible at: https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2017/04/A_HRC_WGAD_2017_57.pdf.

282 Global Freedom of Expression, Columbia University, "Nyanzi v. Uganda", 2021, accessible at: https://globalfreedomofexpression.columbia.edu/cases/case-dr-stella-nyanzi/.

283 Chapter Four, "Andrew Karamagi and Robert Shaka v Attorney General (Constitutional Petition No.5 of 2016)", accessible at: https://chapterfouruganda.org/resources/judgements/judgment-andrew-karamagi-and-robert-shaka-v-ag-petition.

284 African Centre for Media Excellence, "Lessons from the court's decision about Uganda's computer misuse law", 2023, accessible at: https://acme-ug.org/2023/01/18/lessons-from-the-courts-decision-about-ugandas-computer-misuse-law/#:~:text=The%20law%20should%20be%20clear,what%20constitutes%20a%20criminal%20offence.

285 Ibid.

286 Uganda Legal Information Institute, "Anti-Pornography Act", 2014, accessible at: https://ulii.org/akn/ug/act/2014/1/eng@2014-02-17.

287 Interviews with women's rights lawyers and digital rights activists in Uganda, 23–24 October 2024.

288 Parliament of Uganda, "The Sexual Offences Bill", 2024, accessible at: https://bills.parliament.ug/uploads/3555The_Sexual_Offences_Bill,2024.pdf.

289 Interviews with women's rights lawyers and digital rights activists in Uganda, 23–24 October 2024.

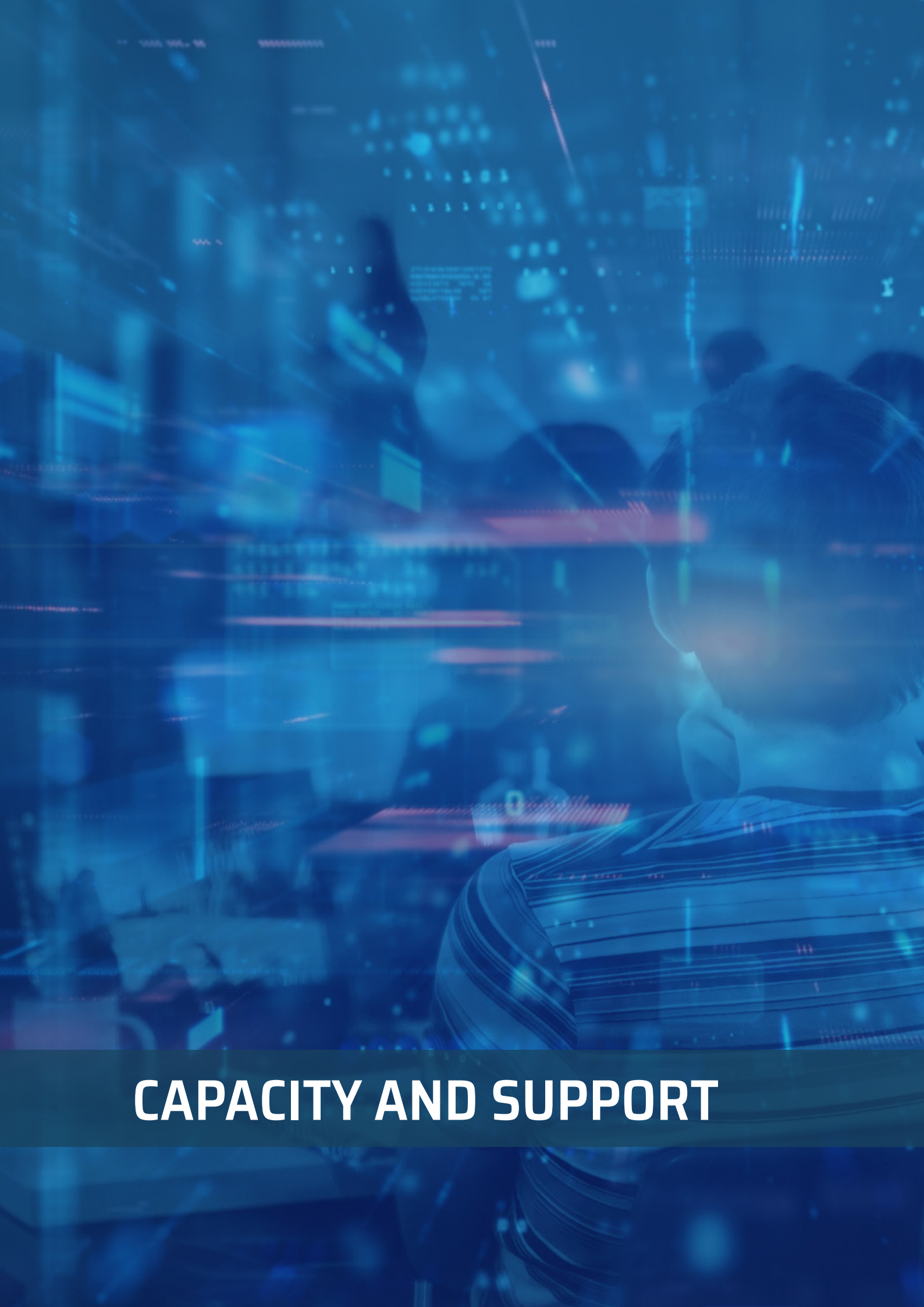
From a policy perspective, the **Digital Uganda Vision** provides a strategic framework for leveraging ICTs to empower citizens, promote inclusion and foster innovation while ensuring the security of information and personal data as well as privacy. The **Third National Development Plan (2020/21–2024/25)** underscores cyberspace as both a platform for progress and a battleground for disinformation and cybercrime, emphasizing the need for robust safeguards. The **National Cybersecurity Strategy** further reinforces these goals by guiding the secure management of ICT resources to ensure their sound operation and protection against security threats. Together these frameworks establish a comprehensive vision for building a secure, innovative and inclusive digital ecosystem.[290]

Positive trajectories but room for improvement

The respective countries are at different stages of fostering and sustaining conducive legal frameworks. While there have been efforts by all four countries, there is scope for more to be done. Clear, consistent and accessible legal avenues for addressing cybercrimes and online harms must be ensured, while adhering to the rule of law and human rights standards.

Namibia's lack of dedicated cybercrime legislation remains a significant barrier to advancing access to justice. However, the apparent political will, regional obligations under the Malabo Convention and developments such as the United Nations Convention against Cybercrime suggest that compliant legislation may soon be enacted. **Sierra Leone** is on a promising trajectory, but safeguards are needed to prevent misuse of its legal framework. Strong legal precedents, clear procedural guidelines and a review of ambiguous legislative language can help ensure laws are applied consistently and only for legitimate claims. **South Africa** also shows progress, yet challenges remain regarding public awareness and the accessibility of legal frameworks, which can hinder access to justice. **Uganda**'s legal environment, however, is less conducive. While constitutional challenges and potential reforms like the Sexual Offences Bill are encouraging, concerns around the Anti-Pornography Act and the Computer Misuse Act highlight the need for further law reform and public participation in legislative processes.

290 Uganda's Ministry of ICT and National Guidance, "Ugandan National Cybersecurity Strategy 2022-2026", DigWatch, 2023, accessible at: https://dig.watch/resource/ugandan-national-cybersecurity-strategy-2022-2026.



CAPACITY AND SUPPORT

The technical capacity of and support for law enforcement, investigative professionals and legal and judicial professionals in Namibia, Sierra Leone, South Africa and Uganda reflect both shared challenges and varying progress.

Training and capacity-building

Namibia faces significant challenges equipping its police force to address cybercrimes effectively, including a lack of structured and comprehensive training programmes tailored to investigating them.[291] The police training curriculum has yet to include courses on cybercrimes or basic computer skills, exacerbating the already low levels of digital literacy among officers.[292] A study on leveraging technology to enhance effective electronic policing revealed that 30 per cent of respondents identified computer illiteracy among police officers as a barrier to implementing innovations.[293]

This gap is particularly problematic in handling sensitive cases, such as online child sexual exploitation and abuse, which require both technical expertise and a child-friendly, trauma-informed approach.[294] Research reveals an inability to investigate online child sexual exploitation and abuse effectively, with one representative from the Office of the Prosecutor General noting that it prevents such cases from reaching court for proper adjudication.[295] Despite general optimism that Namibia's cybercrimes legislation will soon be enacted, stakeholders are concerned that the police, prosecutors and judges may need additional training and capacity development on emergent technologies to implement it effectively.[296]

Uganda, similarly to Namibia, faces significant challenges in the fight against cybercrime; some police stations lack basic resources like computers, highlighting the technological gaps in law enforcement.[297] There is also a pressing need for a structured training and certification programme to address the gaps in cybersecurity skills. The current education system does not adequately incorporate the use of ICT and the awareness of cybersecurity issues at all levels.

By contrast, **Sierra Leone** has taken significant steps towards addressing cybercrime through capacity-building initiatives and collaborative training efforts, reflecting a growing commitment to improving knowledge and skills across the criminal justice system.[298] Recent initiatives have included training programmes for police,

291 Interview with Detective Chief Inspector Ratjindua Tjivikua, Head of Cybercrimes, NamPol, 9 October 2024.

292 Nelago and others, "Leveraging Technology to Enhance Effective Electronic Policing in Developing Countries", IST Africa, 2022, accessible at: https://ieeexplore.ieee.org/document/9845626.

293 Ibid.

294 ECPAT, INTERPOL, UNICEF, "Disrupting Harm in Namibia".

295 Ibid.

296 Interview with Communications Regulatory Authority of Namibia, 9 October 2024.

297 Interview with staff at UPF, 24 October 2024.

298 Interviews with staff at NC3, 4–5 November 2024; Interview with staff at the Cyber Investigation and Forensic Unit, SLP, 4 November 2024.

prosecutors and judges, focusing on critical areas such as the provisions of the new cybercrime law, cybercrime fundamentals, handling electronic evidence and managing international information requests.[299] The establishment of training-of-trainers programmes and collaborations with international partners such as INTERPOL have further strengthened the capacity for sustainable training.[300] Police officers interviewed in the scope of this research have expressed gratitude for these opportunities.[301]

Despite these efforts, challenges remain in Sierra Leone. Prosecutors face difficulties in securing convictions due to insufficient evidence, often stemming from inadequate police investigations.[302] Judges, too, require specialized training, particularly when traditional evidence rules are inadequate to address the technical nuances of cybercrimes. While training provided by organizations like the United Nations Office on Drugs and Crime (UNODC) has been beneficial, there is a clear need for dedicated resources, such as e-evidence guidelines or specialized cybercrime courts.[303]

Notably, **South Africa**'s cybercrime legislation emphasizes the need to establish and maintain sufficient human and operational capacity to detect, prevent and investigate cybercrimes.[304] It mandates that the police provide basic cybercrime-related training to its officers. Additionally, it requires collaboration with higher education institutions, both domestically and internationally, to develop accredited training programmes for police personnel specifically engaged in cybercrime detection, prevention and investigation. Despite these provisions, gaps remain in the implementation of effective training programmes.[305] While initial police training includes foundational investigative techniques through initiatives like the Detective Learning Program and Resolving of Crime, these efforts are largely geared towards traditional crime investigation.[306] Many officers lack the specific skills and resources required to handle cybercrime cases, especially at the early stages of a cybercrime where victims often seek immediate support.[307]

299 SLP, "40 Police Officers Concludes Cyber and Digital Evidence Training", 2023, accessible at: http://www.police.gov.sl/uncategorized/40-police-officers-concludes-cyber-and-digital-evidence-training/.

300 Interviews with staff at NC3, 4–5 November 2024; Interview with staff at the Cyber Investigation and Forensic Unit, SLP, 4 November 2024.

301 Interview with staff at the Cyber Investigation and Forensic Unit, SLP, 4 November 2024.

302 Interviews with staff at NC3, 4–5 November 2024.

303 Interview with staff at the Cyber Investigation and Forensic Unit, SLP, 4 November 2024; Interviews with staff at NC3, 4–5 November 2024.

304 Republic of South Africa, "Act No. 19 of 2020".

305 Interview with staff at the Cybercrime Investigation Component, DPCI, 26 November 2024.

306 Mmabatho Aphane, Jacob Mofokeng, "South African Police Service Capacity to Respond to Cybercrime: Challenges and Potentials", Journal of Southwest Jiaotong University 56 (4): 165–186, 2021, accessible at: https://www.researchgate.net/publication/355089776_SOUTH_AFRICAN_POLICE_SERVICE_CAPACITY_TO_RESPOND_TO_CYBERCRIME_CHALLENGES_AND_POTENTIALS.

307 Interview with staff at the Cybercrime Investigation Component, DPCI, 26 November 2024.

Efforts to address these shortcomings include the development of an enhanced cyberthreat intelligence system and a cybersecurity strategic plan by SAPS.[308] This initiative aims to predict and deter cyber-related threats and includes basic cybercrime detection training for station-level officers. These skills are designed to help officers identify, categorize and open dockets for cybercrime offences. While this represents progress, the overall capacity to detect and prosecute cybercrime-related cases remains limited, underscoring the need for more comprehensive and specialized training programmes.

South African civil society has adopted a promising practice to support judicial digital literacy. Media Monitoring Africa has intervened as an amicus curiae ("friend of the court") to provide guidance on the nuances of the application of human rights online,[309] including cases on hate speech, harassment, defamation and discrimination.[310] They are presently preparing a handbook for judges to assist them in addressing online harms.[311] This is a good practice because it enhances the judicial capacity to understand and apply human rights principles in the digital age, ensuring that courts are better equipped to address complex issues. Ultimately, it fosters a more informed and effective legal response to online harms and cybercrimes.

Challenges in retaining skilled personnel

Retaining skilled personnel to investigate cybercrimes presents a significant challenge across the selected countries. In **Namibia**, a shortage of qualified individuals with IT, cybersecurity and investigative skills hinders recruitment. The need for personnel who can bridge the gap between technical expertise and traditional policing is critical, but limited prioritization and understanding from senior leadership result in a lack of growth opportunities within the key departments. As a result, after being trained, personnel often leave to seek opportunities elsewhere, particularly in the private sector. The lack of clear benefits or career advancement in this field makes retaining specialized experts difficult.[312] **South Africa** faces a similar issue, with many skilled professionals leaving for the private sector's better salaries and benefits. This trend highlights the competitive

308 Pieter Matsaung, David Tubatsi Masiloane, "The role of cyber intelligence in policing cybercrime in South Africa: Insights from law enforcement officers", African Security Review, 2024, accessible at: https://doi.org/10.1080/10246029.2024.2421225.

309 Interview with digital rights activist in South Africa, 15 November 2024.

310 In "Mavhidula (on behalf of the South African Human Rights Commission) v Matumba (01/2021)", Media Monitoring Africa raised pertinent questions about a series of posts on Twitter and whether they amounted to harassment; in "Economic Freedom Fighters v Manuel, ZASCA 172, 2020", it presented arguments as amicus curiae to the Supreme Court of Appeal on the appropriate balance between the rights to freedom of expression, dignity and reputation and the "reasonable reader" notion in a social media context; and in "South African Human Rights Commission & another v Lagardien (2023/2391)", it is advancing submissions on the appropriate balance between the rights to freedom of religion, freedom of expression, equality and dignity on WhatsApp groups.

311 Interview with human rights lawyers in South Africa, 25 November 2024.

312 Interview with Detective Chief Inspector Ratjindua Tjivikua, Head of Cybercrimes, NamPol, 9 October 2024.

nature of the job market and the challenge of keeping personnel committed to public service roles in cybercrime investigations.[313]

Uganda, with a good pool of graduates in computer-related fields, faces comparable challenges in retaining talent due to insufficient budgetary incentives and opportunities for growth within the public sector. Retention remains an issue due to competitive external opportunities and a lack of adequate incentives within the public sector. Improving budget allocations and offering better opportunities for career advancement could help to address these retention challenges.[314]

In comparison, **Sierra Leone** has seen success in attracting and retaining young, highly skilled staff. The country has made efforts to invest in upskilling and fostering a sense of ownership among the workforce, offering opportunities for engagement with the international community and professional certifications. By involving personnel in structural discussions and decision-making, Sierra Leone is cultivating a motivated and committed workforce that is more likely to stay and contribute to the country's growing cybercrime response efforts.[315]

Tools, resources and infrastructure

In many countries, a significant challenge in the fight against cybercrime is the lack of adequate resources and infrastructure to support effective investigations. **Namibia**, for instance, faces financial constraints that hinder the development of its cybercrime investigation capabilities.[316] While the country has a national forensic lab, it is not under the control of the police, and the desire for an independent lab capable of performing its own cybercrime analysis remains unmet.[317] The lack of sufficient technological resources, coupled with unreliable Internet access and underdeveloped ICT infrastructure, results in delayed case docket clearance and impedes crime prevention efforts. Approximately 60 per cent of respondents in a local study attribute this resource deficiency to the failure to combat cybercrime effectively.[318] Despite government recognition of the issue, it is perceived as being underprioritized.[319] Additionally, the court system requires documents to be filed in hard copy, with limited scope for introducing evidence that is best presented electronically as is often the case with cybercrimes.[320]

313 Interview with staff at the Cybercrime Investigation Component, DPCI, 26 November 2024.

314 Interview with staff at the UPF, 24 October 2024.

315 Interviews with staff at NC3, 4–5 November 2024.

316 Interview with Detective Chief Inspector Ratjindua Tjivikua, Head of Cybercrimes, NamPol, 9 October 2024.

317 Interview with Communications Regulatory Authority of Namibia, 9 October 2024.

318 Nelago and others, "Leveraging Technology to Enhance Effective Electronic Policing in Developing Countries".

319 Interview with Detective Chief Inspector Ratjindua Tjivikua, Head of Cybercrimes, NamPol, 9 October 2024.

320 Interview with Detective Chief Inspector Ratjindua Tjivikua, Head of Cybercrimes, NamPol, 9 October 2024.

Sierra Leone faces similar hurdles. Most of the funding for its cybersecurity efforts comes from international donors, suggesting that the government may not have the political will to fully invest in the necessary technological infrastructure.[321] However, the establishment of the National Cybersecurity Advisory Council, with the Deputy President as a key figure, indicates some political commitment to improving the country's digital security.[322] Another significant step was the launch of the National Digital Forensics Lab and the National Cyber Security Incident Response Team in January 2025, housed at the NC3 in Freetown. This milestone marks a considerable advance in Sierra Leone's cybersecurity capabilities and reflects a growing capacity to address cyberthreats.[323]

In **South Africa**, budget constraints and challenges such as frequent controlled power outages (known as load shedding) continue to impede the effective use of tools and resources. Although some investigative tools exist, they are scattered across different departments and are often underutilized due to siloed working environments. The lack of reliable Internet access and online tools further hampers investigative efforts, as officers must rely on their personal devices to carry out their duties.[324]

Uganda, too, faces resource challenges, particularly in the area of forensic services.[325] A positive development in Uganda is the commissioning of a modern forensic lab, which is expected to support quicker investigations and, ultimately, improve conviction rates in the courts.[326] However, continued investment is needed to ensure the lab reaches its full potential and enhances the overall effectiveness of the police force in tackling cybercrime.

321 Interviews with staff at NC3, 4–5 November 2024.

322 Interviews with staff at NC3, 4–5 November 2024.

323 Economic Community of West African States, "ECOWAS and Sierra Leone Launch National Cybersecurity Incident Response Team and Digital Forensics Lab in Freetown", 2025, accessible at: https://www.ecowas.int/ecowas-and-sierra-leone-launch-national-cybersecurity-incident-response-team-and-digital-forensics-lab-in-freetown/.

324 Interview with staff at the Cybercrime Investigation Component, DPCI, 26 November 2024.

325 Interview with staff at the UPF, 24 October 2024.

326 UPF website, "Police's Modern Lab Commissioned", 2021, accessible at: https://upf.go.ug/polices-modern-lab-commissioned/.

Collaborative efforts

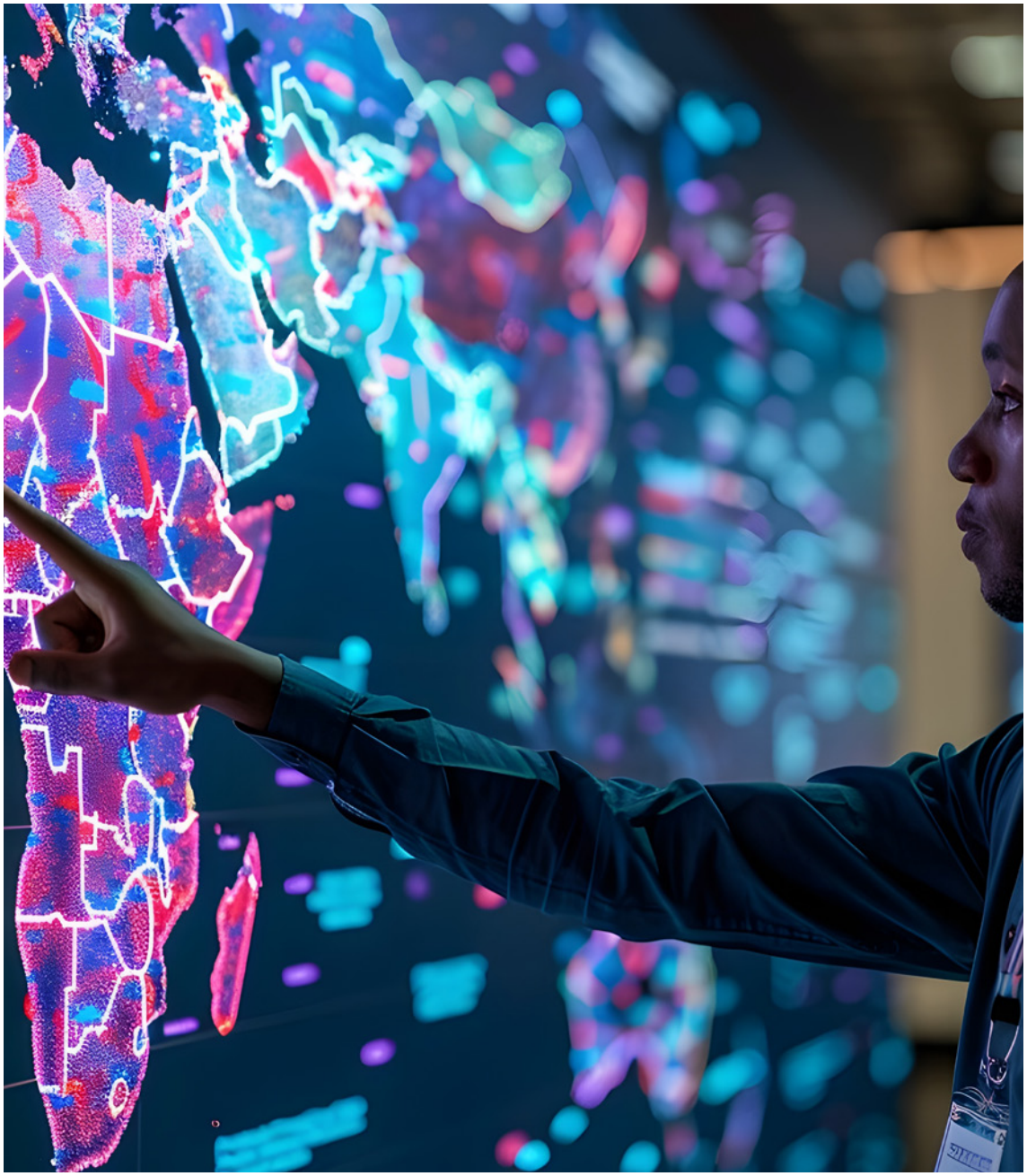
Across all the countries discussed, there is a shared recognition of the importance of collaborative, multi-stakeholder governance to address cybercrime effectively.[327] Many emphasized the need for improved communication between departments and an eagerness to establish more integrated training programmes that involve the police, prosecutors, judges and civil society. Several stakeholders across the counties highlighted the significance of cooperative governance and regional support as essential components of a successful cybersecurity strategy. Collaborations with cybersecurity experts were also seen as a crucial way to enhance the effectiveness of responses to cyberthreats.

The need for more resources is also a common concern, with all countries advocating for collaboration with other nations to share resources, tools and infrastructure. This exchange of expertise and technologies can create opportunities for mutual learning and strengthen national capabilities. A key area of focus is integrated training programmes that bring together justice system stakeholders, as these can improve coordination and ensure a more unified response to cybercrime. Interregional collaboration is also welcomed, as it provides valuable avenues for sharing best practices and enhancing collective capacity.

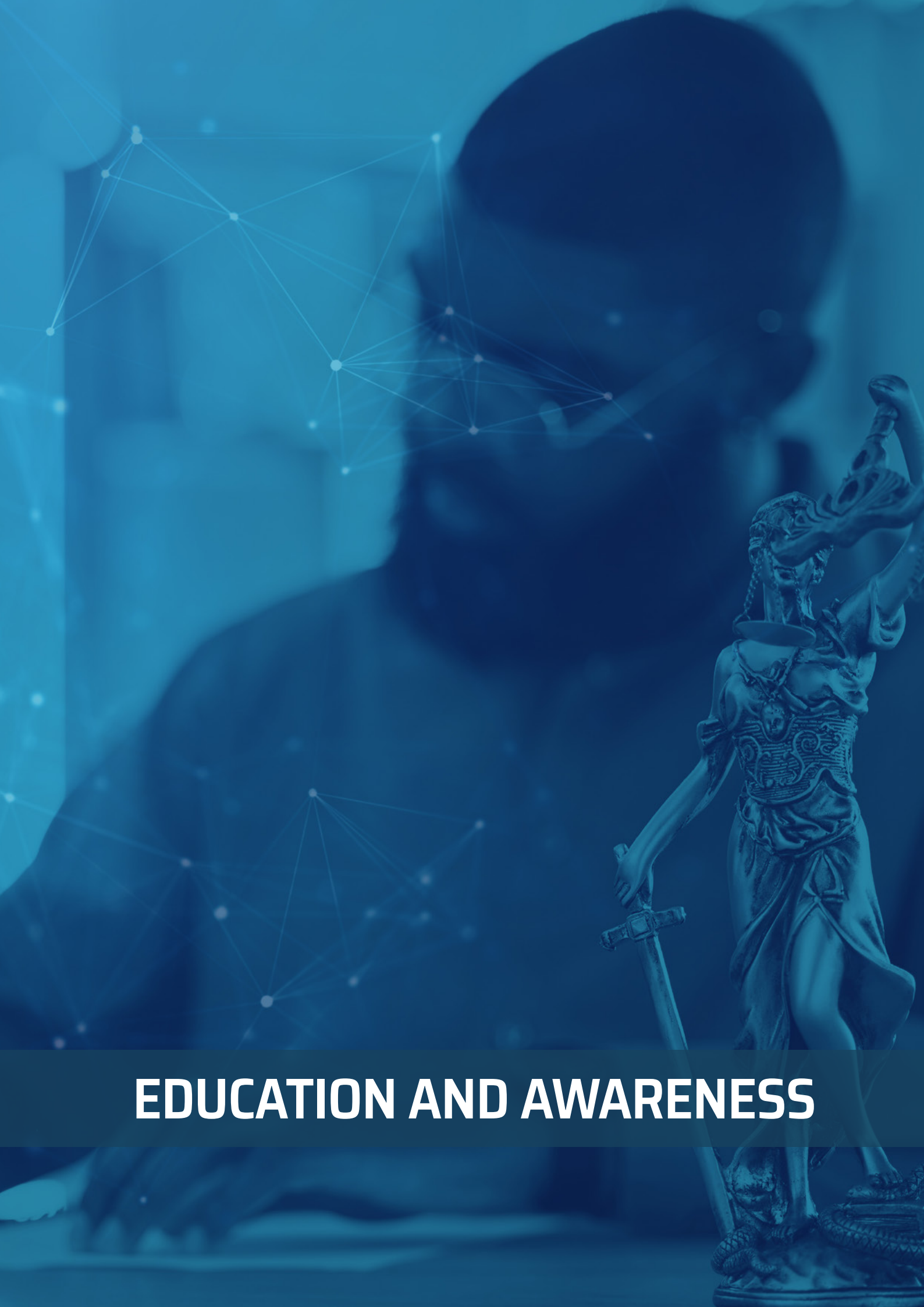
Civil society plays a vital role in this multi-stakeholder approach, with NGOs, social workers and other organizations calling for joint training activities to strengthen their ability to respond to cyber-related issues.[328] These collaborative efforts not only promote shared learning but also foster a sense of collective responsibility for tackling the complexities of cybercrimes and online harms. Through such initiatives, countries can build more resilient, informed and coordinated systems for addressing the growing challenges posed by cyberthreats.

327 Interview with staff at the Cybercrime Investigation Component, DPCI, 26 November 2024; Interview with staff at the Cyber Investigation and Forensic Unit, SLP, 4 November 2024; Interview with Communications Regulatory Authority of Namibia, 9 October 2024; Interview with staff at the UPF, 24 October 2024.

328 Interview with a non-governmental organization working on children's rights in Namibia, 10 October 2024.



“Building cybercrime response capacity requires more than tools—it demands sustained investment, inter-agency coordination, and talent retention across the justice chain.”



EDUCATION AND AWARENESS

Education and awareness are critical to address the challenges posed by the digital divide and ensure equitable access to justice. While strides have been made to improve digital literacy and foster online safety, significant gaps remain. Aligned with underreporting as noted above, a lack of education and awareness not only perpetuates disparities but also hinders cybercrime victims asserting their rights and seeking remedies. Many are unaware that certain harmful online actions constitute crimes, lack knowledge of their legal rights or do not know how to report incidents or pursue justice effectively.

Digital literacy and the impact on access to justice

Namibia faces significant challenges related to digital literacy, as its digital divide exacerbates existing inequalities and limits opportunities for those without access to technology.[329] Many schools and communities lack the resources or qualified instructors to teach digital literacy, leaving individuals, particularly vulnerable and marginalized groups, unable to navigate the digital world. Information dissemination in underserved communities, such as informal settlements, is often erratic and dependent on individuals rather than organized efforts, leading to low levels of awareness, especially regarding cybersecurity.[330]

Sierra Leone also faces significant challenges addressing low digital literacy rates. Combined with limited opportunities for developing digital skills, they hinder many individuals from fully and safely participating in the online world. In particular, the country's youth require foundational to advanced digital skills to take advantage of the opportunities offered by the digital economy. However, few primary or secondary schools in Sierra Leone teach computer skills or have access to computer labs. The lack of reliable Internet access and electricity infrastructure further complicates efforts to integrate ICTs into education.[331] While some progress has been made thanks to recent interventions by both the public and private sectors, digital illiteracy among youth and persons with disabilities is persistently low. Some research suggests that a significant portion of Sierra Leoneans still lack basic online protection skills: approximately 80 per cent do not have the essential knowledge or techniques needed to safeguard themselves against cybercriminals.[332]

329 Communications Regulatory Authority Namibia, "Embracing the Digital Future: The Crucial Role of Digital Literacy in Namibia", 2024, accessible at: https://www.cran.na/embracing-the-digital-future-the-crucial-role-of-digital-literacy-in-namibia/.

330 Elmarie Biermann, "A Digital Odyssey".

331 Sierra Leone Ministry of Communication, Technology and Innovation, "Sierra Leone Digital Transformation Project: Comprehensive study to assess the supply and demand of digital skills and to evaluate the potential of the gig economy to provide employment opportunities to youth, women, and people with disabilities in Sierra Leone", 2024, accessible at: https://moic.gov.sl/wp-content/uploads/2024/03/SLDTP-Digital-Skills-and-Gig-Economy-Studies-TOR.pdf.

332 Ibrahim Abdulai Sawaneh, "Cybercrimes: Threats, Challenges, Awareness, and Solutions in Sierra Leone", Asian Journal of Interdisciplinary Research 3 (1): 185–195, 2020, accessible at: https://www.researchgate.net/publication/339812214_Cybercrimes_Threats_Challenges_Awareness_and_Solutions_in_Sierra_Leone.

Aligned with this trend, **South Africa** faces challenges bridging the digital divide, which has a profound impact on digital literacy, particularly in rural areas. This divide is further exacerbated by the high cost and limited availability of infrastructure, networks, devices, services and data. This hinders many South Africans from accessing the online world and, when they do, they are often not equipped to engage with it safely. Stakeholders observed that many people in South Africa do not know how to safeguard themselves from cybercrimes, and are also often unaware that the harms they have suffered may be unlawful.[333]

In **Uganda**, the digital divide between urban and rural areas remains a significant barrier to widespread digital literacy. Stakeholders estimate that roughly 30 per cent of the population can effectively use digital tools but most people lack basic knowledge about cybercrimes and protection measures.[334] Taking mobile money as an example, a study in Uganda's Lango and West Nile regions found that 60 per cent of female respondents lacked the digital skills necessary to carry out mobile money transactions. This makes them vulnerable and places them at risk if they do engage online.[335]

A novel approach to education in Uganda has emerged from a proposal by a key stakeholder emphasizing the need to focus on Members of Parliament.[336] The idea is that by equipping them with the necessary knowledge on digital issues, they will be better informed when reviewing and passing related bills. While there have been improvements in police awareness-raising efforts, there is a recognized need for further engagement with several stakeholders. As the decision makers who ultimately pass laws, Members of Parliament must be at the centre of these educational initiatives, but civil society could play a role by sharing information and engaging with them to help them understand the real-world challenges affecting their communities.

333 Interview with staff at the Cybercrime Investigation Component, DPCI, 26 November 2024; Interview with human rights lawyers in South Africa, 25 November 2024.

334 Interview with digital rights activist in Uganda, 23 October 2024.

335 United Nations Capital Development Fund, "Using a Digital Literacy Toolkit to Narrow the Digital Skills Gap for Women and Smallholder Farmers in Uganda", 2023, accessible at: https://www.uncdf.org/article/8113/using-a-digital-literacy-toolkit-to-narrow-the-digital-skills-gap-for-women-and-smallholder-farmers-in-uganda.

336 Interview with digital rights activist in Uganda, 23 October 2024.

Positive practices

Namibia is paying special attention to digital literacy initiatives. Civil society organizations and the government have made notable strides in digital literacy and cybersecurity awareness. For example, LifeLine/ChildLine Namibia have conducted various training sessions such as the "Parenting in the Digital Age" initiative, reaching 202 parents/guardians; and "Online Child Sexual Exploitation and Abuse", which engaged 2,068 participants in 2024. Additionally, six child protection training sessions, which include elements of online safety, reached 159 participants in 2024.[337]

The Namibian government has also taken significant steps to improve digital literacy and cybersecurity awareness. MICT has signed a five-year Memorandum of Understanding with LifeLine/ChildLine Namibia to intensify efforts to protect children from online threats. This partnership focuses on equipping children with the knowledge to navigate the digital world safely.[338] Furthermore, MICT has launched several initiatives including online public awareness sessions, a WhatsApp bot linked to weekly cybersecurity sessions and the iSecure website.[339] The iSecure platform, launched in 2024, serves as a resource for general cybersecurity information and aims to raise awareness about the dangers of cybercrime in Namibia.[340] These efforts highlight a growing recognition of the importance of digital literacy and cybersecurity address both the risks and opportunities of the digital world, especially for rural and limited-access populations.

The **Sierra Leone** National Cybersecurity Coordination Centre, in partnership with the Ministries of Communications and Education, the World Bank and UNDP, launched the National Cyber Awareness Schools Debate in 2024. This initiative saw 16 schools participate in a competition aimed at raising cybersecurity awareness among students.[341] Another notable initiative is the creation of Bridge the Digital Divide – Sierra Leone, an NGO dedicated to providing free digital tools, equipment and digital skills training at both national and local levels.[342] Together, these efforts reflect a growing recognition of the importance of improving digital literacy in Sierra Leone and enhancing the country's capacity to engage in the digital economy.

337 Interview with a non-governmental organization working on children's rights in Namibia, 10 October 2024.

338 Alfred Shilongo, "Namibia's cyber strategy focuses on children", IT Web Africa, 2024, accessible at: https://itweb.africa/content/j5aIrvQA1AxvpYQk.

339 Interview with staff at MICT, 9 October 2024.

340 "iSecure", accessible at: https://isecure.na/.

341 AYV News , "Annie Walsh: Champions of Cyber Awareness Schools Debate", 2024, accessible at: https://ayvnews.com/annie-walsh-champions-of-cyber-awareness-schools-debate/.

342 ITU Academy, "Bridge the Digital Divide Sierra Leone - Sierra Leone (BDDSL)", accessible at: https://academy.itu.int/bridge-digital-divide-sierra-leone-sierra-leone-bddsl.

In response to its own challenges, **South Africa** has a few examples of efforts to promote digital literacy. One notable programme is Web Rangers, a digital literacy project aimed at equipping young people with the skills and knowledge necessary for online safety.[343] Launched in 2016, Web Rangers empowers youth to take ownership of their digital footprints and use their knowledge to create their own innovative campaigns promoting safe and responsible Internet usage. Beyond safety, the programme also emphasizes media literacy, helping young people develop critical thinking skills to engage with news and information in a discerning manner. This initiative fosters a sense of active citizenship, enabling participants to self-regulate and protect themselves from risks such as cyberbullying and online sexual misconduct.

Additionally, the Library and Information Association of South Africa launched the South African Digital Literacy Day in 2024 as part of Global Media and Information Literacy Week.[344] This initiative, a response to UNESCO's recommendation to promote digital literacy, aims to educate and empower communities to interact productively with technologies. Other awareness campaigns, such as those hosted by the South African Banking Risk Information Centre, encourage individuals to be vigilant online and take precautions to protect their personal information.[345] The SAPS also provide tips on how to be safe online.[346]

There are also positive developments underway to enhance digital literacy and online safety in **Uganda**. This ranges from creating comic books to educate people about their rights[347] to an educational toolkit designed to help young people stay safe online.[348] The UPF send bulk SMS text messages to members of the public, broadcast messages on the news and go to schools as part of their cybercrime education and awareness efforts.[349]

The positive practices highlighted across various countries demonstrate promising steps towards addressing digital literacy gaps and promoting online safety. These initiatives underscore the importance of empowering individuals and communities to navigate the digital world effectively and securely. However, while commendable, more focused and inclusive strategies are needed to ensure that programmes and initiatives are accessible to all, particularly vulnerable and marginalized groups.

343 "Web Rangers", accessible at: https://webrangers.co.za/.

344 Library and Information Association of South Africa, "South African Digital Literacy Day", 2025, accessible at: https://www.liasa.org.za/events/EventDetails.aspx?id=1899806.

345 South African Banking Risk Information Centre, "SABRIC urges South Africans to #TakeACloserLook this National Cyber Security Awareness Month", 2024, accessible at: https://www.sabric.co.za/media-and-news/press-releases/sabric-urges-south-africans-to-takeacloserlook-this-national-cyber-security-awareness-month/.

346 SAPS, "Cybercrime prevention tips", accessible at: https://www.saps.gov.za/alert/cybercrime_prev_tips.php.

347 Interview with digital rights activist in Uganda, 23 October 2024.

348 Internet Society Uganda Chapter, "E-Safety Education Toolkit for Young People in Uganda", accessible at: https://isoc.ug/wp-content/uploads/2019/10/Tool-Kit-final.pdf.

349 Interview with staff at UPF, 24 October 2024.

To achieve comprehensive empowerment, programmes must adopt a dual approach by being **proactive** and **reactive**. Proactively, initiatives should focus on equipping individuals with the skills and knowledge to protect themselves online, fostering digital literacy and building resilience against cyberthreats and risks. Reactively, efforts should prioritize raising awareness of victims' rights, guiding them on the steps to take after experiencing cybercrimes and providing clear pathways to report incidents and access remedies. By combining proactive education with reactive support mechanisms, stakeholders—government, civil society and the private sector—can create a nuanced framework that empowers individuals to use digital tools safely and to seek justice effectively when harm and crime occur.

RECOMMENDATIONS

Key trends in research

Notwithstanding the challenges, collecting reliable data on cybercrimes, available research, case law and stakeholder engagement highlight that cybercrime is a pressing and pervasive issue in Africa. The infiltration of cybercrime into financial and personal realms is evident, with individuals increasingly targeted by online fraud, identity theft, phishing scams and unauthorized access to personal data. As digital platforms become more integral to daily life, the potential for exploitation grows, leaving users vulnerable to both financial loss and psychological harm among other consequences.

Women are disproportionately impacted by cybercrimes—particularly in the form of online harassment, cyberstalking and image-based abuse—and this gendered dimension often intersects with patriarchal societal norms and systemic inequalities. This makes women more susceptible to abuse and less likely to report incidents due to fear of stigma, re-victimization or ineffective responses from law enforcement. This trend underscores the urgent need for gender-sensitive policies and mechanisms to address the unique vulnerabilities faced by women in the digital sphere.

Cybercrimes result in significant rights violations, including breaches of privacy, freedom of expression and the right to dignity. Victims often face compounded harm as these violations ripple into their professional, personal and psychological well-being. For example, online harassment and abuse can silence voices, discourage participation in public life and deepen inequalities. The lack of accessible justice mechanisms further exacerbates these rights violations, leaving many victims without recourse and emboldening perpetrators to continue exploiting digital vulnerabilities. This research underscores critical gaps and challenges addressing cybercrimes and ensuring equal access to justice in the focus countries.

Six overarching trends emerge:

1. Lack of available data

A significant gap exists in the collection and publication of official statistics on cybercrimes. This lack of available data inhibits the ability of governments, law enforcement and policymakers to understand the scope and nature of cyberthreats. Without accurate data, it is difficult—near impossible—to allocate resources effectively, develop targeted interventions or craft informed legal and policy responses. For victims, the absence of reliable data can diminish their visibility in the justice system, reinforcing perceptions that their grievances are insignificant or ignored.

2. Underreporting

Underreporting is a universal issue, influenced by a combination of stigma, fear of re-victimization and limited knowledge of legal rights and reporting mechanisms. Many victims remain unaware that the online harms they experience constitute crimes or that remedies are available. For others,

the prospect of encountering insensitive responses or systemic barriers discourages them from seeking justice. This perpetuates a cycle where victims remain invisible and systemic improvements are hindered by a lack of documented cases.

3. Gendered impact of cybercrimes

In every focus country, cybercrime disproportionately impacts women, with higher levels of personal cybercrimes such as cyberstalking, online harassment and cyberbullying compared to men. Although statistics are limited, stakeholder feedback highlights this gender disparity. The complex underlying factors include patriarchal norms, limited access to the Internet and insufficient digital literacy, all of which increase women's vulnerability to cybercrimes.

4. Need for a conducive legal framework

While legal responses to cybercrimes are evolving, existing frameworks often lack clarity, accessibility or enforcement capacity. A conducive legal environment is crucial for access to justice, ensuring that victims have the means to seek redress and that offenders are held accountable. This research emphasizes that laws must be human rights-based, clearly defined and include operational standards to enable effective implementation.

5. Capacity gaps

The limited technical capacity of law enforcement, the judiciary and other stakeholders is a widespread barrier. Many professionals lack the tools, training and knowledge to identify, investigate and prosecute cybercrimes effectively. This undermines the justice system's ability to respond to cybercrimes and erodes trust among victims, further deterring them from seeking help.

6. Existing education efforts need further development

Current education and awareness initiatives, while promising, need further development and scaling to achieve a balance between proactive and reactive approaches. Proactive measures focus on equipping individuals with digital literacy skills and strategies to stay safe online; reactive efforts involve empowering victims to respond effectively when harms occur. Both are fundamental to fostering an empowered and accessible justice system.

Evidence-based recommendations

To address these trends and empower victims of cybercrimes while strengthening access to justice and community resilience, the following recommendations are proposed:

Implement gender-transformative responses

Due to clear gender disparities, all recommendations and responses need to be seen through a gender-transformative lens. It is essential to **adopt gender-transformative approaches** that not only address the immediate harms caused by online violence but also challenge the structural and systemic inequalities that fuel it. A gender-transformative response goes beyond merely addressing the symptoms of cybercrimes—it seeks to shift the underlying power dynamics, create more equitable access to digital spaces and ensure that women and marginalized groups are empowered to participate safely in the digital world.[350]

Ratify relevant international treaties

The four focus countries should ratify and domesticate international treaties like the Malabo Convention, the Budapest Convention and the United Nations Convention against Cybercrime. Specifically, Uganda is encouraged to ratify the Malabo Convention and Budapest Convention, and Namibia is also encouraged to ratify the Budapest Convention. These frameworks provide guidance on establishing effective legal frameworks, promoting international cooperation and ensuring a harmonized approach to combat cybercrime.

Ratification signals a commitment to address cyberthreats and builds trust among victims and stakeholders. Subject to each country's domestication process, **local law should be infused with these regional and international frameworks as a matter of urgency** to provide a strong rights-based foundation for cybercrime responses. This integration will ensure that domestic laws are grounded in international human rights principles while addressing the evolving nature of cyberthreats. By doing so, countries can develop holistic and robust frameworks that respect human rights, protect victims and enable effective justice mechanisms.

350 Rebecca Emerson-Keeler, Amrit Swali, Esther Naylor, "Integrating gender in cybercrime capacity-building: A toolkit", Chatham House, 2023, accessible at: https://www.chathamhouse.org/sites/default/files/2023-07/2023-07-05-integrating-gender-in-cybercrime-capacity-building-emerson-keeler-et-al.pdf.

Develop model laws and conduct legislative audits

A **comprehensive model law on cybercrime** should be developed at the continental level, supported by regional and international bodies. This model law could update, build on and align with existing efforts, such as the SADC Model Law on Computer Crime and Cybercrime[351] and the United Nations Economic Commission for Africa Guide on Cybersecurity Legislation,[352] while addressing any gaps they may have. The proposed model law would adopt a **victim-centred approach**, focusing on empowering victims and ensuring their rights are protected. This would include **clear definitions** of various forms of cybercrime in precise terms, including personal and financial cybercrimes, to eliminate both ambiguities that may hinder enforcement or prosecution and misuse or abuse aimed at stifling dissent. Additionally, encouraging strong legal frameworks can help prioritize budgets more effectively, ensuring that resources are allocated towards addressing cybercrime challenges. As was raised by several stakeholders, this in turn can support the development of technical capacities, the acquisition of necessary tools and the implementation of robust systems to combat cybercrimes and protect victims.

The model law would also establish **accessible and user-friendly channels** for victims to report cybercrimes, including anonymous reporting options to address fears of stigma or re-victimization. Additionally, it would incorporate provisions that **streamline investigative and prosecutorial processes**, such as standardized evidence collection, admissibility guidelines and timelines for handling cases. This would ensure timely and effective responses to cybercrime complaints. In addition, and unlike existing model laws, it would incorporate guidance on **capacity building**, **education and awareness**.

To complement the development of this model law, **legislative audits** should be conducted in individual countries to assess existing cybercrime laws and regulations. These audits would, among others, evaluate the effectiveness of current laws and the extent to which they adequately **address emerging online harms and cybercrimes**; ensure the laws **align with human rights principles**; identify gaps and bottlenecks that may hinder access to justice; and consider clearer pathways for justice. Audits could be conducted by regional or international bodies as well as through potential peer-review mechanisms.

351 ITU, SADC, "Computer Crime and Cybercrime: Southern African Development Community (SADC) Model Law", 2013, accessible at: https://www.veritaszim.net/sites/veritas_d/files/SADC%20Model%20Law%20on%20Computer%20Crime%20and%20Cybercrime.pdf.

352 United Nations Economic Commission for Africa, "A Guideline for a model law on computer enabled and computer related crimes in the African Union Member States", 2022, accessible at: https://uneca.org/sites/default/files/Guideline_Model_Cybersecurity_Law-UNECA.pdf#:~:text=%E2%80%9CGuideline%E2%80%9D%20shall%20mean%20suggested%20cybersecurity%20legislative%20content%20for,introduction%20of%20new%20legislation%20or%20reforming%20existing%20law.

Establish clear reporting processes

To effectively address cybercrime and improve access to justice, **clear and accessible reporting processes** must be established and supported by appropriate training and tools for law enforcement agencies. These mechanisms should be designed to empower victims, build public trust and ensure efficient responses to cybercrime incidents. This requires streamlining user-friendly reporting and guidance channels such as hotlines, WhatsApp bots sharing guidance and online portals with clear instructions on how to file a report and secure digital evidence.

Develop clear coding systems for cybercrimes

Countries must establish standardized and comprehensive **coding systems** to categorize and document cybercrimes accurately. These systems are critical for improving data collection, understanding trends and crafting evidence-based responses. This needs to be coupled with law reform efforts to ensure that the definitions relied upon for the development of the codes are clear. This would likely be a multi-stakeholder task force involving law enforcement, legal experts and civil society designing and implementing coding systems tailored to local contexts. Learning from South Africa—where codes are available but the absence of training renders them ineffective—it will be necessary to train police officers, prosecutors and judges to use coding systems effectively, ensuring consistent data collection and reporting.

Consideration should also be given to **simplifying coding systems for victims of cybercrimes**. A user-friendly public-facing system could align with the law enforcement version and use clear, simple language. Avoiding legal jargon and technical terms will help victims identify the type of crime they have experienced. Incorporating icons, images or short descriptions next to each category could also make the system more accessible. Law enforcement should be trained on victim-sensitive questioning to enable victims to provide relevant information easily, which in turn can assist tagging the crime for proper categorization.

Create practical Standard Operating Procedures (SOPs)

Police and other law enforcement bodies need **practical and accessible SOPs** tailored to cybercrimes. These guidelines should outline step-by-step procedures for responding to cybercrime cases, ensuring consistency, efficiency and victim-centred approaches. SOPs should be developed to guide law enforcement officers on the proper steps for recording, investigating and managing cybercrime cases. These SOPs should ensure consistency, transparency and adherence to human rights standards.

Country learning exchanges can play a critical role in strengthening the development of SOPs. South Africa could share its experiences and provide guidance on establishing reporting mechanisms and frameworks developed during its cybercrime legislative process. Sierra Leone could highlight its ongoing efforts through the working group aimed at developing SOPs, addressing warrant

issuance and ensuring proper chain-of-custody protocols for electronic evidence, by offering valuable insights into challenges and solutions.

Provide comprehensive training for justice sector stakeholders

All stakeholders expressed appreciation for the training they had received, noting its positive impact on their understanding and handling of cybercrime cases. They collectively requested more training to further enhance their capacity to address emerging challenges in the digital space effectively.

Accordingly, it is essential to **implement comprehensive training programmes** that target key stakeholders in the justice sector, including law enforcement, prosecutors and judges. These stakeholders are on the frontlines fighting cybercrimes and upholding victims' rights, so equipping them with the necessary knowledge and tools is critical.

Joint training was mentioned by several stakeholders. The primary objective of joint training is to ensure that all parties involved in the legal process understand their respective roles and responsibilities, as well as the interdependencies of their functions. Joint training fosters a comprehensive understanding of how each stakeholder's actions impact the others in the justice system. For example, law enforcement officers responsible for investigating and collecting evidence need to understand the legal thresholds required for evidence to be admissible in court. Prosecutors, in turn, must grasp the technicalities of cybercrimes and the evidence presented by law enforcement to build a strong case. Judges, being the final arbiters, must understand not only the legal aspects but also the technical intricacies of cybercrimes to adjudicate fairly and impose appropriate penalties.

By ensuring that law enforcement, prosecutors and judges are equipped with the necessary legal, technical and victim-focused knowledge, there is greater potential for the effective administration of justice. This knowledge also helps foster trust in the justice system, encouraging more victims to come forward and report their experiences. Ultimately, the goal of such training programmes is to strengthen the capacity of the justice sector to serve the needs of victims and effectively combat cybercrimes, contributing to a safer and more just society for all.

Implement a "Know Your Rights" campaign

Implementing "**Know Your Rights" campaigns** is a crucial step towards empowering individuals and ensuring they can access justice in the face of cybercrimes. These campaigns should aim to educate the public on the legal rights available to them when they experience cybercrimes and online harms, as well as the **steps they can take to seek justice**. Such campaigns can help break down the barriers of knowledge gaps and fear that often prevent victims from coming forward. By informing individuals of their right to privacy, protection from online abuse and the legal avenues available for redress, these initiatives foster greater confidence in the justice system and encourage reporting of cybercrimes. These campaigns should include information about **online safety**, such as recognizing potential online threats, protecting personal data and understanding privacy settings to ensure users can safeguard themselves while navigating the digital world.

To ensure a wide-reaching impact, campaigns should leverage diverse media platforms to communicate key messages across different demographics effectively. Traditional methods such as radio and SMS messages are valuable for reaching underserved and rural communities where Internet access may be limited. Social media and online platforms, on the other hand, offer an opportunity to engage younger, tech-savvy populations who may yet be more susceptible to online threats. The use of local languages, relatable scenarios and accessible messaging will further enhance the reach and effectiveness of these campaigns. Engaging community leaders, local influencers and stakeholders who have firsthand experience with cybercrimes can make these campaigns more relatable and impactful. This can also include the development of materials that highlight specific examples of cybercrimes, the potential consequences for perpetrators and the available legal remedies for victims.

CONCLUSION

As the digital landscape continues to expand, so too do the threats that accompany it—threats that, in many ways, risk undermining the very progress digitalization and technology promise. This is as true for Africa as it is for the rest of the world. Cybercrime is not just a technological challenge; it is a matter of justice. Cybercrime disproportionately affects the most vulnerable, often leaving victims without recourse and obstructing meaningful access to justice. Recognizing and addressing this reality is not just a policy consideration but a necessity for safeguarding fundamental rights in the digital age.

Through its focus on Namibia, Sierra Leone, South Africa and Uganda, this research reveals that while there are significant challenges to address cybercrimes, there is also a growing recognition of the need to empower victims and improve access to justice. While these findings stem from an analysis of these four countries, they reflect broader trends that are relevant across the continent. Issues such as underreporting, the lack of clear and accessible legal frameworks and inadequate training for justice sector stakeholders underscore the urgency of comprehensive reforms. However, the emerging positive practices, including educational initiatives, offer promising avenues for change. The recommendations provided—from developing model laws to enhancing public awareness campaigns and improving training for justice sector actors—lay the foundation for a more robust, victim-centred approach to tackle cybercrimes.

The journey ahead is one of collaboration and innovation. Regional and international partnerships can support the development of clear, accessible systems that ensure victims of cybercrimes are not only heard but can also pursue justice effectively. By fostering inclusive and proactive measures—such as improving digital literacy, enhancing reporting mechanisms and building the capacity of all stakeholders—we can move towards a future where victims are empowered, rights are safeguarded and justice is accessible for all.

unicri
United Nations
Interregional Crime and Justice
Research Institute

www.unicri.org