IRJCS: International Research Journal of Computer Science
Volume 12, Issue 07, September 2025
ISSN: 2393-9842
https://www.irjcs.com/archives

Criminal Uses of Information and Communication Technologies (ICTs) in Sub-Saharan Africa: Emerging Trends, Security Concerns, and Policy Perspectives

Ehigiator Egho-Promise
Department of Computing and Digital Tech.,
University College Birmingham, United Kingdom
eegho-promise@ucb.ac.uk
ORCID: https://orcid.org/0000-0001-8948-1813
George Asante
Department of Information Technology Education,
Akenten Appiah-Menka University of Skills Training and Entrepreneurial Development,
Kumasi, Ghana
gasante@aamusted.edu.gh
ORCID: https://orcid.org/0000-0001-8061-5387
Udoh Ekereuke
Department of Computing, QA Higher Education,
London, United Kingdom
ekereuke.udoh@qa.com
ORCID: https://orcid.org/0000-0003-1655-8829

Publication History
Manuscript Reference: IRJCS/RS/Vol.12/Issue07/SPCS10081|ResearchArticle | Open Access | Double-Blind Peer Reviewed Article ID: IRJCS/RS/Vol.12/Issue07/SPCS10081Received:24,August 2025,Revised:30,August 2025, Accepted: 10 September 2025 Published Online: 18 September 2025
http://www.irjcs.com/volumes/Vol12/iss-07/02.SPCS10081.pdf
Article Citation: Ehigiator,George,Udoh(2025),Criminal Uses of Information and Communication Technologies (ICTs) in Sub-Saharan Africa: Emerging Trends, Security Concerns, and Policy Perspectives **.** IRJCS: International Research Journal of Computer Science, Volume 12, Issue 07 of 2025 pages 260-271
doi:> https://doi.org/10.26562/irjcs.2025.v1207.02
BibTeX Ehiigiator@2025ICT

Abstract: This study explores the new trends, driving factors and governance challenges to cybercrime in Sub-Saharan Africa (SSA). This research employed a mixed-methods design, incorporating a survey, interviews, and a literature review. The results indicate that the cyber security situation is advanced and dynamic, with the extensive deployment of phishing, viruses, and personal imitation on social media, as well as practices targeting small firms, learning institutions, and the general population. Many of the survey participants attested that they had experience of ICT-related crimes, showing an increased exposure to cyber threats in industries. The research also points to the high relationship between unemployment among young people and their involvement in cybercrime. The regulatory issues are still a problem, as the majority of the participants view national systems against cybercrime as ineffective. These observations are supported by the interview information that highlights the following issues as common obstacles to cyber security: infrastructural gaps, inadequate regional co-operation, and insufficient institutional capability. Considering these results, the study recommends a multi-layered policy-technology framework that includes legal reform, technology innovation, collaboration between the government and the business, and residents' awareness to build cyber resilience in the region. The study makes a strong case for a concerted legal framework, cross-border collaboration, and digitally inclusive policies that can help in alleviating cyber risks and bringing security to the digital destiny of SSA.
Keywords: ICT, Cyber security, cybercrime, Sub-Saharan Africa, Criminal

INTRODUCTION

Rapid digitalization is underway across sub-Saharan Africa, transforming economies and daily life. Mobile phone ownership and internet connectivity have expanded significantly in the past decade. As of 2023, mobile penetration in sub-Saharan Africa had reached about 44% of the population, and roughly 27% of people were using mobile internet (GSMA Intelligence, 2025). A fintech revolution accompanies this mobile-driven connectivity boom; the region has seen an explosion in mobile money and digital payment services (Adewopo et al., 2025). By 2024, sub-Saharan Africa counted over one billion registered mobile money accounts (double the number in 2020), representing more than half of all mobile money wallets in the world (GSMA Intelligence, 2025; South African Times, 2025). Such growth in connectivity and financial technology has brought many benefits, improving access to services and economic inclusion for millions (Pantserev 2022).

However, the digital boom has also given rise to new forms of criminal activity leveraging information and communication technologies (ICTs). Both cyber-enabled crimes (traditional offences, such as fraud, theft, or extortion, conducted via digital tools) and cyber-dependent crimes (offences that exist only because of ICT, such as hacking or malware attacks) are on the rise. Criminals have been quick to exploit the expanding digital ecosystem, often outpacing users' awareness and defensive measures. Africa was the region with the highest number of weekly cyberattacks per organization in the world (Bhebe, 2022).

Threat actors ranging from lone hackers to syndicates have targeted the proliferation of mobile devices and online services. Their attacks include phishing scams, fraudulent mobile money transactions, ransomware attacks, and data breaches. Thus, alongside the opportunities from ICT growth, sub-Saharan African countries are confronting a new wave of security concerns in the digital realm (Mapiye et al. 2023).

Even though ICT has spurred socio-economic development in sub-Saharan Africa, it has also introduced new vulnerabilities. A growing reliance on digital platforms means that banking, communications, and other services are exposed to cyber risks. Criminal actors are adept at exploiting these vulnerabilities, often outpacing the ability of legal frameworks or security measures to adapt. Cybercrime is advancing faster than the capacity of many states to respond, with one report finding that 75% of surveyed African countries acknowledge their cybercrime laws and investigative resources need significant improvement (Atalayar, 2025).

Consequently, African economies collectively lose an estimated $4 billion each year to cybercriminal activities (Kshetri 2019). One illustration of the lag in response is the African Union's Malabo Convention on Cyber Security (adopted in 2014), which took nearly a decade to come into force and still lacks widespread ratification. These gaps underscore the need for a region-specific analysis of ICT-facilitated crimes in sub-Saharan Africa to understand emerging trends and to inform more effective, proactive responses. The main purpose of this study is to explore the criminal exploitation of ICTs in sub-Saharan Africa, assess emerging trends and security concerns, and propose strategic perspectives for mitigation. Specifically, the study seeks to**:**

- Identify and classify the major ICT-related crimes in sub-Saharan Africa.
- Analyse the socio-economic, legal, and technical factors contributing to the rise of digital crime in the region.
- Evaluate the effectiveness of existing policy, legal, and institutional responses to cybercrime in sub-Saharan Africa.
- Recommend multi-facet strategies for combating these ICT-facilitated criminal activities.

In this study, a case study is conducted on the nations chosen from sub-Saharan Africa, specifically Nigeria, Kenya, Ghana, and South Africa, to review the regional trend. It includes crimes that merely utilize the internet (cyber-enabled, e.g., online fraud, extortion, impersonation through digital platforms), as well as those that could not occur without the internet (cyber-dependent, e.g., hacking, malware attacks that rely on the existence of networked systems). Still, in either case, it is civilian (as opposed to state-sponsored) and financial (as opposed to online warfare) (Ganda 2024). It is worth noting a couple of limitations. Data on cybercrimes remains limited in most countries in Africa, which makes analysis difficult. The fact that the four countries were identified can be seen as a limitation to the generalisation of the study's results. Lastly, the rapidly developing aspect of technology implies that new threats may emerge within a short period. Thus, any recommendations may need to be reconsidered in light of the evolving digital landscape.

II. REVIEW OF RELATED STUDIES

2.1 ICT Development and Digital Transformation in Sub-Saharan Africa

In Sub-Saharan Africa, there have been significant developments in the area of ICTs, especially the high-speed growth in mobile broadband, digital identity, and online financial services, including mobile money platforms. These inventions have played a significant role in enhancing connectivity, financial access and accessibility to public amenities in towns and rural setups. Nevertheless, the area still has significant problems associated with infrastructure shortages and inadequate digital skills required to perform well in the new digital world. Consequently, despite an increase in the velocity of digital transformation, its unequal distribution is also a risk of further social and economic stratification.

2.2 Conceptualizing cybercrime

Cybercrime is a crime conducted through the application of digital technology to target individuals, organizations, or governments. The term covers a broad scope of offences that include cyber-dependent crimes (ones which could not have been committed without digital technology, like hacking and malware distribution), and cyber-enabled crimes (traditional types of crime, facilitated by technology, including fraud and identity theft) (Wall, 2024). Digital fraud is a branch of cybercrime characterized by deceptive actions aimed at gaining profits, including phishing, business email compromise (BEC), and mobile money fraud.Transnational cyber threats span national boundaries and complicate policing as they tend to span multiple countries with jurisdictional difficulties (UNODC, 2013). Diverse authorities have various classifications of cybercrime. The UNODC classifies cybercrimes as falling under the offences against the confidentiality, integrity and availability of data, computer-related fraud and content-related crimes (UNODC, 2013). Interpol, in turn, pays more attention to monetary online crimes, including cyber banking crimes and ransom ware. In contrast, the African Union (AU) emphasizes those issues that are peculiar to this region, i.e., mobile money fraud and SIM swap fraud (African Union, 2014). These typologies emphasize the dynamic character of cyber threats that requires flexible legal and policy solutions. The absence of a harmonized legal framework is regarded as the crucial difficulty in defining Cybercrime in Africa. Whereas specific laws have been introduced in countries, including Nigeria (Cybercrimes Act, 2015), Ghana (Cyber Security Act, 2020 (Act 1038)) and South Africa (Cybercrimes Act, 2020), some countries still have old penal codes that are not sufficient to compact new forms of cyber threat (Chawki et al., 2015). This discrepancy makes cross-border co-operation during investigation of cybercrimes difficult.

2.3 Trends in ICT-Related Crime in Africa

Along with the skyrocketing digital revolution in Africa, Cybercrime has skyrocketed. Unfortunately, email fraud, notably Business Email Compromise (BEC), is getting out of control as criminals pretend to be executives and authorize payroll redirection scams (Bisson, 2020). It is reported that African companies lose millions of dollars every year due to such scamming with the key areas being Nigeria, Ghana, and South Africa (Kaspersky, 2024). Other rising issues are mobile money fraud due to the inequalities in the authentication of systems such as M-Pesa and MTN Mobile Money (Kshetri, 2019). Social engineering frauds are employed by criminals to extract PINs or exploit the agent networks to divert money. In the same way, SIM swap scams, in which attackers steal the mobile phones of a given victim to circumvent two-factor authentication, have also risen in jurisdictions such as South Africa and Kenya (ITU, 2021). Romance scams and phishing are still among the most popular frauds because criminal attackers rely on playing with human emotions to cheat a victim. Also, there have been ransom ware-related takeovers of such critical services as healthcare and government systems, which were the case during the 2021 attack of the Kenya eCitizen portal (Interpol, 2021). There has also been the rise of a serious danger of social media manipulation, especially through the political arena. In elections in Nigeria and Kenya, there have been cases when disinformation campaigns affected the mass audience, which was organized both by internal and external forces. Those trends demonstrate the overlapping of technological weaknesses and socio-economic urges fuelling Cybercrime in Africa.

2.4 Theoretical Frameworks for Understanding Cybercrime

Various criminological theories aid in explaining the dynamics of Cybercrime in Africa. One of such theories is that of Routine Activity Theory: A motivated offender, a target, and the lack of a capable guardian come together, according to Cohen and Felson (1979). Applying to cybercrime, poor Cyber Security and low digital literacy will pose a risk to being victimized (Wang et al., 2021). As an example, the increase of phishing in Africa can also be explained by poor users' awareness and institutional protection. According to the General Strain Theory (Agnew, 1992), persons might resort to committing a crime when they see economic deprivation and fewer opportunities for achieving legitimate goals. The youth unemployment has been considered to have a relation with Cybercrime in Africa, specifically in Nigeria, in what has become known as the Yahoo Boys and involves under-employed youths committing cybercrimes as a means of survival (Chawki et al., 2015). Cybercrime may also be applied to the Technology Acceptance Model (TAM) (Davis, 1989), initially formulated to describe the adoption of new technologies by its users. Hackers use vulnerabilities in the usability of the systems, such as weak policies on password strength, to execute attacks. Nevertheless, Africa's research in cybercrime has been mainly based on the Western theoretical frameworks with limited local modification (Bada and Von Solms, 2019). In future studies, researchers ought to generate specific frameworks taking into consideration the reality of Africa as a special socio technical environment.

2.5 Legal and Policy Landscape on Cybercrime in Africa

Concerted challenges, such as poor cross-border co-operation and legally ineffective frameworks, are hampering efforts to curb cybercrimes in African countries. Although there have been enactments of some laws on cybercrimes in some countries, including the Cybercrimes Act (2015) in Nigeria and the Cybercrimes Act (2020) in South Africa, it is unevenly applied. The laws remain archaic in many countries without sufficient provisions to deal with the prevailing cyber threats. This is because, even though the African Union Malabo Convention (2014) aimed to standardise Cyber Security legislation on the continent, it has not come into effect yet in many countries, though it is effective in 15 of them as of 2023 (African Union, 2023). The inability to ascertain the technical and financial capacity to undertake measures towards Cyber Security is a major setback, especially in small economies. Internationally, the Budapest Convention (2001) provides international standards regarding the laws on cybercrimes, yet most countries in Africa do not comply with this convention due to issues with sovereignty (Radebe et al., 2024). Comparative evaluation shows that the legal systems of Africa are outdated in comparison with the rest of the world, especially in investigating the case of digital evidence and cooperation with other countries. To enhance the regional policies, it is essential to match the international best practices with realities in a particular region.

2.6 Research Gap in African Cybercrime Studies

Even though cybercrime has become an increasingly imminent risk, Africa has been faced with a deficiency of empirical studies as well as theoretical contextualization. The current body of research draws mostly on anecdotal rather than on systematic data collection. Also, there is a failure on the part of African leaders to have evidence-based policy on cyber security, as this tends to be reactive and thus ineffective. Even policymakers have to adopt foreign studies without the localized studies, resulting in models that may not suit the socio technical circumstances in the region (Kshetri, 2019). It is suggested that further studies should focus on local empirical studies and context-based theoretical formulations to come up with contextualized solutions to cyber security.

III. RESEARCH METHODOLOGY

The study employs a mixed methods design to assess the legislation and enforcement of cybercrime in the sub-Saharan region, utilising both qualitative and quantitative procedures to gain a comprehensive understanding of the problem (Creswell and Creswell, 2018).

3.1 Philosophy of the study and approach

This study is based on an interpretive paradigm that recognises the subjective character of the social phenomena and the critical role of context in human experiences (Saunders et al., 2019). The paradigm can be effectively applied when analysing cybercrime law, as it provides a detailed account of stakeholders' viewpoints, legal interpretations, and enforcement issues (Bryman, 2016).

A pragmatic approach is also included, which makes the research problem-focused and solution-oriented, situated between theoretical knowledge and practical policy execution (Morgan, 2014). The adopted mixed-methods approach leverages the advantages of both qualitative and quantitative studies (Creswell, 2014). The qualitative tools, namely interviews and policy analysis, provide informative and situational data on the legal and operational issues of cybercrime enforcement (Yin, 2018).Quantitative approaches and tools, such as surveys and statistical analysis, contributed to the identification of general trends and patterns of cybercrime victimization and general awareness (Field, 2018). The twofold strategy enhances the validity and reliability of the research results through methodological triangulation (Denzin, 2017).

3.2 Research Design

This study employs a multi-case research design, in which specific countries in sub-Saharan Africa are selected for a comparative analysis (Yin, 2018). The research combines three major methodological elements: research and analysis of laws and regulatory frameworks on cybercrime (Bowen, 2009); ethnography of digital methods, including observation of trends in cybercrime (Pink et al., 2016); and a survey approach using structured online questionnaires concerning ICT users (Fowler, 2013). The multi-faceted design of the study considered the case of cybercrime holistically, through the evaluation of macro-level policy and the assessment of micro-level user experiences (Patton, 2015).

3.3 Collection of Data

The primary data collection involves two approaches, namely semi-structured interviews of Cyber Security experts, law enforcers in charge of cybercrime, legal professionals, and victims of cybercrime, and online surveys of ICT and financial service consumers placed in a set of countries. The surveys employ the stratified sampling method, which aims to capture individuals with diverse demographic characteristics. In addition, various sources were utilized to gather secondary data, including Cybercrime Reports published by Interpol, ECOWAS, and national Computer Emergency Response Teams (CERTs). These reports provide statistical data on trends in cybercrime (Interpol, 2021). Legal Documents - Court decisions, laws, and policy statements were used to determine the legality of the process used in cybercrime. Archives and scholarly articles provide historical context and comparative applications to complement primary data.

3.4 Data Analysis

The data gathered is assessed using a combination of qualitative and quantitative methods. To recognise similarities between the interview transcripts and policy documents and extract themes, they were coded using NVivo software, and inductive coding was employed, allowing themes to emerge naturally rather than being imposed. Tools of statistics measure the responses of surveys to interpret the frequency, correlation, and other patterns involved in cybercrime victimisation (Field, 2018). Regression analysis was used to evaluate the interrelationship between variables (Tabachnick and Fidell, 2019). The methods of cross-case comparison distinguish common problems and regional variations in the matters of cybercrime law (Miles et al., 2014).

3.5 Ethics

The importance of ethical compliance in the research process was advocated. Informed consent was obtained from all participants after they had been provided with clear information about the study's purpose and their rights (Wiles et al., 2012). All data was scrubbed of personal identifiers to safeguard personal confidentiality, and magnetic data was stored securely following the GDPR specifications (GDPR, 2018). Institutional boards ethically evaluated the appropriateness of the study protocol in terms of research integrity.

3.6 Conclusion

The chapter has elaborated on the methodological perspective of the study, which is based on mixed methods with a greater focus on qualitative aspects to present depth and a quantitative scale to show breadth (Creswell and Creswell, 2018). The incorporation of policy analysis, digital ethnography, surveys, and cross-case a comparison ensures that the research on cybercrime legislation in sub-Saharan Africa is conducted robustly (Yin, 2018). Meanwhile, ethical concerns ensure that the safety and rights of participants are safeguarded during the research. The following sections present the resultant findings of this methodological process.

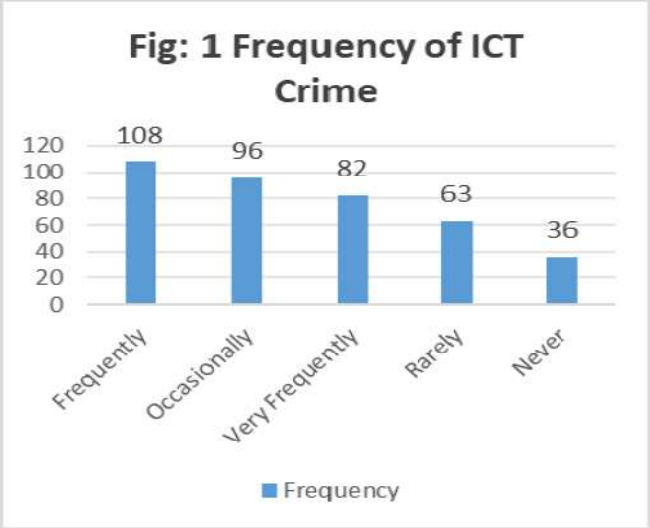
IV. ANALYSIS OF ICT-ENABLED CRIMES IN SUB-SAHARAN AFRICA

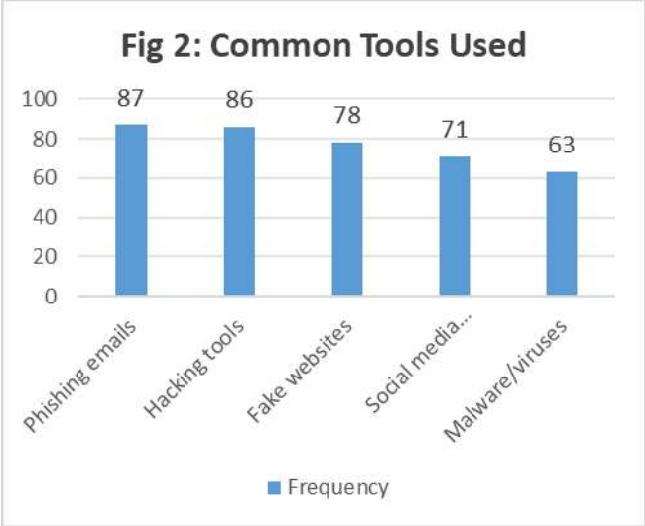
This section gives a multifaceted synthesis of essential findings of the study. It also discusses the efficacy of the regulatory framework, infrastructural shortages, and the magnitude of horizontality or verticality when it comes to addressing cyber threats. These insights form the basis of having governance priorities and developing a region-specific cyber security framework that is sensitive to the issues of the region.

4.1 Patterns and Trends of Criminal Use of ICT

The survey results indicate that 108 respondents expressed that ICT crimes happened frequently, 96 occasionally, and 82 very frequently, meaning cyber threats are a very present problem in the area. When it comes to tools employed by criminals, the most frequently mentioned ones were phishing emails (87 responses) and hacking tools (86), fake websites (78), and social media impersonation (71), which implies a combination of more technical and deception-related approaches. Regarding the primary targets, small businesses (84) and educational institutions (84) were the most common ones, and the general public (73), government institutions (72), and financial institutions (72) were also amongst the most targeted ones. These trends indicate the necessity to introduce multi-sector cyber security policies and nationwide digital literacy campaigns to reduce increased threats. Results from interview data demonstrate that financially motivated cyber crimes were reported most as ICT-enabled crimes without exception in Sub-Saharan Africa. The representatives of the companies repeatedly specified mobile money fraud, phishing attacks, SIM swap fraud, and business email compromise (BEC) to prevail, since the region is gradually transitioning towards the use of digital banking and financial services.

Such crimes are usually enabled by malware, fraudulent investment sites, and crypto fraud to attack an individual user as well as institutional systems. Coupled with monetary exploitation, there is anxiousness towards socially and politically manipulative cyber attacks, including social media impersonation, relationship fraud, online blackmail, and misinformation.





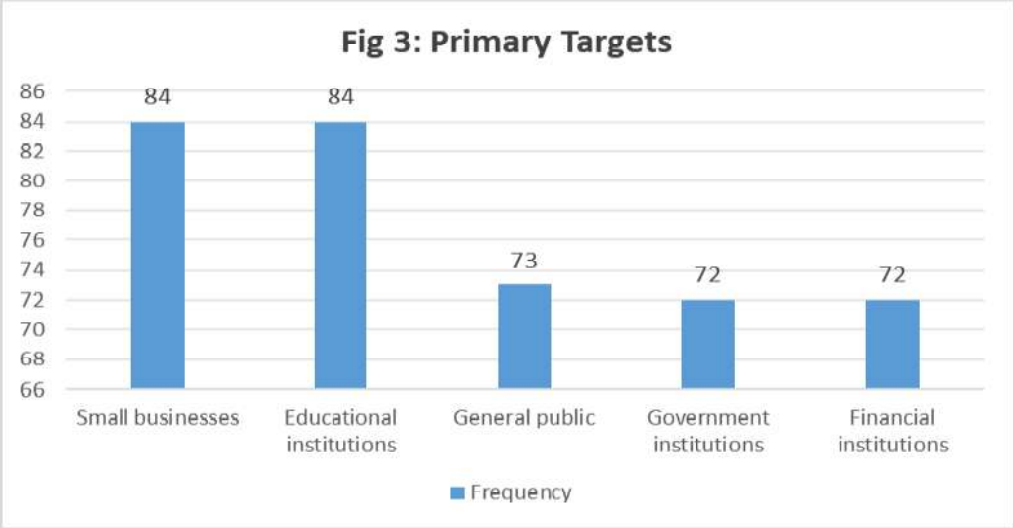


Table 1: Patterns and Trends of Criminal Use of ICT

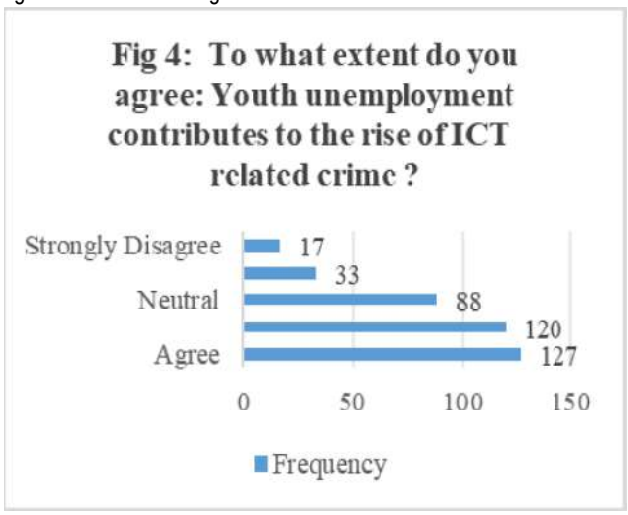
Theme	Key Insights Across Participants (P001–P010)
1. Financially Motivated Cybercrimes	• Mobile money fraud, phishing, business email compromise (BEC), and SIM swap fraud were reported in nearly every country (P001, P002, P003, P004, P005, P006, P007, P010). • Use of fake e-commerce websites, card-not-present fraud, and fake investment/crypto platforms also emerged as key trends. • Rise in ransom ware attacks targeting both private companies and critical infrastructure (P001, P002, P005, and P010).
2. Social and Politically Manipulative ICT Crimes	• Common reports of online impersonation, social media scams, and romance scams (P002, P003, P004, P006, P010). • Increasing cases of cyber defamation, blackmail, and social media blackmail (P004, P007, P008). • Political disinformation and deep fake content used for destabilization or influence during elections (P003, P009). • Website defacement and cyber stalking also noted (P007, P009).

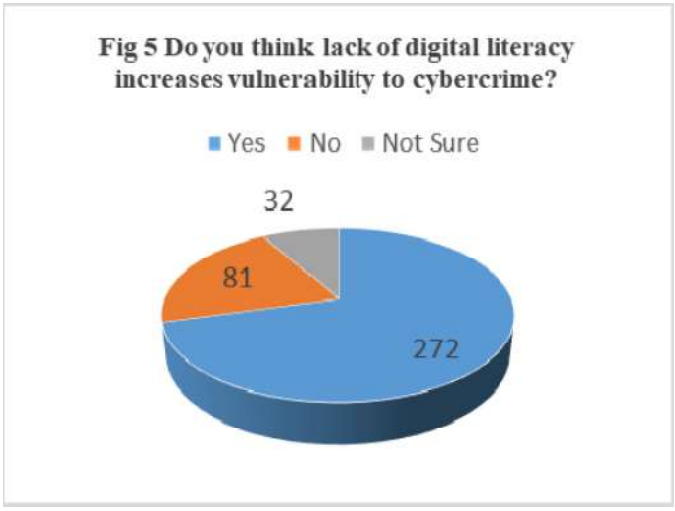
Specifically, another risk factor is the increasing use of ICTs with deep faking, cyber defamation, and politically fraught messages during campaigns, which is an aspect of exploiting the power of ICTs to bias the views and reputation or social damage of other persons.

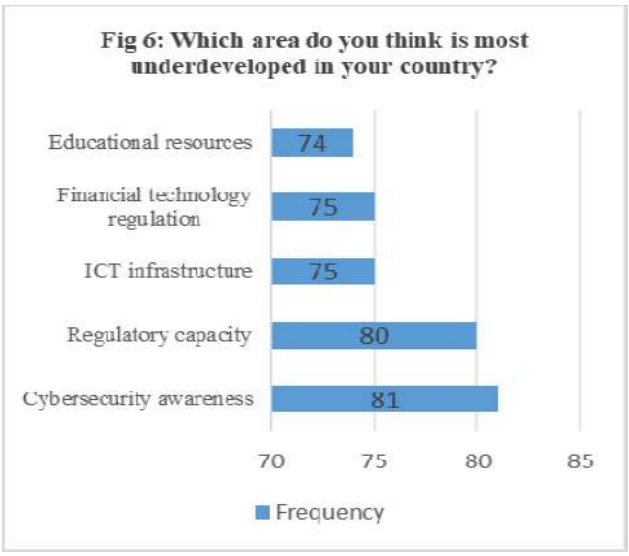
4.2 Socio-Economic and Infrastructural Factors

The statistics point to robust socio-economic and infrastructural issues associated with ICT crime in Sub-Saharan Africa. For instance, 247 people (127 Agree, 120 strongly Agree) agree that youth unemployment is a factor that leads to cybercrime, which testifies to long-term social insecurities. On the same note, 272 respondents agreed that the risk of cybercrime would be enhanced by the absence of digital literacy, which was an indicator that educational programs are urgently required.

Upon enquiry about the worst underdeveloped areas, at the lead were cyber security awareness (81) and regulatory capacity (80), indicating gross inadequacy, followed by ICT infrastructure (75) and fintech regulation (75).With regard to regulatory environment, 170 of the respondents rated the existing structures ineffective or very ineffective, whereas only 135 believed them effectual or very effectual. Hence, there is a common ground to be upset with a current state and an urgent need to change a structure.







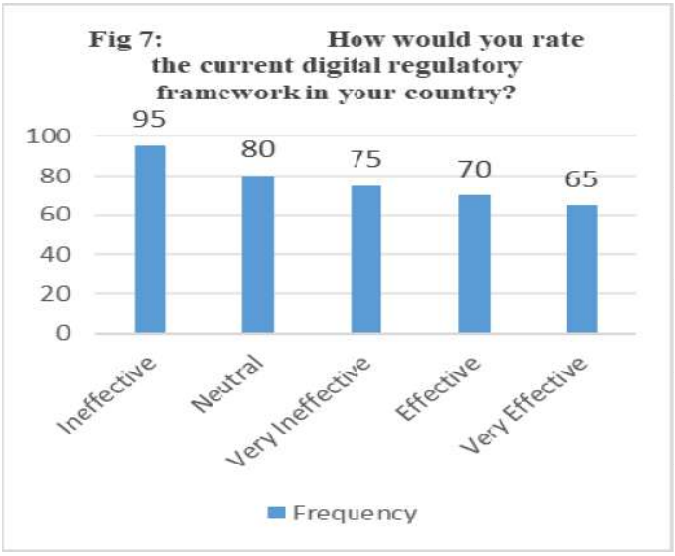


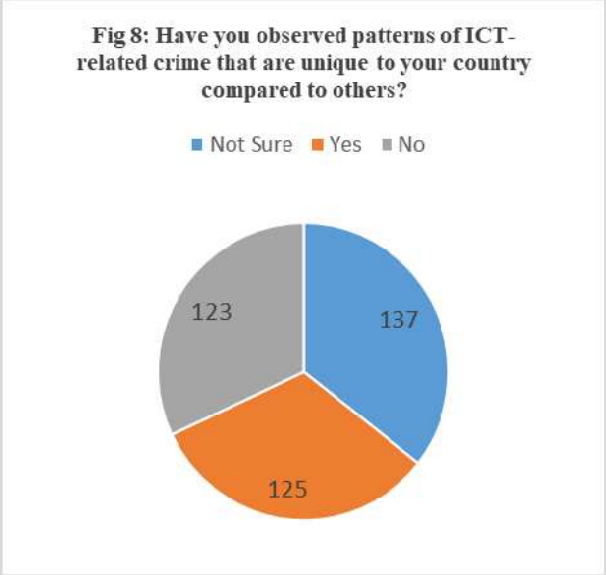
Table 2: Socio-Economic and Infrastructural Factors

Theme	Key Insights Across Participants (P001–P010)
1. Youth Unemployment and Economic Marginalization	• All participants (P001–P010) identified youth unemployment as a core driver. Digitally skilled but economically marginalized youth turn to cybercrime as a survival or enrichment strategy. • Economic frustration, poverty, and lack of alternative income sources are linked to criminal online activity (P002, P005, P006, P009).
2. Digital Illiteracy and Weak Cyber Security Ecosystems	• A lack of digital awareness among general users primarily rural populations and older citizens was highlighted by most participants (P001, P003, P004, P006, P007, P008). • Weak regulatory frameworks, outdated laws, and limited institutional capacity hinder cybercrime prevention (P001, P005, and P009). • Rapid digitalization without proportionate cyber security investment was frequently cited (P003, P004, P006).

Interview data highlights that there were two main drivers, youth unemployment and poor digital governance. Most respondents inferred massive unemployment among the youth as the primary trigger of the increasing cases of digital crime, where most technologically savvy yet jobless youths turned out to consider digital crime as an avenue to earn a living. Meanwhile, the already quick digitalization process in the region has outstripped both users and their state of being prepared and cyber security. Gap in digital literacy, especially among rural and aging groups, coupled with the low level of enforcement mechanisms, the outdated laws of cyberspace, and the lack of inter-agency coordination, has exposed both a person and an institution to attack. This socio-economic pressure, in combination with the infrastructural lapse, has brought up a climate where ICT-enabled crime can revive with little to no deterrence.

4.3 Case Study Insights

Figure 8reports the finding that 137 respondents said they were not sure about unique cybercrime patterns in their countries and this indicates the possibility of little local mappings of data or understanding. There is a relatively equal proportion of those who said Yes (125) and No (123), indicating uncertainty or non-clarity of whether there is a significant difference in national patterns.



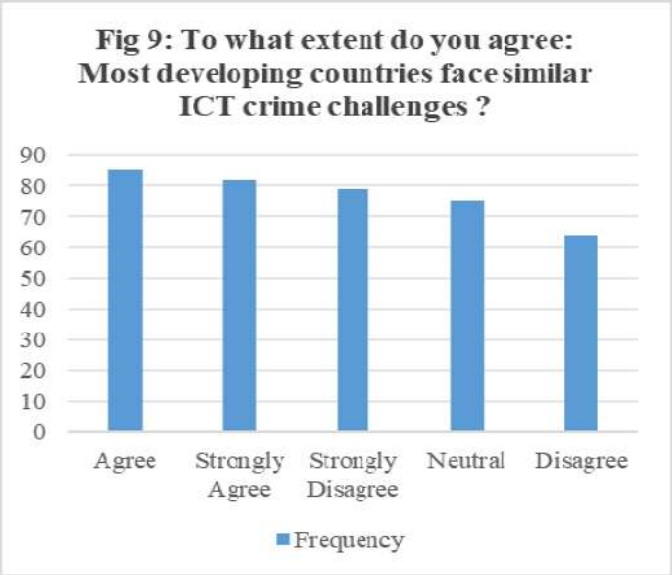


Figure 9 (overall 167 respondents: 85 Agree and 82 Strongly Agree) confirmed that all countries in Sub-Saharan Africa encounter similar challenges of cybercrime, and this area presents the possibility to develop regional co-operation among countries. However, there is a significant opposition of 79 respondents, who strongly disagree. This is an indication of the different experiences or perceptions of the respondents, something that may not go well with collaborative attempts in policies. As a final point, the results affirm the necessity and difficulty of unified cyber security operations in Sub-Saharan Africa. Although a considerable number of respondents also recognize generic challenges in the region, the high levels of uncertainty and inconsistency regarding local trends indicate a lack of situational sensibility and evidence-based analysis. This shows that before regional co-operation can be effective, there is a need to first invest in regional race to gain maturity in local cyber security intelligence, capacity build-up in cyber security, and local awareness to facilitate perception bridging and forge a united and informed front on the policy.

V. LEGAL AND POLICY ANALYSIS

5.1 Evaluation of National Cybercrime Laws

The threat of cybercrime has been recognized by the governments of Sub-Saharan African (SSA) countries in recent years, and they have already responded to this threat by taking measures to establish legal grounds to fight it. Even though there is legislation in most countries dealing with numerous cybercrimes, the quality, uniformity, and enforceability of such laws differ significantly. This produces a stitching together of legal tools that usually lack the sophistication required under the contemporary cyber threat environment. Certain nations have also done a good job in the legislation of crimes involving electronic crimes, identity theft, unauthorized access and data breach. Nevertheless, such laws are often too old and do not cover emerging forms of technology like malicious use of artificial intelligence (AI). Through the interview with experts, it has been identified that in all the countries, the presence of cybercrime laws is established (e.g. in Nigeria in 2015 , in Kenya in 2018, in Ghana in 2020), but due to the absence of the training of judges, inefficiencies of the procedure, and poor technical knowledge, implementation and enforcement are severely limited. Laws that have been rendered outdated or uncouth also paralyze prosecutorial effectiveness in certain states. There is an immense disjunction between law and working capability.

Table 3: Legal Framework

Country	Legal Framework	Key Weaknesses Noted
Kenya	Computer Misuse and Cybercrimes Act (2018)	Poor enforcement; weak digital evidence handling
Nigeria	Cybercrime Act (2015)	Silos among agencies; weak judicial capacity
Ghana	Cyber Security Act (2020)	Poor public awareness; lack of tech skills in judiciary
Ethiopia	Computer Crime Proclamation. No. 958/2016	Vague definitions; slow enforcement
Senegal	Cybercrime Law and Data Protection, 2008-11.	No coverage for new threats like crypto fraud
South Africa	Cybercrimes Act (2021)	Jurisdictional overlaps; interpretation inconsistencies
Rwanda	Cyber Security Law. No. 60/2018	Low rural enforcement; coordination challenges

Pantserev (2022) explains that although AI systems are being built to support development in the region, they are also used to conduct disinformation campaigns, automated fraud, and psychological manipulation, which national legislations pay little attention to. In addition, in a case where sufficient laws are enacted, implementation is still a problematic issue. The understanding of cybercrime laws and ability of the judges to interpret and enforce the laws is usually impoverished.

According to Abubakari (2021) and Malawi, Kumwenda et al. (2024), the widespread issues that have affected Anglophone West Africa are corruption, political manipulation, and poor execution of policies. The lack of ICT equipment distributed by the government (and thus available to the officers) often makes them uses personal handheld devices. This is not only a functional constraint of investigative abilities, but it is equally a thing that interferes with the professionalism and confidentiality of investigating sensitive cases involving crimes conducted via a computer. Nationalistic legislations against cybercrime are set to remain largely cosmetic, without regular training programmes and investment in digital infrastructure.

5.2 International and Regional Co-operation

Regional and international collaborations and measures in regard to Cyber Security have been established, but with patchy and, in most cases, symbolic growth. The African Union (AU) Malabo Convention, which was enacted in 2014, offers a detailed guideline in the field of Cyber Security, cybercrime law, and data protection. The strategies of most countries, as the Malabo Convention, ECOWAS, Interpol, and the African Union Cyber Security strategies, are beneficial. As revealed in the interview findings, there is a system in co-operation, little to no sharing of intelligence, slow exchanges of data and poor harmonization of national and regional legislations. Countries are still relatively minimal in terms of real-time co-operation, even when they have been involved in the forums.

Table 4: Common Challenges

Regional Body	Level of Support Observed	Common Challenges Identified
African Union	Provided frameworks like the Malabo Convention	Weak national alignment; non-ratification (e.g., Nigeria)
Interpol	Cross-border case support, training	Limited real-time coordination, slow data exchange
ECOWAS/EACO	Promoting legal harmonization and forums	No operational joint task forces or alert systems
Country Engagement	All countries participate at some level	Implementation and institutionalization remain weak

Nevertheless, as demonstrated by Pantserev (2022), the convention has not been ratified in many AU member states, and thus it is underutilized and without much influence. On the same note, regional economic blocs such as ECOWAS, Southern African Development Community (SADC) and East African Community (EAC) have come up with model laws and strategies to harmonize Cyber Security practices. These are the ECOWAS Directive on Combating Cybercrime and the SADC Model Law on Computer Crime and Cybercrime. Although these efforts are reasonable, inequality in the national priorities and resources is a barrier to their practical implications. According to Abubakari (2021), the existence of incoherence between national and regional regulations forms gaps that cybercriminals can use. Also, law enforcement interagency co-operation is often undone by the absence of trust, technological know-how, and the ability to talk to each other at the digital level. The co-operation with global organizations such as Interpol has not been very successful. Interpol has enabled combined efforts, capacity-building efforts, and development of tools to report cases of cybercrime.

5.3 Institutional Capacity and Challenges

Proper execution and using cybercrime policies and laws rely strongly on the institutional capability of the involved authorities. The sad thing is that most of the countries of SSA are really struggling in this aspect. Where they exist, National Computer Emergency Response Teams (CERTs) are frequently underfunded, understaffed, and ill-equipped with the infrastructure to react in real time to cyber incidents. The participants reported significant gaps in the national CERTs and law enforcement agencies. Cybercrime prevention and prosecution are hindered by lack of trained staff, inadequate funding, antiquated or non-existent digital forensics labs and low awareness in rural areas. It is not harmonized among the agencies that work inefficiently, and mistrust and confidentiality make the involvement of the private sector weak.

Table 5: Common Issues Raised

Challenge Area	Common Issues Raised	Countries Affected
Staffing and Training	CERTs and police are under-trained and overworked	All 10 participants (esp. Nigeria, Kenya)
Forensics and Tools	Lack of modern labs/tools; poor chain of custody	Ghana, Ethiopia, Senegal, Nigeria
Inter-agency Silos	Overlaps, rivalry, poor communication	South Africa, Nigeria, Rwanda
Reporting and Awareness	Victims do not trust the system or lack awareness	Senegal, Kenya, Ethiopia, Rwanda

The same case applies to law enforcement agencies. In 2024, it was discovered that police departments in Malawi, especially those in rural locations, such as Muloza, function without the basic resources in ICT (Kumwenda et al., 2024). Police officers have to utilize their cellphones to collect information and pursue cyber crimes. Not only does this undermine the integrity of investigations, but it shows that there is an impending need to invest systematically in cyber security resources and training. Another important problem is the absence of specialised training. According to Pantserev (2022), the ever-accelerating rate of threats in the sphere of cyber security demands continuous learning and upskilling, and this rarely appears in the priorities of the national budget. Lack of coordination of various national agencies is also compromised by budgetary limitations and loose governance systems. Absence of inter-agency co-operation and division of tasks leads to ineffective efforts aimed at addressing the issue of cybercrime; they will be scattered and chaotic.

VI. TOWARDS A FRAMEWORK FOR CYBER SECURITY AND PRIVACY GOVERNANCE

6.1 Proposed Model: Multi-Layered Policy-Technology Framework

To address the pressing cyber security challenges in SSA, a multi-layered framework combining legal, technological, and social interventions is essential (Egho-Promise et al, 2024). This approach must be grounded in local realities while being responsive to global cyber trends. Community Awareness: Raising awareness among citizens is crucial in reducing the human vulnerabilities exploited by cybercriminals. Kumwenda et al. (2024) found that many people are already using mobile phones for crime reporting and community safety, but lack guidance on how to identify and report digital threats. Public education campaigns can empower individuals to use technology safely and report suspicious activity. Legal Reform: Outdated and inconsistent legal frameworks must be revised and harmonised. As Abubakari (2021) argues, effective cybercrime legislation requires not only technical accuracy but also political independence. Legal reform should be guided by regional frameworks like the Malabo Convention and supported by international best practices. Tech Innovation: SSA countries must also invest in local technological innovation. Roger et al. (2022) and Wang et al. (2023) both highlight the role of ICT in improving agricultural productivity, governance, and economic resilience. Home-grown technologies can be tailored to local needs and offer scalable solutions for both development and security. International Partnerships: Collaboration with global institutions such as the World Bank and Interpol can provide much-needed technical expertise, funding, and policy guidance. Salimi (2025) notes that during the COVID-19 pandemic, the World Bank shifted its education strategy in SSA to include multimodal ICT solutions, a model that could be replicated in the cyber security sector.

6.2 Stakeholder Engagement

Appropriate governance of Cyber Security includes the assistance of various stakeholders. Digital threats are complex and dynamic, and require more than governments to solve them. Public-Private Co-operation Companies in the telecom sector, banks and information technology companies can work closely with the government, and this will result in more secure systems in place. Kumwenda et al. (2024) reveal that in Malawi, citizens frequently use telecoms to report their crimes. Rationalising these types of other-than-formalised co-operation is possible to improve responsiveness and efficiency. Universities, Telecoms, and NGOs also have a role to play. Universities can play a key role in training digital skills and in policy research, as well as through partnerships with NGOs. NGOs may also contribute as a useful community outreach and digital literacy campaign agent. As stated by Mapiye et al. (2023) and Cordes and Marinova (2023), the culture of inclusive ICT access, especially in agriculture and e-commerce, would call in a web of informed and motivated players that operate across fields.

6.3 Technology as Enabler and Protector

Technology should not only be considered an essential developmental tool but also as a way of protecting against cyber threats. New technologies have a great promise of enhancing security, transparency, and privacy. Such technologies include Artificial Intelligence, Blockchain, and Digital Forensics. Artificial intelligence tools are already implemented in the sphere of education and crime investigation. Salimi (2025) describes the possibility of AI and blockchain to guarantee equal access to digital education, whereas Kumwenda et al. (2024) talk about the opportunity of digital forensics to improve investigations of police work. Privacy-Preserving Tool and Mobile Security Apps also play a role. In SSA, mobile phones are the leading way of getting online, and, therefore, it is important to provide their security. Mobile applications that are secure can guard personal information, promote safe financial operations, and lead to service availability. Wang et al. (2023) and Botchie et al. (2022) stated that mobile technologies have already altered such sectors as agriculture and mobile finance, and now they have to defend them, too. Due to the digital journey of Sub-Saharan Africa, tremendous possibilities await the region, but it also puts it in grave Cyber Security danger. Existing law and the abilities in institutions are not entirely prepared to deal with the increasingly complex environment of threats. However, a multi-layered approach based on such aspects as legal reform, education of the population, innovative technology, and international co-operation has an opportunity to start the formation of a sustainable, inclusive, and secure digital landscape in SSA. Cyber Security cannot be considered a specialized problem anymore; it is a fundamental element of national progress, human security and integration of the continent. In the absence of it, the prospect of digital inclusion might not be achieved.

VII. DISCUSSION

7.1 Interpreting Key Findings

7.1.1 Alignment with or Divergence from Global Cybercrime Patterns

The findings of this study reveal that despite a series of similarities between Sub-Saharan Africa (SSA) and the rest of the world regarding cybercrime patterns, which include financial crime motives, phishing attacks, and ransom ware, there are significant discrepancies that relate to the context of the region. And that is, Its socio-economics, and infrastructure (Talesh, 2025). Similarly to international trends, the digital financial channels like mobile money are usually misused; however, only their introduction rate is by far higher in SSA because most of the population is under banked (Kitimbo, 2021). In this regard, the social engineering concept, such as romance fraud and social networking fraud, also matches trends spotted worldwide (Chaganti et al., 2021), but is more socially widespread because of the lack of control and digital visibility recognition. Moreover, as opposed to other more advanced areas, where cybercrime is, in the majority, transnational and highly organized, in SSA, they are much more often committed by persons lacking economic and political power or by loosely structured groups. This is based on the very correlation between the high youth unemployment rates and the issue of increasing cases of digital criminality, which was revealed in interviews and survey findings (Idris, and Maikomo, 2024). Ineffective enforcement, stale laws, and underfunded institutions are a strong indicator of a marked contrast between the regions that have more established Cyber Security landscapes (Testart Pacheco, 2016; Ali, 2024).

7.1.2 Region-Specific Challenges and Solutions

There are several region-related challenges faced by SSA which foster its susceptibility to cybercrime.

Among them are ineffective or aged legal basis, acute deficiency of qualified staff in the law enforcement community or the judicial community, lack of coordination among agencies, and poor investment in Cyber Security infrastructure (Longe et al., 2009; Tahiru, 2018; Mphatheni and Maluleke, 2022; Walumoli, 2021). Moreover, there were also problems of poor digital literacy, especially in people living in the country and among older adults, which has been discovered to be strongly related to resistance to digital fraud. A biased topography of national and regional collaboration is also pointed out in the study. Although there is a framework like the Malabo Convention led by the AU and the ECOWAS model laws, the low level of ratification and implementation shows a governance gap (Ewulum, 2023; Uebel, 2025). Specific solutions to cybercrime in the region should thus encompass synchronised cybercrime laws, strategic investments in digital forensics and capacity building at the ground level (Adel, 2020). Most importantly, regional Cyber Security has to be made specific to institutional and socio-economic vulnerabilities in a multi-layered policy-technology framework as it has been suggested in Section 6.

7.2 Implications for Policy and Practice

7.2.1 for Governments

Governments need to revise and align their legislation on cybercrime with the recent cyber-related threats, including AI-enabled fraud and cryptocurrency-related scams. Special financing must be used to train the judges, police officers, and prosecutors on digital forensic and evidence processing. They need improved coordination of the agencies, and national CERTs should be treated as hubs of national intelligence and response to cybercrime.

7.2.2 For the Technology Sector

The tech industry, including Internet Service Providers (ISPs), fintechs, and telecoms businesses and sectors, should be incorporated intothe national Cyber Security approach in order to create a secure platform and exchange intelligence. There should be incentives offered to local startups and Research and Development (R&D) institutions to produce scalable, contextually appropriate Cyber Security tools (e.g., mobile applications to detect fraud or rural cyber awareness). There is a need to make investments in the firm and secure ICT infrastructure, especially in rural and peri-urban regions.

7.2.3 For Educational Institutions and NGOs

Universities, schools and non-governmental organizations should be at the forefront with regard to region-wide programs on digital literacy in the fields of online safety, privacy, and wise use of ICT. The topic of Cyber Security awareness should be included in school programs and college classes to create long-lasting resilience. NGOs have to be activated as intermediaries to cyber education and grassroots response, especially in regions with a poor institutional base.

VIII. CONCLUSION

This study has provided comprehensive details, trends, perpetrators and facilitating factors about ICT-based crimes in Sub-Saharan Africa (Horyey and Odei-Mensah, 2025). This study affirms that cybercrime is not only prevalent in the region but is also becoming more advanced. Two major categories of crimes dominated, namely, felonies committed with financial goals in mind, like phishing, SIM swap fraud, stealing money with the use of mobile phones and ransom ware and crimes that manipulate people and politicians socially and politically, including romance scams, cyber defamation, online impersonation and disinformation campaigns, especially during elections. Such crimes are committed mainly by youth who are digitally literate but economically marginalized, and they are taking advantage of the systemic vulnerabilities as well as the adoption of digital technologies. This kind of act usually has a cause, and it is known to be caused by unemployment, poverty, and legitimate economic opportunities. Weaknesses in infrastructure allow the occurrence of crime, including old Cyber Security laws, insufficiently equipped law enforcement agencies, and a high level of digital illiteracy, especially in rural areas and among ageing demographics. Institutional intervention is frenzied. The legal frameworks are sometimes present but not well-implemented, or misapplied, compared to new threats like fraud or crimes with AI or crypto currencies. Regional and international frameworks of cooperation, such as the Malabo Convention by the AU and Interpol systems, are in existence, but their application is habitually poor and mostly cosmetic. Overall, the study noted that there is an urgent requirement for properly structured, well-funded, and situation-specific Cyber Security policies.

REFERENCE

1. Abubakari, Y. (2021). The reasons, impacts and limitations of cybercrime policies in Anglophone West Africa: A review. PrzestrzeńSpołeczna, 1(1/2021 (21).
2. Adel, A., (2020). Developing a Digital Forensic Capability for Critical Infrastructures: An Investigation Framework'. Auckland University of Technology.
3. Adewopo, V. A., Azumah, S. W., Yakubu, M. A., Gyamfi, E. K., Ozer, M., and Elsayed, N. (2025). Comprehensive analytical review of cybercrime and cyber policy in West Africa. Journal of Electrical Systems and Information Technology, 12(1), 1-23. https://doi.org/10.1186/s43067-025-00216-x
4. African Union. (2014). African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention).
5. Agnew, R. (1992). Foundation for a General Strain Theory of Crime and Delinquency. Criminology, 30(1), 4787. https://doi.org/10.1111/j.1745-9125.1992.tb01093.x
6. Ali, M.D.J., (2024). Cybercrime and Cyber Security: A Critical Analysis of Legal Frameworks and Enforcement Mechanisms. Bharati International Journal of Multidisciplinary Research and Development, 2(8), pp.137-154. https://doi.org/10.70798/Bijmrd/020800017

7. Atalayar (2025). Interpol warns of rise in cybercrime in Africa, Atalayar. Available at: https://www.atalayar.com/en/articulo/new-technologies-innovation/interpol-warns-of-rise-in-cybercrime-in-africa/20250628190000216267.html (Accessed: 3 July 2025).
8. Bada, M., and Von Solms, B. (2019). A Review of Cybercrime in Africa. Journal of Cyber Security, 5(1).
9. Balisane, H., Egho-Promise, E., Lyada, E., Aina, F., Sangodoyin, A., & Kure, H. (2024). The effectiveness of a comprehensive threat mitigation framework in networking: A multi-layered approach to cyber security. International Research Journal of Computer Science, 11(06), 529-538. https://doi.org/10.26562/irjcs.2024.v1106.03
10. Bhebe, Q. P. (2022). Social Media and National Security in Sub-Saharan Africa: the case of Zimbabwe (2000-2017) (Doctoral dissertation, University of Johannesburg). Available at: https://ujcontent.uj.ac.za/view/pdfCoverPage?instCode=27UOJ_INSTandfilePid=139329920007691and download=true
11. Bisson, D. (n.d.). FBI Pegs 2020 Cybercrime Costs at $4 Billion - Actual Losses Likely Higher. [online] www.cybereason.com. Available at: https://www.cybereason.com/blog/fbi-pegs-2020-cybercrime-costs-at-4-billion
12. Botchie, D., Sarpong, D., and Meissner, D. (2022). Chain upgrading, technology transfer, and legitimacy: The Schumpeterian character of China in the information and communication technology sector in SSA. Technological Forecasting and Social Change, 183, 121898. https://doi.org/10.1016/j.techfore.2022.121898
13. Bowen, G. A. (2009). Document analysis as a qualitative research method. Qualitative Research Journal, 9(2), 27-40.
14. Bryman, A. (2016). Social research methods (5th ed.). Oxford University Press.
15. Chaganti, R., Bhushan, B., Nayyar, A. and Mourade, A., (2021). Recent trends in social engineering scams and a case study of gift card scam. arXiv preprint arXiv:2110.06487.
16. Chawki, M., Darwish, A., and Khan, M. A. (2015). Cybercrime in Africa: A Critical Review. Springer.
17. Cohen, L. E., and Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. American Sociological Review, 44(4), 588608. https://doi.org/10.2307/2094589
18. Cordes, D. L., and Marinova, D. (2023). Systematic literature review of the role of e-commerce in providing pathways to sustainability for poverty alleviation in Sub-Saharan Africa. Discover Sustainability, 4(1), 7. https://doi.org/10.1007/s43621-022-00109-3
19. Creswell, J. W. (2014). Research design: Qualitative, quantitative, and mixed methods approach (4th ed.). Sage.
20. Creswell, J. W., and Creswell, J. D. (2018). Research design: A qualitative, quantitative, and mixed method approaches (5th ed.). Sage. https://doi.org/10.4135/9781071817942
21. Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quarterly, 13(3), 319340. https://doi.org/10.2307/249008
22. Egho-Promise, E., Lyada, E., & Aina, F. (2024). Towards improved vulnerability management in digital environments: A comprehensive framework for cyber security enhancement. International Research Journal of Computer Science, 11(05), 441-449. https://doi.org/10.26562/irjcs.2024.v1105.01
23. Ewulum, C., (2023). The legal regime for cross-border data transfer in africa: a critical analysis. Available at SSRN 4546964.
24. Field, A. (2018). Discovering statistics using IBM SPSS Statistics (5th ed.). Sage.
25. Fowler, F. J. (2013). Survey research methods (5th ed.). Sage. https://doi.org/10.4135/9781452230184
26. Ganda, F. (2024). The influence of democracy, corruption, economic growth and ICT on carbon emissions in Sub-Saharan African countries: does FDI matter?. Journal of Open Innovation: Technology, Market, and Complexity, 10(3), 100324. https://doi.org/10.1016/j.joitmc.2024.100324
27. GDPR. (2018). General Data Protection Regulation. European Union.
28. GSMA Intelligence (2025) GSMA Intelligence, GSMA Intelligence. Available at: https://www.gsmaintelligence.com/research/research-file-download?reportId=50121andassetId=12080.
29. Horvey, S. S., and Odei-Mensah, J. (2025). Towards economic growth in Sub-Saharan Africa: is there a synergy between insurance market development and ICT diffusion?. Information Technology for Development, 31(1), 178-205. https://doi.org/10.1080/02681102.2024.2361478
30. Idris, M. and Maikomo, J.M., (2024). Impact of digital economy on youth unemployment in Nigeria. KASU Journal of Economics and Development Studies, 10(2), pp.25-38.
31. Interpol. (2021). Global cybercrime report.
32. ITU (2025). Global Cyber Security Index. [online] Available at: https://www.itu.int/pub/D-STR-GCI.01-2021
33. Kaspersky (2024). Cyberthreat landscape in Africa: risks and opportunities. [online] /. Available at: https://www.kaspersky.com/about/policy-blog/cyberthreat-landscape-in-africa-risks-and-opportunities
34. Kitimbo, A., (2021). Mobile money and financial inclusion of migrants in sub-Saharan Africa. In Research handbook on international migration and digital technology (pp. 251-266). Edward Elgar Publishing. https://doi.org/10.4337/9781839100611.00029
35. Kshetri, N. (2019) 'Cybercrime and Cyber Security in Africa', Journal of Global Information Technology Management, 22(2), pp. 77–81. https://doi.org/10.1080/1097198X.2019.1603527
36. Kumwenda, D., Tembo, M., Mphande, C., Nundwe, V., and Chazema, T. A. (2024). Digital Defiance's Affecting Use of Information Communication Technology Deployed for Prevention and Detection of Crime in Community Policing in Malawi. American Journal of Applied Scientific Research, 10(2), 24-34. Available at: https://doi.org/10.11648/j.ajasr.20241002.11

37. Longe, O., Ngwa, O., Wada, F., Mbarika, V. and Kvasny, L., (2009). Criminal uses of information & communication technologies in sub-Saharan Africa: trends, concerns and perspectives. Journal of Information Technology Impact, 9(3), pp.155-172.
38. Mapiye, O., Makombe, G., Molotsi, A., Dzama, K., and Mapiye, C. (2023). Information and communication technologies (ICTs): The potential for enhancing the dissemination of agricultural information and services to smallholder farmers in sub-Saharan Africa. Information Development, 39(3), 638-658. Available at: https://repository.up.ac.za/bitstream/handle/2263/90587/Mapiye_Information_2023.pdf?sequence=1
39. Miles, M. B., Huberman, A. M., and Saldaña, J. (2014). Qualitative data analysis: A methods sourcebook (3rd ed.). Sage.
40. Morgan, D. L. (2014). Pragmatism as a paradigm for social research. Qualitative Inquiry, 20(8), 1045-1053. https://doi.org/10.1177/1077800413513733
41. Mphatheni, M.R. and Maluleke, W., (2022). Cyber Security as a response to combating cybercrime: Demystifying the prevailing threats and offering recommendations to the African regions. International journal of research in business and social science, 11(4), pp.384-396. https://doi.org/10.20525/ijrbs.v11i4.1714
42. Pantserev, K. A. (2022). Malicious use of artificial intelligence in Sub-Saharan Africa: Challenges for Pan-African Cyber Security. Vestnik RUDN. International Relations, 22(2), 288-302. https://doi.org/10.22363/2313-0660-2022-22-2-288-302
43. Patton, M. Q. (2015). Qualitative research and evaluation methods (4th ed.). Sage.
44. Pink, S., Horst, H., Postill, J., Hjorth, L., Lewis, T., and Tacchi, J. (2016). Digital ethnography: Principles and practice. Sage.
45. Radebe, F.M. and Njenga, K., 2024. Bibliometric mapping of scientific production and conceptual structure of cyber sextortion in Cyber Security. Social Sciences, 14(1), p.12. https://doi.org/10.3390/socsci14010012
46. Roger, M., Shulin, L., and Sesay, B. (2022). ICT development, innovation diffusion and sustainable growth in sub-Saharan Africa. Sage Open, 12(4), https://doi.org/10.1177/21582440221123894
47. Salimi, F. (2025). Aligning policy and practice: The World Bank's approach to EdTech in Sub-Saharan Africa. Policy Futures in Education, 14782103251324275. Available at: https://doi.org/10.1177/14782103251324275
48. Saunders, M., Lewis, P., and Thornhill, A. (2019). Research methods for business students (8th ed.). Pearson.
49. South African Times (2025) Africa Surpasses One Billion Mobile Money Wallets, Trading $1 Trillion in 2024, The Southern African Times. Available at: https://southernafricantimes.com/africa-surpasses-one-billion-mobile-money-wallets-trading-1-trillion-in-2024/ (Accessed: 3 July 2025).
50. Tabachnick, B. G., and Fidell, L. S. (2019). Using multivariate statistics (7th ed.). Pearson.
51. Tahiru, A., (2018). Cyber Security in Africa: The Threats and Challenges!. Cyberpolitik Journal, 3(5), pp.91-104.
52. Talesh, S.A., (2025). Insuring Cyberinsecurity: Insurance Companies as Symbolic Regulators. Univ of California Press. https://doi.org/10.1525/luminos.243
53. Testart Pacheco, C.A., (2016). Understanding the institutional landscape of cyber security (Doctoral dissertation, Massachusetts Institute of Technology). https://doi.org/10.2139/ssrn.2756608
54. Uebel, I.A.I., (2025). Intervention & Regional versus Global Governance: A Case Study Analysis of UN, AU & ECOWAS Legal Framework in the Mali Conflict.
55. United Nations: United Nations Office on Drugs and Crime (UNODC) (2013). COMPREHENSIVE STUDY ON CYBERCRIME - Draft February 2013. [online] Available at: https://www.unodc.org/documents/organized-rime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.
56. Wall, D.S., 2024. Cybercrime: The transformation of crime in the information age. John Wiley and Sons.
57. Walumoli, B., (2021). A Critical Analysis of the Challenges Facing Counter cybercrime in 21st Century Africa: a Focused Comparison of Kenya and Rwanda (Doctoral dissertation, University of Nairobi).
58. Wang, J., Lin, Q., and Zhang, X. (2023). How does digital economy promote agricultural development? Evidence from Sub-Saharan Africa. Agriculture, 14(1), 63. https://doi.org/10.3390/agriculture14010063
59. Wang, S.Y.K. and Hsieh, M.L., 2021. Digital robbery: ATM hacking and implications. Springer Nature. https://doi.org/10.1007/978-3-030-70706-4
60. Wiles, R., Crow, G., Heath, S., and Charles, V. (2012). Anonymity and confidentiality. In The SAGE handbook of interview research (pp. 537-554).
61. Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed.). Sage.