INTERPOL

INTERPOL AFRICA CYBERTHREAT ASSESSMENT REPORT 2025

4TH EDITION

MAY 2025

LEGAL DISCLAIMER

TABLE OF CONTENTS

Foreword by INTERPOL	**4**
Foreword by AFRIPOL	**5**
Acknowledgement	**6**
Executive Summary	**7**
1. Introduction	**9**
2. The evolving cyberthreat landscape in Africa	**10**
3. Cyberthreat Trends and Insights across African sub-regions	**20**
4. Challenges in combating cybercrime in Africa	**23**
5. Positive developments in Africa's Cybersecurity landscape	**26**
6. Recommendations and conclusion	**30**
About INTERPOL	**33**

Neal Jetton
Director, Cybercrime Directorate
INTERPOL

FOREWORD BY INTERPOL

The African continent stands at a critical juncture in its digital evolution. As connectivity deepens and digital innovation accelerates, so too does the complexity of the cyberthreats facing the region. These threats are not constrained by borders - they are transnational, fast-moving, and increasingly sophisticated. They target the very infrastructure that underpins progress: financial systems, public services, critical infrastructure, and, most importantly, the trust of citizens in the digital future.

This fourth edition of the INTERPOL Africa Cyberthreat Assessment provides a vital snapshot of the current situation. Informed by operational intelligence, extensive law enforcement engagement, and strategic private-sector collaboration, it paints a clear picture of a threat landscape in flux where malware, especially ransomware, online scams including via phishing, as well as business email compromise, continue to dominate, while emerging dangers like AI-driven fraud, online image based sexual abuse and digital sex crimes, and cybercrime-as-a-service demand urgent attention.

At INTERPOL, we recognize that no single agency or country can face these challenges alone. The scale and speed of cybercrime demand a unified, coordinated, and intelligence-led response. Through the Africa Joint Operation against Cybercrime (AFJOC), and in close partnership with AFRIPOL, we are strengthening operational capabilities, deepening trust between national cybercrime units, and fostering the kind of cross-border cooperation that makes meaningful disruption of cybercriminal networks possible.

This report also reflects the growing resilience and capability across African law enforcement. From successful regional operations to new legislative reforms and capacity-building efforts, progress is being made. Yet, the road ahead remains long. Gaps in digital literacy, legislative harmonization, investigative resources, and access to digital evidence continue to challenge effective enforcement.

To all our partners - whether in law enforcement, government, industry, or civil society - this report is both a call to action and a foundation for collaboration. It is only by working together, sharing knowledge, and building trust across borders and sectors that we can secure Africa's digital future.

I extend my sincere appreciation to the African Cybercrime Operations Desk and all those who contributed to this report. Your efforts reinforce our collective resolve to build a safer, more resilient digital environment for all. Lastly, I would like to thank the law enforcement community of our African member countries for their dedication to combatting cybercrime and making the world a safer place.

Amb. Jalel Chelba
Acting Executive
Director of AFRIPOL

FOREWORD BY AFRIPOL

The African continent is entering an era of rapid digital transformation, bringing unprecedented opportunities for the economic, social, and institutional development of its Member States. This momentum reflects a collective commitment to accelerating digital inclusion, improving public services, and fostering local innovation. However, this major progress also comes with growing and sophisticated threats in cyberspace, which endanger the security of states, critical infrastructure, businesses, and African citizens.

In the face of these complex challenges, AFRIPOL stands as a leading continental organization in developing a coordinated, ambitious, and context-specific response tailored to African realities. Our commitment is clear: to promote strong digital sovereignty capable of effectively protecting our societies against increasingly ingenious cyberthreats, often transnational in nature and evolving as rapidly as the technologies themselves.

In 2024, AFRIPOL intensified its efforts through close cooperation with INTERPOL, specialized regional structures, national security agencies, and strategic private sector partners. Major joint operations, such as Operation Serengeti, led to the dismantling of sophisticated criminal networks specializing in ransomware, financial fraud, targeted phishing, and attacks on government information systems. These operational successes highlight the importance of inter-agency cooperation, information sharing, capacity pooling, and coordinated continental response.

In parallel, AFRIPOL continued to strengthen the skills of law enforcement personnel through specialized and targeted training programs, covering key areas such as criminal intelligence analysis, tracing illicit financial flows, digital investigations, cyber surveillance, and the protection of critical infrastructure. The strategic agreements signed with Kaspersky and Group-IB in 2024 marked a decisive step in our commitment to equipping Member States with the necessary resources to prevent and respond to major incidents, through enhanced access to technological tools, threat intelligence, and international expertise.

In 2025 and beyond, AFRIPOL will focus its efforts on three strategic priorities: (1) further strengthening international and inter-African cooperation to build a unified response to transnational threats; (2) closely supporting Member States in scaling up their operational, human, and technological capacities; and (3) systematically integrating emerging innovations, particularly artificial intelligence and blockchain technologies, to anticipate risks and adapt our strategies in real time.

Cybersecurity is not merely a technical issue; it has become a fundamental pillar of stability, peace, and sustainable development in Africa, as outlined in Agenda 2063. It directly concerns the digital sovereignty of states, the resilience of our institutions, citizen trust, and the proper functioning of our economies. It is in this spirit of shared responsibility, continental solidarity, and continuous innovation that AFRIPOL renews its commitment to building a secure, inclusive, sovereign, and resilient African cyberspace serving peace, security, and collective progress.

ABBREVIATIONS AND ACRONYMS

AFJOC	African Joint Operation against Cybercrime
AFRIPOL	African Union Mechanism for Police Cooperation
AI	Artificial Intelligence
APK	Android Package Kit
AU	African Union
BEC	Business Email Compromise
CaaS	Cybercrime-as-a-Service
CEO	Chief Executive Officer
CSAM	Child Sexual Abuse Material
DDoS	Distributed Denial of Service
ESCCOM	Eswatini Communications Commission
FCDO	Foreign, Commonwealth and Development Office
GB	Gigabyte
GEPF	Government Employees Pension Fund (South Africa)
ICT	Information and Communication Technology
MLA	Mutual Legal Assistance
OIBSA	Online Image Based Sexual Abuse
SIM	Subscriber Identity Module
SMS	Short Message Service
TB	Terabyte
UAE	United Arab Emirates
UK	United Kingdom
UN	United Nations
UNESCO	United Nations Educational, Scientific and Cultural Organization
USD	United States Dollar

ACKNOWLEDGEMENT

This report was drawn up by the Africa Cybercrime Operations Desk with the support of the African Joint Operation against Cybercrime (AFJOC), and funded by the United Kingdom's Foreign, Commonwealth and Development Office (FCDO). For questions about the report, please contact us at AfricaDesk@interpol.int.

This report is the culmination of a thorough analysis of information gathered from a variety of sources, including African member countries and INTERPOL private sector partners such as Bi.Zone, Group-IB, Kaspersky, and Trend Micro. Additionally, INTERPOL's own intelligence and operations units have been leveraged to inform and enrich the report, ensuring a comprehensive and nuanced understanding of the issues.

We gratefully acknowledge the contributions of 43 out of 54 African member countries that completed the cyberthreat assessment questionnaire and provided valuable insights that informed this report.

EXECUTIVE SUMMARY

Cybercrime is accelerating across Africa, threatening public safety, financial systems, and digital trust. While more countries are responding, many still face serious structural challenges that limit their ability to detect, investigate, and disrupt cyberthreats.

Law enforcement capacity remains uneven. A majority of countries report shortages in cybercrime investigative skills, limited access to digital forensic tools, and insufficient infrastructure. Although several countries have launched dedicated cybercrime units, these often operate with limited resources and personnel.

Legal frameworks are improving, but progress is fragmented. Some member countries have modernized cybercrime legislation but, in many cases, the countries surveyed indicate that their legal frameworks and prosecution capacity need improvement. Such laws could also be better aligned with regional and international standards. These gaps continue to hinder prosecutions and the admissibility of digital evidence.

Cross-border coordination remains a major obstacle. While INTERPOL-facilitated operations have achieved notable results, countries report that formal cooperation channels such as Mutual Legal Assistance (MLA) processes remain slow and underutilized. Jurisdictional issues, lack of trust, and limited access to global digital platforms further complicate regional enforcement efforts.

Emerging threats are evolving rapidly. Criminal use of artificial intelligence, synthetic media, and mobile-enabled fraud schemes is outpacing the capacity of many agencies to respond. These threats often exploit legal and operational blind spots and require new forms of inter-agency and international collaboration.

Despite these challenges, there are encouraging signs of progress. Several member countries have strengthened public-private partnerships, updated legislation allowing for more effective prosecution of cybercrimes, and taken part in successful regional operations. Awareness of cybercrime risks is growing, and more national police services are prioritizing digital investigation capabilities.

This report outlines the core cybercrime challenges facing Africa, emerging threat trends, and real-world examples of both systemic barriers and operational success. It concludes with recommendations for enhancing national capabilities, strengthening legal and procedural frameworks, and deepening international cooperation - all of which are essential to building long-term resilience.

1. INTRODUCTION

Africa's accelerating digital transformation is reshaping economies, governance, and society. Despite leveraging the latest technologies and innovation, it has also significantly expanded the attack surface for cybercrime. As digital adoption grows, so do the threats targeting financial systems, public services, businesses, and end users.

To better understand and address this evolving risk landscape, INTERPOL conducted a continent-wide cyberthreat assessment. The report draws from a **detailed survey of African law enforcement agencies, operational intelligence, insights from INTERPOL private-sector partners, and open-source information.** This multi-source approach ensures a grounded and comprehensive view of regional trends.

This assessment follows the 2024 African Cyberthreat Assessment Report, building on the findings from last year's report. It aims to provide an updated perspective on the cybersecurity landscape and to track the progress made in addressing the challenges previously highlighted.

The goal of this report is to support law enforcement, policymakers, and cybersecurity stakeholders in identifying emerging threats, addressing capability gaps, and enhancing cooperation at national and regional levels. Investigating cybercrime at any level has direct impact on victims and potential victims located across the globe. Through collective efforts, Africa's digital future will be more secure.

2. THE EVOLVING CYBERTHREAT LANDSCAPE IN AFRICA

Africa's rapid digital transformation has significantly increased connectivity and driven the widespread adoption of technologies such as mobile banking, e-commerce, and cloud computing, fostering economic growth and innovation.[1] However, this expansion has also introduced cybersecurity challenges, as digital infrastructures became increasingly attractive targets for cyberthreat actors. With over 500 million Internet users in the region, many countries still lack adequate cybersecurity measures leaving businesses and individuals vulnerable to attacks.[2] Many countries across the continent face challenges such as legal frameworks that are still taking shape, limited cybersecurity investment, and digital literacy gaps, further exacerbating these risks.

The widespread use of smartphones has made mobile platforms a primary target for cybercriminals, particularly in regions with high mobile banking adoption. Additionally, the growing integration of Internet of Things (IoT) devices in sectors such as agriculture, healthcare, and manufacturing presents new security risks, as many of these devices lack robust protection.[3] Several African nations, including Ethiopia, Zimbabwe, Angola, Uganda, Nigeria, Kenya, Ghana, and Mozambique, are among the most frequently targeted globally in 2024, according to malware detection data from the International Telecommunication Union (ITU) Global Cyberthreat Index.[4] This underscores the need for more robust cybersecurity frameworks to protect digital advancements and ensure long-term resilience in the region.[5] [6]

The INTERPOL Africa Cyberthreat Assessment Report 2025 highlights a sharp increase in cybercrime incidents across Africa. Over two-thirds of INTERPOL's African member countries surveyed have identified cyber-dependent and cyber-enabled crimes as accounting for a medium to high share of all crimes. Notably, cybercrime accounts for more than 30% of all reported crimes in both Western and Eastern Africa, making it a major concern in these subregions:

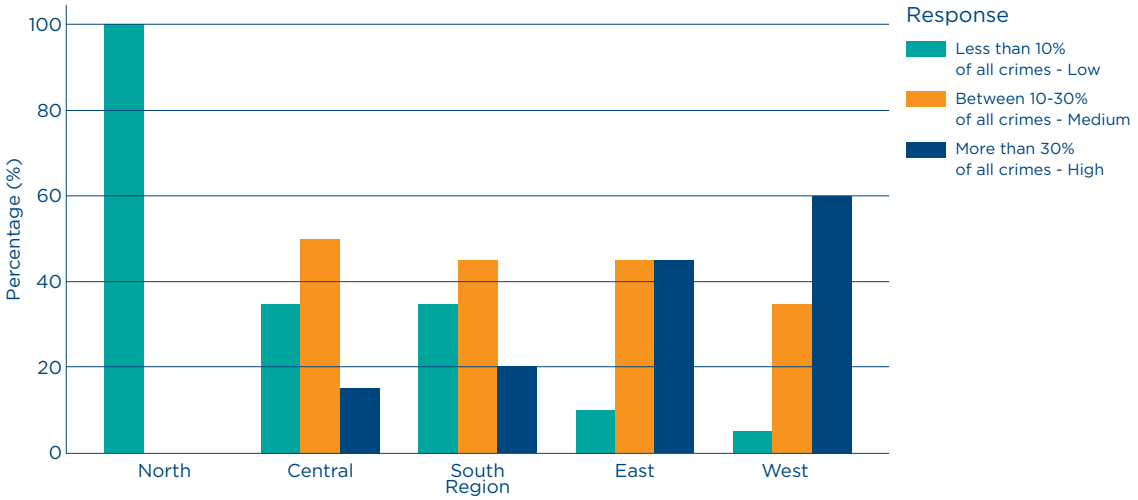


Figure 1: Perceived cybercrime risk levels across African subregions as reported by INTERPOL Africa member countries in the 2025 Survey.

1 GSMA, The Mobile Economy of the Sub-Saharan Africa: https://event-assets.gsma.com/pdf/GSMA_ME_SSA_2024_Web.pdf
2 https://innovation-village.com/cybersecurity-in-africa-emerging-threats-and-solutions
3 GSMA, The Mobile Economy of the Sub-Saharan Africa: https://event-assets.gsma.com/pdf/GSMA_ME_SSA_2024_Web.pdf
4 https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf
5 Check Point, The State of Cyber Security 2025: https://www.checkpoint.com/security-report
6 https://it-online.co.za/2024/09/13/africa-faces-urgent-cybersecurity-challenges

Previous editions of the Report identified ransomware attacks, banking trojans, stealers, online scams, phishing, business email compromise (BEC), and malicious software offered as a service, such as spyware and phishing kits, as the most prevalent cyberthreats.[7] Online scams, particularly phishing, continue to be the most frequently reported cybercrimes among INTERPOL member countries, while ransomware and BEC remain widespread. In addition, digital sextortion and identity theft are reported as significant cyberthreats by African member countries.

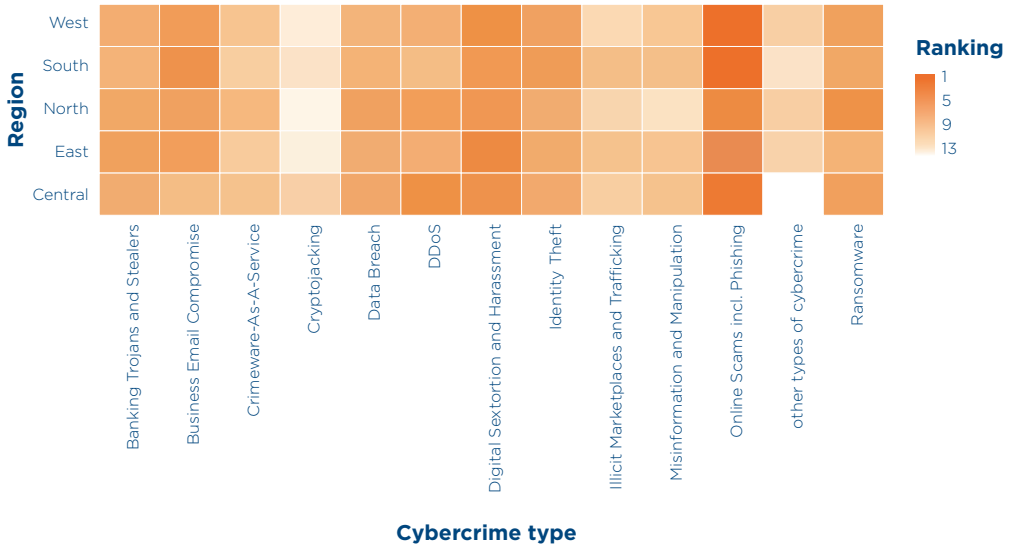


Figure 2: Most frequently reported cyberthreats across African INTERPOL member countries in 2024, based on law enforcement survey data.

Banking trojans, info stealers, and Cybercrime-as-a-Service (CaaS) have seen a decline in reported incidents compared to previous years. This trend could indicate improved law enforcement efforts, better cybersecurity awareness, or a shift in cybercriminal tactics toward more effective methods such as social engineering and AI-driven scams.

Many INTERPOL member countries in the African region have reported a growing financial and operational impact of cybercrime, with online scams, Business Email Compromise (BEC), ransomware, and Distributed Denial-of-Service (DDoS) attacks identified as the most financially damaging threats across all sub-regions. Between 2019 and 2025, cyber incidents across the continent resulted in estimated financial losses exceeding $3 billion[8], with the finance, healthcare, energy, and government sectors among the hardest hit.[9] These critical industries are prime targets for cybercriminals who create operational disruption and data breaches resulting in significant financial consequences.

7 INTERPOL Africa Cyberthreat Assessment Report 2024: https://www.interpol.int/en/content/download/21048/file/24COM005030-AJFOC_Africa%20Cyberthreat%20Assessment%20Report_2024_complet_EN%20v4.pdf

8 https://african.business/2025/02/apo-newsfeed/over-half-of-africans-fear-financial-losses-from-cybercrime-survey-finds

9 Group-IB, Hi-Tech Crime Trends Report 2023/2024; Middle East & Africa Cyberthreat Landscape: https://www.group-ib.com/resources/research-hub/hi-tech-crime-trends-2023-mea/

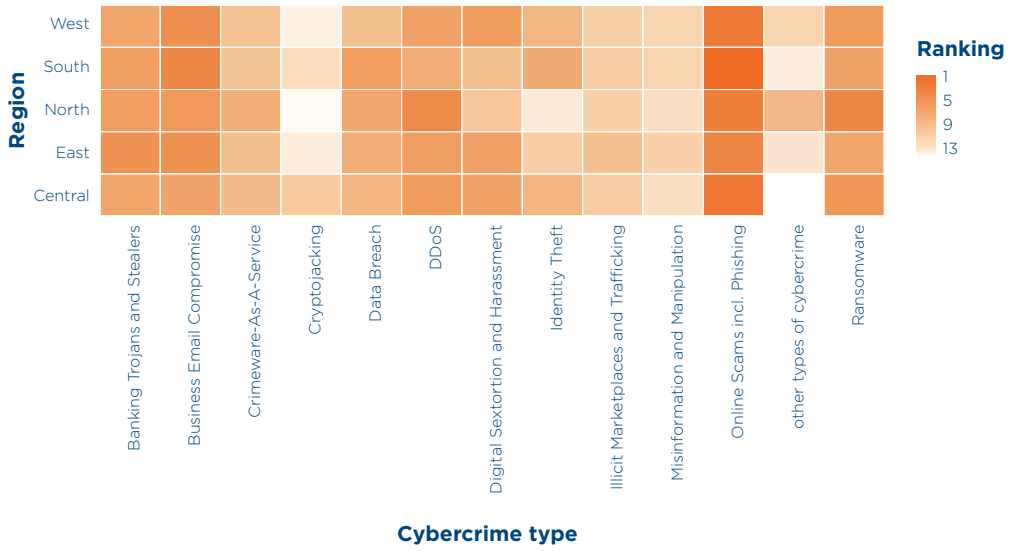


Figure 3: Average ranking of cybercrime types by reported financial impact across African subregions, based on INTERPOL member country data.

As reported by INTERPOL African member countries, cybercriminals are continuously refining their tactics, utilizing social engineering, artificial intelligence, and instant messaging platforms to launch increasingly sophisticated attacks. Both domestic and international cybercriminal networks exploit human vulnerabilities as a primary method, employing advanced deception techniques to target organizations and individuals.

2.1 The Most Widespread Cyberthreats in Africa in 2024

The latest survey findings from INTERPOL African member countries and private partners[10], combined with regional cybersecurity reports, identify online scams, ransomware, business email compromise (BEC), and digital sextortion as the most significant cyberthreats. This section provides a detailed analysis of the evolving cyberthreat landscape, highlighting the most prevalent threats in Africa in 2024.

2.1.1. ONLINE SCAMS

Online scams are sharply increasing in several countries as cybercriminals constantly adapt their methods to exploit vulnerabilities and defraud both individuals and businesses. Fraudulent activities, including phishing and romance scams, have grown increasingly sophisticated through the strategic use of social engineering, artificial intelligence, and manipulation via social media platforms. INTERPOL member countries have highlighted these online scams as among the most critical cyberthreats facing Africa in 2024, pointing to their rising frequency and severe impacts. This is confirmed by additional sources, including data from INTERPOL private partners.

10 Data received from four INTERPOL private partners: Group-IB, Trend Micro, Kaspersky, and Bi.Zone.

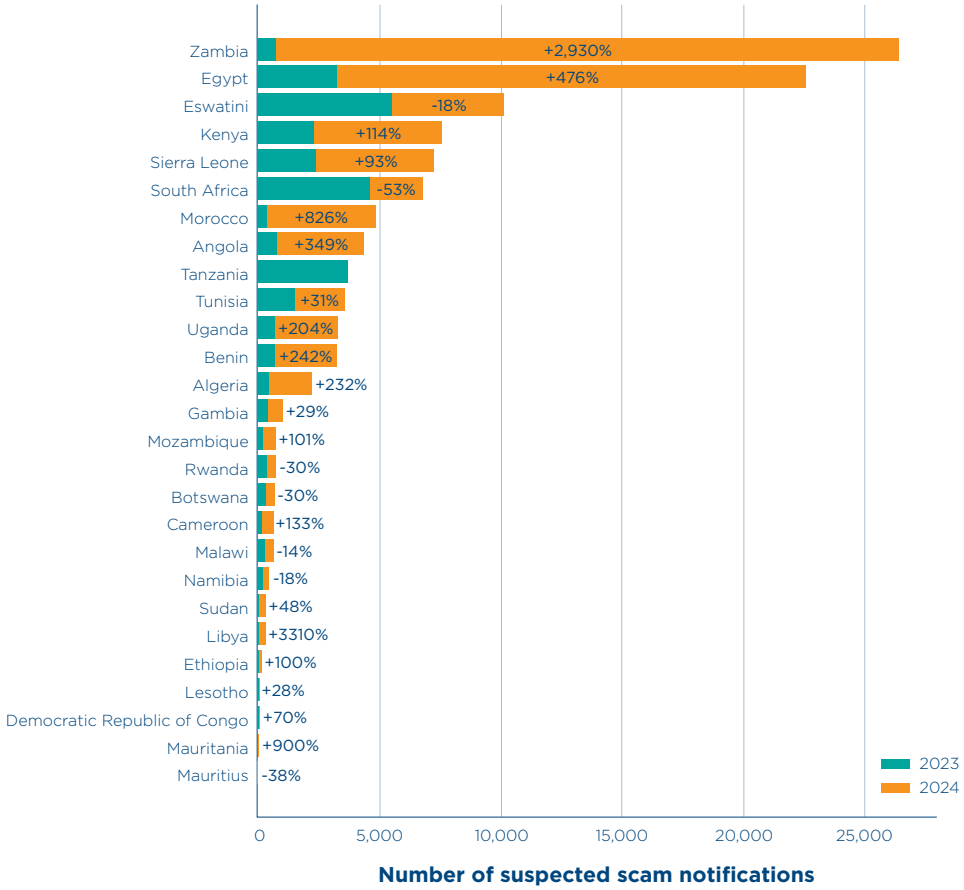


Figure 4: Increase in scam notifications across African regions from 2023 to 2024, based on data provided by Kaspersky.

The surge in online scams is closely linked to Africa's accelerating digital transformation.[11] Criminals capitalize on the growing online activity, in particular social media usage, digital commerce and mobile banking, to perpetrate fraud. Data from INTERPOL African member countries indicate that victims of such crimes are diverse as they affect individuals across all age groups, genders, and professional backgrounds. While the survey data from member countries highlight that some groups are more vulnerable, it is also clear that all demographics are at risk.

Online scams, via phishing, continues to be Africa's most prevalent cyberthreat in 2024, impacting both individuals and organizations across the continent. INTERPOL member countries have identified phishing as the leading cybersecurity concern, citing its high frequency and extensive reach. According to digital security reports, phishing accounts for 34% of all cyber incidents detected throughout Africa.[12] Cybercriminals leverage phishing by impersonating trusted entities via emails, messaging platforms, or fraudulent websites, tricking individuals into providing sensitive information such as login credentials, financial data, or personal identification details.[13] Once obtained, this information facilitates unauthorized access, identity theft, and financial fraud. The growing sophistication of these phishing schemes significantly increases vulnerabilities within critical sectors, including banking, government institutions, and telecommunications..

11 GSMA, The Mobile Economy of the Sub-Saharan Africa: https://event-assets.gsma.com/pdf/GSMA_ME_SSA_2024_Web.pdf

12 ESET Threat Report: https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-threat-report-h22024.pdf

13 INTERPOL Africa Cyberthreat Assessment Report 2024: https://www.interpol.int/en/content/download/21048/file/24COM005030-AJFOC_Africa%20Cyberthreat%20Assessment%20Report_2024_complet_EN%20v4.pdf

INTERPOL's survey data indicate a notable evolution in phishing tactics, which have become increasingly tailored, localized, and technologically sophisticated, evolving beyond traditional mass email scams toward targeted social engineering attacks. Cybercriminals now regularly impersonate recognized authorities and prominent corporations, exploit widespread unemployment through fabricated job offers, and use mobile platforms for prize-related and emergency-based scams. Additionally, mobile-based phishing (smishing), voice phishing (vishing), and social media phishing campaigns exploit victims' trust and emotional triggers, further widening the threat landscape.[14] The accessibility of affordable phishing tools on illicit online marketplaces contributes significantly to the proliferation of these schemes. Cybercriminals are also integrating AI-generated text, audio, and video to enhance the credibility and persuasiveness of phishing campaigns, adapting their messaging to reflect local languages and cultural nuances.[15]

Data provided by INTERPOL African member countries also highlighted that the impact of phishing extends broadly across multiple sectors in Africa, each with distinct vulnerabilities and repercussions. Financial institutions face considerable losses due to credential theft and unauthorized transactions, undermining consumer trust and hindering digital financial inclusion. Telecom companies encounter challenges with brand exploitation, SIM-swap fraud, and mass SMS scams, adversely affecting reputation and operational efficiency. Additionally, governments, healthcare institutions, and educational facilities grapple with compromised citizen data, operational disruptions, and diminished public confidence, emphasizing the need for robust, sector-specific mitigation strategies.

In 2024, romance scams surged across Africa, becoming one of the continent's most widespread online scams. Fraudsters are using more advanced and damaging tactics, fuelled by rising Internet access and the expanding reach of social media. Data provided by INTERPOL member countries indicate that criminals typically initiate contact with victims via social media, messaging services, and online dating apps. Fraudsters aim to cultivate personal relationships by exploiting vulnerabilities, a process that can range from very brief interactions to prolonged engagements lasting several years. Once the illusion of trust is established, fraudsters then manipulate their victims into surrendering money or other assets.

Romance scams are a widespread concern across Africa, with certain regions experiencing higher reported levels. In particular, West African countries, including Nigeria, Ghana, Côte d'Ivoire, and Benin, have been identified as areas where romance fraud networks are particularly active.[16] A notable recent trend involves fraudsters initially luring victims with romantic promises and subsequently coercing them into investing cash in fraudulent cryptocurrency schemes.[17]

Romance scams have become highly profitable forms of cybercrime, causing significant emotional and financial harm. In one notable Nigerian case, a single scammer amassed over USD 1.9 million from multiple victims before arrest.[18] INTERPOL data reveal numerous cases where African victims repeatedly paid scammers, sometimes depleting retirement funds or accumulating debts. Many cases remain unreported due to victims' feelings of shame, guilt, and social stigma, suggesting the actual financial impact is far greater than officially documented.[19] Given the rising complexity and scale of these scams, African law enforcement agencies urgently require specialized training and enhanced forensic capabilities to effectively address and investigate this growing threat.

14 https://www.kaspersky.com/about/press-releases/kaspersky-reports-nearly-900-million-phishing-attempts-in-2024-as-cyber-threats-increase
15 https://cltc.berkeley.edu/2025/01/16/beyond-phishing-exploring-the-rise-of-ai-enabled-cybercrime
16 https://theconversation.com/online-romance-scams-who-nigeria-and-ghanas-fraudsters-are-how-they-operate-and-why-they-do-it-247916
17 https://www.reuters.com/world/africa/almost-800-arrested-over-nigerian-crypto-romance-scam-2024-12-16/
18 https://www.interpol.int/en/News-and-Events/News/2024/Arrests-in-international-operation-targeting-cybercriminals-in-West-Africa
19 https://www.knowbe4.com/hubfs/Online-Scams+Victims-Africa-report-2024.pdf

2.1.2. RANSOMWARE

In 2024, INTERPOL member countries identified ransomware as one of the most prevalent cyberthreats across the African continent, posing a growing risk to governments, businesses, and critical services. Data from INTERPOL's private-sector partners indicates that monthly ransomware detections in Africa rose in 2024 compared to the previous year.[20] These attacks are particularly concerning because of their high financial impact, their potential to severely disrupt critical infrastructure, and the damage they inflict on affected organizations and individuals. Reports from cybersecurity firmss[21] and INTERPOL private partners show that South Africa and Egypt suffered the highest number of ransomware incidents in 2024, followed by other highly digitized economies such as Nigeria, Kenya, the Gambia, Tunisia and Morocco. Algeria, Ethiopia and even more compact states like Benin also reported significant attacks, underscoring that ransomware is a continent-wide challenge, especially in countries with more developed digital infrastructure.

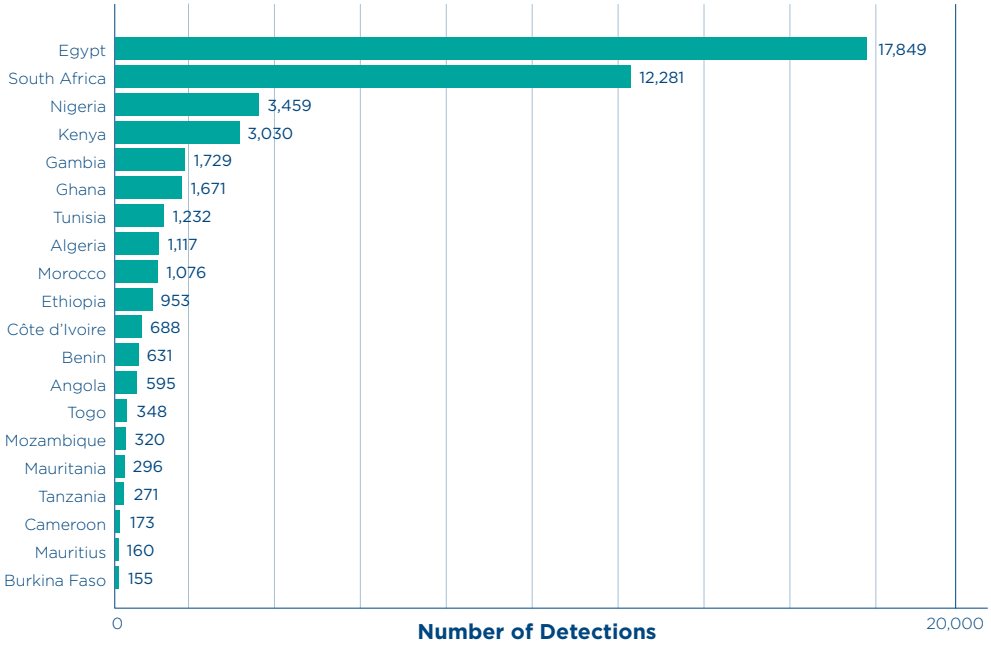


Figure 5: Top 20 African countries by number of ransomware threat detections in 2024, based on data from Trend Micro.

The financial impact of ransomware in Africa was considerable in 2024. Some incidents involved outright theft, such as the cyber heist at the Nigerian fintech firm Flutterwave in April, which reportedly diverted around USD 7 million.[22] In other cases, ransom demands ranged from tens of thousands to millions of dollars, often requested in cryptocurrency, resulting in significant financial burdens. Furthermore, ransomware disruptions led to lost revenue, reduced productivity, halted commerce, and sizable recovery expenses.

20 According to data provided by Trend Micro, 2024.

21 https://falconfeeds.io/blogs/cyber-attacks-in-africa-a-comprehensive-analysis-of-trends-from-january-to-august-2024-206317

22 https://africa.businessinsider.com/local/markets/fintech-giant-flutterwave-loses-naira11-billion-to-security-breach

Cameroon's electric utility (ENEO) disrupted power management operations, while the breach at Kenya's Urban Roads Authority (KURA) compromised vital road infrastructure data.[23] Government databases were also affected, including the December 2024 hacks of Kenya's Micro and Small Enterprise Authority (MSEA) and Nigeria's National Bureau of Statistics (NBS).[24] In South Africa, the Department of Defence fell victim to the Snatch ransomware group in late 2024, losing 1.6 TB of data, including their president's contacts.[25] The telecommunications sector faced similar threats, exemplified by Telecom Namibia's breach in late 2024, during which approximately 626.3 GB of data, including over 492,000 files, were compromised, affecting more than 619,000 clients.[26] This breach exposed sensitive information belonging to private individuals, businesses, and government entities, underscoring the significant risks to both citizen privacy and national security.[27]

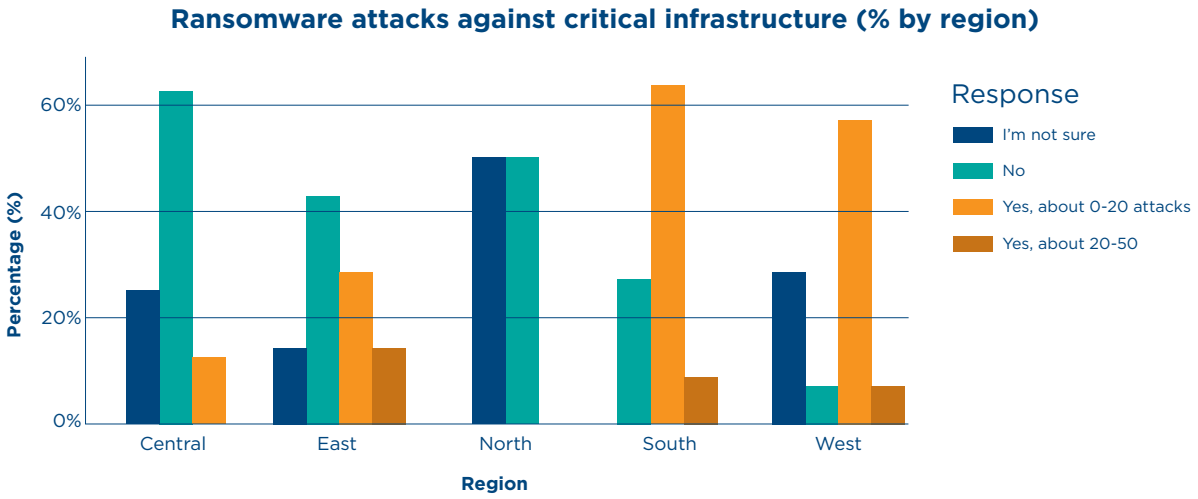


Figure 6: Ransomware attacks against critical infrastructure by region (%), based on survey responses from INTERPOL African member countries in 2024.

According to data from INTERPOL's private partners[28], several hacker groups operated across the African region in 2024. One of the most prominent was LockBit, a prolific Ransomware-as-a-Service (RaaS) gang that remained highly active throughout the year. LockBit is known for its aggressive double-extortion methods, encrypting victims' networks while threatening to publish stolen data, and claimed responsibility for a February attack on South Africa's Government Employees Pension Fund (GEPF).[29] It was also linked to numerous incidents in West Africa.[30] Although authorities temporarily seized LockBit's darknet sites during an international crackdown, the group soon resurfaced to post, or potentially re-post, victim data, causing serious operational disruptions and significant data breaches.[31] The GEPF attack alone affected millions of individuals, highlighting the severe risks posed by LockBit's continued activity.

23 https://adforensics.com.ng/cyberattack-on-africas-top-organizations-2024
24 https://adforensics.com.ng/cyberattack-on-africas-top-organizations-2024
25 https://therecord.media/lockbit-ransomware-takes-credit-for-south-african-pension-fund-attack
26 https://neweralive.na/telecom-hit-by-massive-cyberattack-over-400-000-files-leaked
27 https://dailysecurityreview.com/news/namibia-ransomware-attack-sensitive-data-of-government-officials-and-citizens-leaked/
28 According to data provided by BI.ZONE, 2024.
29 https://therecord.media/lockbit-ransomware-takes-credit-for-south-african-pension-fund-attack
30 https://toptechgh.com/lockbit-ransomware-member-extradited-see-attacks-on-africa
31 https://therecord.media/lockbit-ransomware-takes-credit-for-south-african-pension-fund-attack

Another prominent ransomware actor, Hunters International (Hunters), specifically targets telecom, government, and financial institutions across Africa.[32] In July 2024, Hunters breached Kenya's Urban Roads Authority (KURA), stealing approximately 18 GB of data.[33] They struck again in December, attacking Telecom Namibia and leaking sensitive customer information.[34] Hunters employs a stealthy approach, quietly exfiltrating data before encrypting systems; victims who refuse ransom demands see their data publicly leaked, causing significant operational disruptions and eroding public trust. BlackSuit, an extortion-oriented ransomware group known for targeting major organizations globally, demonstrated its ruthlessness by attacking South Africa's National Health Laboratory Service (NHLS) in June 2024.[35] This severe incident disrupted diagnostics for millions of medical tests, forced cancellations of critical surgeries, and compromised more than 1 TB of highly sensitive data, starkly illustrating ransomware's potential to threaten human health and safety.

2.1.3. BUSINESS EMAIL COMPROMISE

INTERPOL member countries in Africa have identified business email compromise (BEC) as a significant and growing cyberthreat within the broader landscape of online scams. Data from INTERPOL's private sector partners[36] indicate a sharp rise in BEC-related cybercriminal activity across Africa, both in attack volume and financial impact. A substantial number of BEC criminals operate from the continent, particularly in West Africa. According to data from INTERPOL private partners, 11 African nations account for the majority of BEC activity originating from the continent, with a concentration of BEC activity in Nigeria, Ghana, Côte d'Ivoire, and South Africa. In West Africa, some criminal networks have evolved into highly organized, multi-million-dollar enterprises driven by BEC fraud. The transnational syndicate Black Axe has thousands of members worldwide and is responsible for large-scale financial scams that have generated billions.[37]

Data provided by INTERPOL African member countries indicate that in 2024, the finance sector was the most frequently targeted across African Member States. Companies engaged in international trade, frequent financial transactions, and those with underdeveloped security controls were particularly vulnerable to BEC attacks. However, no industry was immune to BEC attacks; organizations of all sizes, from small and medium-sized enterprises to large corporations, were affected. In addition to banks and microfinance institutions, significant incidents were reported in sectors such as the import and export trade, oil and gas, pharmaceuticals, transport, and e-commerce. Attacks on government institutions, as well as the voluntary sector and individuals, were also on the rise across the continent.

Precise numbers of BEC incidents in Africa are challenging to obtain due to underreporting, however, several indicators reveal the scale of the problem. In 2024 alone, 19 African countries collectively reported 10,490 cybercrime-related arrests, suggesting that the actual number of BEC cases is significantly higher, given that only an estimated 35% of cybercrimes are officially reported.[38] A high-profile case illustrating the global impact of African cybercriminal networks occurred in November 2024, when U.S. authorities sentenced Babatunde Ayeni, a 33-year-old Nigerian national, to 10 years in prison for orchestrating a large-scale BEC scheme targeting real estate transactions.[39] Operating from Nigeria and the UAE, Ayeni and his co-conspirators conducted phishing attacks to steal email login credentials from real estate attorneys and agents in the United States. They then impersonated these professionals to redirect mortgage closing payments to fraudulent accounts. The scheme affected over 400 victims and resulted in the theft of USD19.6 million, which was routed into accounts controlled by the fraudsters.[40] This case underscores the transnational nature of BEC crimes and how African cybercriminal networks exploit global financial systems to defraud victims worldwide.

32 According to data provided by BI.ZONE, 2024.
33 https://www.darkreading.com/cyberattacks-data-breaches/ransomware-targeting-infrastructure-telecom-namibia
34 https://magedata.ai/securefact/securefact-cyber-security-news-week-of-december-23-2024
35 https://www.bitdefender.com/en-us/blog/hotforsecurity/ransomware-attack-on-blood-testing-service-puts-lives-in-danger-in-south-africa
36 According to data provided by Trend Micro, 2024.
37 https://africacenter.org/spotlight/black-axe-nigeria-transnational-organized-crime
38 https://therecord.media/orion-carbon-black-bec-scam-millions
29 https://www.justice.gov/usao-sdal/pr/nigerian-national-sentenced-ten-years-20-million-cyber-fraud-scheme
40 https://www.justice.gov/usao-sdal/pr/nigerian-national-sentenced-ten-years-20-million-cyber-fraud-scheme

In terms of modus operandi, data from INTERPOL African member countries indicate that BEC attacks across the continent leverage social engineering, phishing, impersonation, and network intrusion to manipulate financial transactions. A common tactic is fraudulent transfer orders, where cybercriminals impersonate executives, business partners, or government officials to deceive employees into transferring funds. CEO fraud and bank account detail change fraud, particularly in the public sector, are among the most reported schemes. Phishing and credential theft are widely used to gain access to accounts, with some attackers employing WhatsApp-based social engineering by impersonating known contacts. More advanced cases involve network intrusions, where malware is deployed to monitor email exchanges and intervene in payment processes. In West and Southern Africa, criminals frequently use lookalike domains or minor modifications to email addresses to deceive victims. Quotation and payment scams are also prevalent, where fraudsters send fraudulent requests for quotes or claim banking details have changed.

Reports from INTERPOL member countries also indicate that Cybercrime-as-a-Service (CaaS) is fueling the growing sophistication of BEC attacks. Microsoft's Digital Crimes Unit detected a 38% increase in CaaS targeting business email accounts between 2019 and 2022.[41] Threat actors now have access to ready-made phishing kits, allowing them to scale operations efficiently. Illicit platforms such as BulletProofLink further facilitate large-scale BEC campaigns by offering end-to-end services, including templates, hosting, and automation.[42] These platforms also help criminals bypass security measures like "impossible travel" alerts by leveraging residential IP addresses.

Additionally, AI-driven BEC schemes are an emerging threat. INTERPOL issued a purple notice warning concerning criminals misusing AI and deepfake technology to enhance scams.[43] Generative AI enables fraudsters to craft convincing, personalized emails that mimic the style and linguistic patterns of specific individuals or organizations, while deepfake technology is already being used to impersonate executives in phone or video calls. The rapid evolution of AI poses a significant risk by scaling BEC attacks and increasing their authenticity, necessitating close monitoring by member countries.

2.1.4. Digital Sextortion

Digital Sextortion is a category of Online Image Based Sexual Abuse (OIBSA) in which threat actors use sexually explicit images to extort their subjects by threatening to leak images without the consent of the targeted victim. These images may be legitimate, obtained through coercion, deception, or shared voluntarily, or they may be AI-generated or digitally manipulated.[44] Motives for sextortion are typically financially driven; however, other motives include revenge and the coercion of the victim.

OIBSA, specifically digital sextortion, has emerged as a prominent cybercrime across Africa in 2024. Data from INTERPOL African member countries show a significant increase in reports of digital sextortion, with over 60% of countries noting a perceived rise. This trend likely reflects broader shifts in the region's digital environment. Given widespread underreporting, especially with crimes of this nature, the true scale is likely much higher. Importantly, current data exclude reports from victims outside the region, suggesting the threat may be even more widespread and globally interconnected than the regional figures indicate.

41 Microsoft (2023): https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW15yVe

42 INTERPOL Africa Cyberthreat Assessment Report 2024: https://www.interpol.int/en/content/download/21048/file/24COM005030-AJFOC_Africa%20Cyberthreat%20Assessment%20Report_2024_complet_EN%20v4.pdf

43 INTERPOL Africa Cyberthreat Assessment Report 2024: https://www.interpol.int/en/content/download/21048/file/24COM005030-AJFOC_Africa%20Cyberthreat%20Assessment%20Report_2024_complet_EN%20v4.pdf

44 https://www.trendmicro.com/vinfo/sg/security/definition/digital-extortion

The growing impact of OIBSA is reflected in recent enforcement actions by major platforms. In mid-2024, Meta removed over 63,000 Instagram accounts and 7,000 Facebook entities linked to digital sextortion operations in Nigeria.[45] [46] While it remains unclear when these accounts were first identified, the scale of the action suggests either a sharp escalation in threat activity or mounting external pressure on platforms to respond - both significant indicators of the crime's growth. Many of these accounts were linked to organized cybercriminal networks, some of which were involved in recruiting and training perpetrators and distributing operational manuals for conducting digital sex crimes.[47] [48] This points to a tactical evolution: sextortion is being weaponized not just as an isolated offense, but as a recurring Tactic, Technique, and Procedure (TTP) within traditional scam ecosystems. Some reporting also suggests these networks may overlap with long-standing organized crime groups (OCGs) in West Africa, though further confirmation is needed.[49]

Alongside changes in targeting and scale, new threat vectors have emerged. INTERPOL's private partners report a sharp increase in phishing emails used to initiate sextortion campaigns.[50] Additionally, there has been a rise in AI-enhanced extortion schemes, where synthetic or altered, explicit images are used to deceive victims. The highest number of such incidents was recorded in Morocco, Mali, Egypt, and Mauritania, underscoring the regional distribution. This convergence of phishing, AI tools, and tactics demonstrates a systematization of sextortion; it is no longer limited to opportunistic attackers but is increasingly embedded within broader fraud infrastructures.

Although much of the known OIBSA activity on Meta platforms has involved adult victims, law enforcement has flagged a concerning rise in cases involving teenage boys and girls, including those outside the African region.[51] [52] This apparent shift in victim demographics and expanding geographic scope may indicate a change in strategy. It also raises critical questions around the motivations driving digital sextortion. While financial extortion remains a primary goal, typically through threats to release explicit images, some incidents suggest motivations rooted in psychological manipulation, coercion, or the intent to cause reputational harm. In these cases, perpetrators may be exploiting vulnerabilities for control rather than monetary gain. The psychological toll on victims is substantial. In South Africa, authorities reported a rise in teenage victims, and one adult victim died by suicide following a sextortion incident.[53] In Egypt, a digital support platform received over 250,000 sextortion-related appeals in 2024, mainly from women and girls.[54] [55] These figures reflect a hidden but widespread crisis, where fear, stigma, and emotional distress are routinely exploited by threat actors as part of their method of control.

In response to the growing threat, African law enforcement agencies have intensified efforts, including increased international coordination, cross-border cooperation, and engagement with private sector platforms. However, persistent capacity limitations, legal jurisdiction challenges, and delays in accessing cross-border data continue to hamper investigations. As both offenders and victims span national borders, existing enforcement frameworks struggle to keep pace.

45 https://www.npr.org/2024/07/24/nx-s1-5050709/meta-sextortion-scams-nigeria-facebook-instagram
46 https://www.reuters.com/world/africa/facebook-removes-63000-accounts-nigeria-over-sextortion-scams-2024-07-24/
47 https://tuxcare.com/blog/sextortion-scams-63k-instagram-account-in-nigeria-removed
48 https://www.theverge.com/2024/7/24/24205236/meta-nigeria-financial-sextortion-scam
49 https://www.unodc.org/documents/organized-crime/tools_and_publications/21-05344_eBook.pdf
50 According to data provided by Trend Micro, 2024.
51 https://www.reuters.com/world/africa/facebook-removes-63000-accounts-nigeria-over-sextortion-scams-2024-07-24/
52 https://businesstech.co.za/news/internet/790431/extortion-syndicates-targeting-boys-in-south-africa
53 https://www.theguardian.com/uk-news/article/2024/aug/21/how-west-africas-online-fraudsters-moved-into-sextortion
54 https://allafrica.com/stories/202408190082.html
55 https://www.reuters.com/article/technology/feature-egyptian-women-find-help-online-to-fight-sextortion-threats

3. CYBERTHREAT TRENDS AND INSIGHTS ACROSS AFRICAN SUB-REGIONS

Across the African continent, cyberthreat trends generally follow similar patterns, with online scams, ransomware, business email compromise (BEC) and digital sextortion, identified as the most serious cyberthreats. However, the nature and scale of these threats vary across different subregions due to differences in digital infrastructure, law enforcement capabilities, and cybercrime tactics. This section examines regional cyber trends and developments across West Africa, East Africa, Central Africa, Southern Africa, and North Africa, providing insights into how cybercrime manifests in each sub-region.

3.1 West Africa

- Nigeria, Ghana, Côte d'Ivoire, and Senegal drive a significant share of West Africa's digital economy and cyber activity.[56] • These nations are not only centres of technological innovation and financial services but also key targets for cyberthreats that are reshaping the region's overall cybersecurity ecosystem.
- BEC remains one of the most financially damaging cyberthreats, with West African-based groups targeting companies globally.
- Ransomware attacks remain a top cyberthreat, with cybercriminals, especially those operating under the Ransomware-as-a-Service (RaaS) model, using African organizations as testing grounds for new malware.[57] These attacks typically follow a double-extortion model, encrypting data while threatening to leak sensitive information if ransoms are not paid.
- DDoS attacks remain a major concern in the region. In the first half of 2024, Ghana recorded 4,753 DDoS incidents, with peak attacks reaching 314 Gbps, positioning it among the top DDoS targets in Africa.[58]
- Mobile wallet fraud has risen sharply. Scammers employ social engineering tactics to hijack accounts and solicit emergency funds from unsuspecting contacts. Mobile money fraud, including SIM swap scams and telecom impersonation, is widespread, while identity theft fuels a rise in fraudulent schemes related to investments, betting, and online shopping.
- Romance scams are on the rise, with victims being blackmailed over sensitive information. One recent trend involves fraudsters initially luring victims with romantic promises and subsequently coercing them into investing cash into fraudulent cryptocurrency schemes.

56 https://arxiv.org/html/2402.01649v1
57 https://www.darkreading.com/cyberattacks-data-breaches/criminals-test-ransomware-africa
58 https://toptechgh.com/ghana-hit-with-4753-ddos-attacks-netscout-threat-intelligence-report-1h-2024

3.2 East Africa

- East African countries, Kenya, Uganda, Tanzania, Rwanda, and Ethiopia, are rapidly emerging as technological and financial hubs, significantly advancing digital transformation. However, this progress makes them increasingly attractive targets for cyberthreats, highlighting the urgent need for robust cybersecurity frameworks.
- Ethiopia became the world's most targeted country for cyberattacks in 2024, ranking highest globally in malware detections.[59] • Critical infrastructure, including government institutions, financial services, and significant development projects, are frequently targeted.
- SIM swap fraud has notably increased in Uganda and Tanzania. Criminals exploit mobile network vulnerabilities by fraudulently acquiring replacement SIM cards, often through deception or collusion with insiders, allowing them to hijack victims' phone numbers.
- Digital sextortion is a rising cyberthreat in East Africa. Criminals frequently exploit compromising material to extort victims, particularly targeting women and young individuals.

3.3 Central Africa

- Cyberattacks in Central Africa frequently exploit weak infrastructure protection and outdated systems.
- Social engineering scams remain among the most frequently reported cybercrimes, with criminals leveraging deceptive tactics such as fake employment opportunities and romance scams to exploit unsuspecting victims.
- Financial institutions face growing vulnerability to Business Email Compromise (BEC) fraud and network intrusions. Cameroon and Gabon have reported a significant rise in cyberattacks targeting financial institutions, causing substantial losses.

3.4 Southern Africa

- Southern Africa is recognized for having one of the most advanced cybersecurity ecosystems on the continent, with countries such as South Africa, Namibia, and Botswana making substantial investments in cybersecurity awareness, comprehensive legal frameworks, and AI-driven security technologies.
- Cybercriminals have adopted AI-powered tools to create sophisticated deepfake voice and video impersonations, leading to a considerable escalation in vishing attacks by mimicking CEOs and vendors in 2024.[60]
- Social engineering remains a central tactic in many cyber incidents, often serving as the initial point of attack. SMS phishing (smishing) specifically targeted banking customers, using deceptive messages to compromise user accounts.
- Cybercriminals in Southern Africa are increasingly exploiting emerging fintech trends, including digital banking and cryptocurrencies. Cryptojacking became increasingly prevalent, with financial institutions reporting substantial growth in such incidents during 2024.

59 https://adforensics.com.ng/cyberattack-on-africas-top-organizations-2024/

60 https://qtatech.com/en/article/why-are-cyberattacks-increasingly-targeting-african-financial-institutions?srsltid=AfmBOoqghmt5QRlVko-UqiSdks8zjt99y1nHYR24zzh1vf63gxMYTk2a

3.5 North Africa

- In 2024, North African countries, including Egypt, Algeria, Morocco, Tunisia, and Libya, faced an increasingly sophisticated cyberthreat landscape, influenced by global cybercrime trends and regional geopolitical dynamics.
- Egypt and Morocco were among Africa's most heavily targeted nations due to their extensive Internet penetration and large economies. Egypt accounted for roughly 13% of all cyberattacks on the continent in 2024, ranking second after South Africa.[61]
- Social engineering continues to underpin many cyber incidents across North Africa, ranging from basic scams to highly sophisticated attacks. Businesses were frequently targeted with phishing emails customized in their local language to increase authenticity. Lottery and investment scams remain prevalent, with many reported cases involving WhatsApp messages promising fake prizes or fraudulent cryptocurrency investment opportunities.

CENTRAL AFRICA	EAST AFRICA	NORTH AFRICA	SOUTHERN AFRICA	WEST AFRICA
Low digital literacy and weak infrastructure leave the region vulnerable. • Cameroon saw cyber incidents nearly double in 2024. • Crypto fraud and social engineering scams are increasing. • Financial institutions face growing BEC and network attacks, but most cases go unresolved due to limited cybersecurity capacity.	Digital expansion is outpacing cybersecurity readiness. • Ethiopia led the world in malware detections in 2024, with critical infrastructure at risk. • SIM swap fraud is on the rise in Uganda and Tanzania. • Sextortion and online harassment, especially targeting women and youth, are increasingly common.	Cyberattacks in 2024 surged, driven by geopolitical tension and digital expansion. • Egypt and Morocco were among Africa's most targeted, with Egypt accounting for 13% of all attacks. • Social engineering and phishing scams, often via WhatsApp and fake investments, are widespread.	Home to Africa's most developed cybersecurity, yet still under siege. • AI-driven deepfakes and vishing surged in 2024. • South Africa remains a top target, especially in finance and government. • Cryptojacking and smishing attacks exploiting fintech growth are widespread.	Rapid digital growth-especially mobile money and social media-has made West Africa a cybercrime hotspot. • BEC and ransomware dominate, with Nigeria-based groups like Black Axe and Opera1er leading global scams. • Ghana recorded nearly 5,000 DDoS attacks in early 2024, with telecoms heavily targeted. • Mobile wallet fraud and romance scams are rising, often linked to fake crypto schemes. • AI-enhanced phishing and deepfakes are growing threats.

Table 1: Overview of cyberthreat trends & insights across African sub-regions

61 https://global.ptsecurity.com/analytics/cybersecurity-threatscape-for-african-countries-q1-2023-q3-2024

4. CHALLENGES IN COMBATING CYBERCRIME IN AFRICA

4.1 Fragmented Legal and Policy Frameworks

Cybercrime continues to outpace the legal systems designed to stop it. With 65% of countries reporting no updates to their cybercrime legislation in the past year and more than 75% of countries rating their legal frameworks and prosecution capacity as needing improvement, there is clear evidence of systemic legal gaps.[62]

To address these challenges, several international and regional instruments offer frameworks for strengthening cybercrime legislation:

- **Budapest Convention on Cybercrime[63]:** Provides comprehensive guidelines, including Article 19 which outlines powers for data access and seizure. Only six African countries have ratified it to date.
- **UN Convention on Cybercrime[64]:** Aims to enhance international cooperation in combating cybercrime, with growing support across Africa.
- **AU Malabo Convention[65]:** Focuses on cybersecurity and personal data protection; however, it has been ratified by only 15 African Union Member States to date.

These gaps highlight the growing need for alignment with international legal frameworks - an issue further explored in Chapter 6.

4.2 Capacity and Capability Constraints

Strong laws are only part of the solution - most countries also struggle to enforce them. Survey results show that **90% of respondents** say their law enforcement or prosecution capacity needs some or significant improvement.

The most common limitations include:

- **Training needs:** 95% reported inadequate, inconsistent, or donor-dependent training.
- **Resource constraints:** 95% of countries.
- **Access to specialized tools:** 95% of countries.
- **Technical skill gaps:** 74% of countries.
- **Infrastructure gaps:** 72% of countries.
- **Operational barriers:** 58% face bureaucratic, legal, or institutional obstacles to efficient investigations.

Despite rising caseloads, most countries still lack essential cybercrime infrastructure:

- **30%** have an incident reporting system.
- **28%** use a case management system (CMS).
- **19%** have a cyberthreat intelligence database.
- **29%** maintain a digital evidence repository.

Furthermore, few national institutions are staffed or equipped to respond in real time. Cloud-based crime technology, encrypted messaging platforms, and international investigations often exceed the technical and procedural reach of domestic teams.

62 INTERPOL Cyberthreat Assessment Survey

63 https://www.coe.int/en/web/cybercrime/the-budapest-convention

64 https://www.unodc.org/unodc/en/cybercrime/convention/home.html

65 African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

4.3 Emerging Threats and Evolving Tactics

A growing share of cybercrime in Africa is powered by new tools and tactics - especially those involving AI, synthetic media, and disinformation. These evolving threats are outpacing the capacity of many national agencies to detect, investigate, or contain them.

- **AI-generated deepfakes and extortion**

  In several countries, criminals have used deepfake videos or voice cloning to extort victims. These AI-driven tools enable convincing impersonations, emotional manipulation, and blackmail - often without requiring advanced technical skills.
- **Disinformation campaigns**

  Some agencies reported cases where fabricated news, altered images and fake social media accounts were used to spread panic, incite unrest, or damage reputations. These attacks typically target trust - weaponizing public information channels.
- **The rise of turnkey attack infrastructure**

  Bulletproof hosting services are increasingly used to support CaaS offerings, giving even low-skilled actors access to phishing kits, malware payloads, and scalable automation hosted on infrastructure designed to evade takedown.

Despite these fast-moving threats, 86% of agencies surveyed have not yet integrated AI into their law enforcement operations.[66] As attackers harness AI to enhance scale and deception, this capability gap risks leaving many national agencies behind.

4.4 Limited Cross-Border Cooperation and Intelligence Sharing

Cybercrime routinely crosses borders, but most African countries face challenges in collaborating internationally. In our survey, 86% of agencies said their cross-border cooperation capacity needs improvement, with 44% rating it as needing significant improvement.

Several key limitations were reported:

- **Slow, formal processes:** Procedures such as Mutual Legal Assistance (MLA) requests and extradition are often too slow to match the speed required for effective cybercrime response, underscoring the need for more agile and streamlined cooperation frameworks.
- **Legal and procedural mismatches:** Differences in laws, digital evidence standards, and data privacy regulations create friction when working across jurisdictions. These legal issues are covered in more detail in Section 4.1.
- **Building operational networks and trust:** Some countries face challenges in identifying or reaching foreign counterparts, and there may be limited established contacts or real-time coordination frameworks, which can sometimes result in missed opportunities for joint action.
- **Limited access to platforms and foreign-hosted data:** Agencies report difficulty obtaining information from platforms or service providers headquartered abroad, especially in cases involving foreign nationals or infrastructure located in other jurisdictions.

Despite these barriers, recent operations coordinated under INTERPOL's AFJOC project show that when trusted channels and joint protocols are in place, regional cybercrime responses can be swift and effective.

66 INTERPOL Cyberthreat Assessment Survey

4.5 Barriers to Public-Private Partnerships and Platform Accountability

Cybercrime investigations increasingly rely on cooperation from private-sector partners, particularly tech platforms, telecom providers, and financial institutions. Yet, most African law enforcement agencies face major barriers in building these relationships.

- **Unclear channels for engagement**

  Agencies often struggle to access data from companies like Meta, TikTok, and Snapchat, citing lack of direct contacts, slow response times, and unclear procedures. Without formal agreements or points of contact, requests are often delayed or ignored.
- **Low institutional readiness**

  Few countries have established a Memorandum of Understanding (MoU) or data-sharing agreements with private companies. At the same time, many agencies lack the technical or legal capacity to make effective, lawful requests.
- **Under-engagement of telecom and fintech sectors**

  Despite their central role in fraud and scams—such as SIM swap fraud and mobile money abuse—telecommunications and financial service providers remain underutilized partners in national cybercrime strategies.

→ Survey data show that 89% of African countries rated their cooperation with the private sector as needing significant or some improvement.[67]

As more digital infrastructure is controlled by private entities, law enforcement's ability to act will increasingly depend on access, trust, and structured cooperation—none of which can be left to chance.

67 INTERPOL Cyberthreat Assessment Survey

5. POSITIVE DEVELOPMENTS IN AFRICA'S CYBERSECURITY LANDSCAPE

Africa has made significant progress in cybersecurity, driven by legal reforms, forensic advancements, public awareness initiatives, regional cooperation, and the adoption of emerging technologies. These developments demonstrate a growing commitment to combating cybercrime and strengthening digital security across the continent.

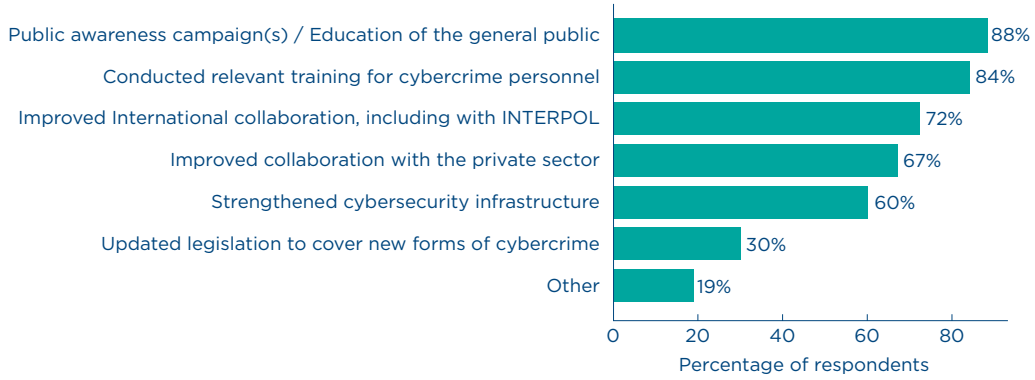


Figure 8: Preventive cybercrime actions implemented by African law enforcement agencies in 2024.

5.1 Strengthening National Cybercrime Frameworks

In 2024, several African nations advanced their legal frameworks to combat cybercrime, reflecting a growing commitment to digital security.

- **Tunisia** became the 70th party to the Budapest Convention on Cybercrime in March 2024, aligning its legal framework with international standards to facilitate cross-border cooperation in combating cybercrime.
- **Nigeria** enacted the Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024, introducing updates to its 2015 legislation. Key changes include the establishment of sectoral Computer Emergency Response Teams (CERTs), clarification of cyberstalking provisions, and the introduction of a cybersecurity levy to fund national initiatives.[68]
- **The Gambia** presented its first dedicated Cybercrime Bill (2023) to Parliament, marking a foundational step toward formalizing its approach to cybercrime.[69]
- **Guinea-Bissau** elaborated its National Cybersecurity Strategy in 2024[70] and has also made significant strides in its broader digital transformation efforts. In January 2025, the government officially launched the National Strategy for Digital Transformation, aimed at improving economic development, data management, governance, and public services.[71]
- Burkina Faso passed Law No. 014-2024/ALT in July 2024, enhancing protection for information systems and codifying responses to cyberthreats including ransomware and online fraud.[72]

These legislative efforts indicate a regional trend towards harmonizing cybersecurity laws with international standards, including references to the Budapest Convention and the United Nations Convention against Cybercrime.

68 https://placng.org/i/documents/cybercrimes-prohibition-prevention-etc-amendment-act-2024/
69 https://mocde.gov.gm/ministry-of-communications-and-digital-economy-of-the-gambia-embarked-on-a-two-day-retreat-to-discuss-the-cybercrime-bill-2023/
70 INTERPOL Cyberthreat Assessment Survey
71 https://unu.edu/egov/news/digital-transformation-project-guinea-bissau-egov-undp
72 https://www.mdenp.gov.bf/fileadmin/user_upload/storages/documents/administratifs/loi_014_systeme_d_information.pdf

5.2 Expanding Institutional and Technical Capabilities

Over the past 18 months, African nations made significant strides in enhancing their cybercrime response capabilities. Investments in specialized units, digital forensics infrastructure, and capabilities development have played a pivotal role in strengthening investigation and enforcement.

- According to survey responses,[73] **67%** of participating countries reported conducting cybercrime-related capacity-building events in 2024, while **44%** stated they had created new - or expanded existing - cybercrime units.
- **Algeria:** In late 2023, Algeria opened a new national headquarters for its Central Cybercrime Unit and expanded operations across all 58 provinces. Units are now segmented by function -surveillance, technical support, and investigations - streamlining enforcement. Ongoing training reinforces these structural reforms.[69] [74]
- **Seychelles:** The Seychelles Police Force has received a suite of digital tools and training equipment from the British government[75] and a digital forensic laboratory donated by the Chinese government[76] in the past 18 months, shortly after setting up their cybercrime unit in 2023.[77] The new tools aim to improve cyber investigations and the quality of digital evidence processing.
- **Benin:** The government established the National Cybercrime Centre (Centre National d'Investigations Numériques, CNIN) to centralize cybercrime investigations and digital forensics.[78] In August 2024, CNIN announced the dismantling of a major cybercriminal network in Comè, demonstrating its operational effectiveness.[79]
- **Togo:** Under its 2024-2028 National Cybersecurity Strategy, Togo is consolidating its cybercrime response by establishing a unified enforcement entity,[80] has opened a new Digital Forensics Laboratory[69] and continues to invest in technical training for investigative personnel.
- **Congo:** In late 2024, the government held specialized training for judicial and law enforcement personnel, covering digital evidence collection and cybercrime investigation techniques.[81]

These developments reflect a broader shift across the continent from fragmented or ad hoc responses to more structured, better-resourced, and increasingly technology-enabled cybercrime enforcement. Continued investment in infrastructure, workforce development, and inter-agency coordination will be critical to sustaining and scaling these gains.

73 INTERPOL Cyberthreat Assessment Survey
74 https://www.horizons.dz/?p=74105
75 http://www.seychellesnewsagency.com/articles/19082/British+government+donates+digital+tech+to+Seychelles+Police+Force+for+better+training+and+results
76 http://www.seychellesnewsagency.com/articles/19616/China+gifts+Seychelles+Police+Force+digital+forensic+lab+to+help+deal+with+cybercrime
77 https://www.nation.sc/articles/16639/cybercrime-unit-in-the-offing--by-vidya-gappy
78 https://cybersecuritymag.africa/benin-renforce-lutte-contre-cybercriminalite-avec-creation-du-cnin
79 https://cybersecuritymag.africa/index.php/le-cnin-demantele-un-vaste-reseau-de-cybercriminels-come-au-benin
80 https://www.togofirst.com/en/justice/2805-14118-togo-to-set-up-single-center-to-fight-cybercrime
81 https://www.wearetech.africa/en/fils-uk/news/tech/congo-hosts-cybersecurity-training-for-judicial-and-law-enforcement

5.3 Increasing Cyber Resilience through Public Awareness

In 2024, 88% of African countries reported conducting public awareness campaigns or educational initiatives aimed at preventing cybercrime, making this the most widespread preventive measure across the continent.

These initiatives typically target vulnerable groups such as students, youth, small business owners, and older citizens, utilizing diverse outreach methods including national TV, radio, social media, SMS alerts, and school programmes.

1. Youth and School-Based Campaigns
Targeting younger audiences remains a strategic focus for many countries, promoting online safety, cyberbullying awareness, and digital literacy.

- **Eswatini:** The Ministry of ICT, in collaboration with ESCCOM and UNESCO, conducted cybersecurity awareness sessions in schools.[82] [83] [84]
- **South Africa:** The Institute of Information Technology Professionals South Africa (IITPSA), through its Special Interest Group for Cybersecurity (SIGCyber) group, hosted the inaugural Cybersecurity Moot Court in Gqeberha. High school students presented arguments on a fictional cyber bullying case before a panel of judges, aiming to deepen their understanding of digital harm and school-level policy solutions.[85]
- **Morocco:** Police have led school-based awareness programmes in partnership with the Ministry of Education and, in May 2024, over 2.1 million people attended the General Directorate of National Security's national open days in Agadir, which featured cybercrime exhibits, student engagement from 845 schools, and the launch of the E-Blagh cybercrime reporting platform.[86] [87]
- Civil society organizations such as Child Online Africa[88] and Better Internet for Kids[89], run programmes like Africa Safer Internet Day, Online Safety and Wellbeing Competition, and Digital Literacy Week, targeting schools, parents, and religious institutions.

2. Mass Media and Social Media Engagement
To maximize reach, countries increasingly rely on social and traditional media platforms for cybercrime prevention messaging.

- **Ghana:** In October 2024, the Cyber Security Authority (CSA) launched the National Cyber Security Awareness Month (NCSAM) under the theme "Combating Misinformation/Disinformation in a Digital Resilient Democracy - Our Collective Responsibility." The campaign featured nationwide media outreach, regional forums, and public education efforts to build digital resilience ahead of national elections.[90]
- **Rwanda:** The National Cyber Security Authority (NCSA) conducted the annual "Tekana Online" campaign throughout October 2024. This initiative utilized television, radio, and social media to educate individuals, families, and organizations on best practices against cyberthreats such as online fraud, ransomware, and phishing.[91]
- **INTERPOL:** In December 2024, INTERPOL ran the #ThinkTwice campaign across its social media platforms. The campaign focused on raising awareness about online threats, including ransomware, phishing, and scams involving generative AI, encouraging users to make informed decisions online.[92]

82 https://independentnews.co.sz/10470/local-news/cybersecurity-awareness-initiative-hits-schools/
83 https://www.facebook.com/story.php?id=100069400350741&story_fbid=850193827303955&
84 https://www.swazilandnews.co.za/fundza.php?nguyiphi=7578&
85 https://www.itweb.co.za/article/iitpsa-sigcyber-raises-awareness-on-cyber-bullying-at-inaugural-moot-court-event/6GxRKqYQrnmqb3Wj
86 https://www.mapnews.ma/fr/actualites/social/jpo-de-la-dgsn-un-nombre-record-de-2120000-visiteurs
87 https://en.hespress.com/85374-moroccan-police-launches-new-platform-e-blagh-to-combat-cybercrime.html
88 https://www.childonlineafrica.org/
89 https://better-internet-for-kids.europa.eu/en/saferinternetday/supporter-listing/africa-safer-internet-day
90 ncsam.csa.gov.gh
91 https://cyber.gov.rw/updates/article/ncsa-launches-cybersecurity-and-data-protection-awareness-campaign/
92 https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-campaign-warns-against-cyber-and-financial-crimes

3. Community-Based Awareness and Cultural Engagement

Localized campaigns using familiar languages and cultural channels are especially effective in underserved and rural communities.

- **Chad:** Authorities in N'Djamena implemented cybercrime awareness programmes using local artists and private radio stations - a strategic choice in a country with varying literacy rates where many communities rely on oral communication. These campaigns used local languages and culturally familiar messaging to educate residents about online scams, helping extend outreach to populations not easily accessed through written or digital content.[93]
- **Democratic Republic of Congo:** Police organize monthly public events to return recovered stolen phones to their rightful owners. Conducted in partnership with the national telecom regulator and the public prosecutor's office, the initiative is widely publicized and aims to discourage the purchase of second-hand phones. These devices are often linked to cybercrimes such as identity theft, extortion, and defamation. The campaign has significantly raised awareness and contributed to reducing such offenses.[89]

4. Institutional and Cross-Sector Delivery Channels

Some of the most wide-reaching awareness campaigns in Africa are delivered through coordinated structures involving multiple ministries, law enforcement agencies, and civil society groups. These institutional partnerships improve reach, messaging consistency, and credibility.

- **Algeria:** Algeria's specialized departments for combating cybercrime coordinated closely with the Ministry of Education, the Ministry of Post and Telecommunications, and civil society organizations to deliver public awareness campaigns. These efforts targeted diverse audiences and were rolled out periodically across a range of platforms, including radio, television, social media, public forums, and advertisements. Authorities monitored effectiveness through social media engagement, increased reporting of cybercrime, and broader public adoption of preventive behaviours.

5.4 Strengthened Law Enforcement Operations

African countries demonstrated increased operational capacity and international collaboration in 2024, particularly through two high-impact cybercrime crackdowns coordinated by INTERPOL.

- **Operation Serengeti** (September-October 2024) was one of the most significant cybercrime enforcement actions on the continent to date. Coordinated by INTERPOL and AFRIPOL, and involving 19 African countries, the operation led to over 1,000 arrests, the dismantling of 134,000 malicious online infrastructures, and the identification of more than 35,000 victims. Authorities targeted ransomware operators, BEC fraudsters, digital extortionists, and investment scam networks. Total financial losses linked to the criminal schemes disrupted during the operation were estimated at USD 193 million globally. Private sector partners, including ISPs, supported the operation by helping take down infrastructure and secure digital platforms.[94]
- **Operation Red Card** (October 2024 – March 2025), conducted under Project AFJOC, brought together cybercrime units from Côte d'Ivoire, Benin, Togo, Rwanda, South Africa, Zambia, and Nigeria. The operation dismantled an online loan scam network by analysing domains, APK files, and social media profiles. Private sector intelligence contributed to Cyber Activity Reports, which were instrumental in identifying criminal infrastructure and threat actors.[95]

Together, these operations signal a growing ability among African countries to participate in complex cross-border cybercrime investigations enabled by stronger coordination, intelligence-sharing frameworks, and public-private collaboration.

93 INTERPOL Cyberthreat Assessment Survey

94 https://www.interpol.int/en/News-and-Events/News/2024/Major-cybercrime-operation-nets-1-006-suspects

95 https://www.interpol.int/en/News-and-Events/News/2025/More-than-300-arrests-as-African-countries-clamp-down-on-cyber-threats

6. RECOMMENDATIONS AND CONCLUSION

In response to the threats, systemic challenges, and capacity gaps identified in this assessment, INTERPOL proposes the following strategic recommendations for law enforcement agencies, policymakers, regional bodies, and international partners. These recommendations are grounded in member country feedback, operational insights, and observed trends, and are intended to guide sustainable, practical, and coordinated improvements to Africa's cybercrime response capabilities.

The recommendations are organized into six thematic areas:

- Strengthening National Capabilities.
- Enhancing Legal and Policy Frameworks.
- Improving Regional and International Cooperation.
- Expanding Prevention and Public Awareness.
- Deepening Public-Private Partnerships.
- Leveraging Emerging Technologies for Cybercrime Prevention.

6.1 Strengthening National Capabilities

African law enforcement agencies must be supported in building the operational, technical, and institutional capacity required to detect, investigate, and disrupt cybercrime effectively. Many countries have made progress, but disparities persist across the continent. Priorities should include:

- establishing and expanding dedicated cybercrime units with sufficient staffing, mandate, and technical resources at the national level;
- investing in cybercrime-specific training for investigators, analysts, prosecutors, and judges, including in areas such as digital forensics, malware analysis, open-source intelligence (OSINT), and financial tracking;
- ensuring sustainable access to modern investigative tools, including licensed digital forensic software and secure digital evidence storage;
- developing and operationalizing national and sectoral Computer Incident Response Teams (CIRTs) with clear protocols for inter-agency coordination;
- retaining specialized cybercrime officers through clear career paths and incentives, to reduce talent drain and ensure long-term effectiveness.

Sustained investment in national capacity is the backbone of an effective and autonomous cybercrime response ecosystem.

6.2 Enhancing Legal and Policy Frameworks

Cybercrime enforcement depends on the existence of robust, current, and enforceable legal frameworks. However, many African countries continue to face legislative gaps that limit their ability to prosecute cyber offenders, access cross-border evidence, or cooperate internationally.

To address these issues, INTERPOL recommends:

- accelerating the adoption and implementation of comprehensive national cybercrime laws, aligned with international standards and covering both cyber-dependent and cyber-enabled crimes;
- ensuring the legal recognition and admissibility of digital evidence, including evidence acquired across borders;
- harmonizing legal definitions and procedures across jurisdictions, to reduce legal fragmentation and enable more effective regional cooperation;
- ratifying and operationalizing international and regional conventions, such as the Budapest Convention on Cybercrime, the African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention) and the UN Convention against Cybercrime;
- developing clear legal pathways for timely access to data held by foreign-based platforms, including through Mutual Legal Assistance Treaties (MLATs) or emergency disclosure frameworks.

Legal reform is a necessary step toward building confidence in law enforcement capabilities and ensuring accountability for cybercriminal activity. These efforts must be matched by investments in judicial training and prosecutorial specialization.

6.3 Improving Regional and International Cooperation

Given the inherently transnational nature of cybercrime, no country can tackle the threat alone. Regional and global cooperation is essential for pursuing cross-border investigations, disrupting threat actor infrastructures, and sharing intelligence in real time.

To strengthen collective response capacity, INTERPOL recommends:

- ratifying and implementing international cybercrime treaties, such as the United Nations Convention against Cybercrime and the Budapest Convention on Cybercrime, to enable faster cross-border investigations and extradition of cybercriminals;
- strengthening intelligence-sharing mechanisms among African nations by expanding participation in AFJOC and other regional and international cybercrime programmes.
- institutionalizing cross-border investigative mechanisms, including formalized processes for evidence sharing, case referrals, and parallel investigations;
- utilizing secure communication platforms, such as INTERPOL's I-24/7 channel, for rapid law enforcement coordination across borders.
- supporting joint operations and multi-country task forces, focused on disrupting cybercriminal networks operating across the region.

INTERPOL and AFRIPOL remain committed to facilitating structured cooperation across Africa and with global partners. Sustained collaboration will be essential to closing enforcement gaps and tackling organized cybercrime groups operating beyond national borders.

6.4 Expanding Prevention and Public Awareness

While technical capabilities and legal tools are essential to fighting cybercrime, prevention remains the most cost-effective and scalable line of defence. Many cybercrimes in Africa - such as phishing, online scams, and romance fraud - rely on social engineering and exploit low levels of digital awareness.

To strengthen prevention efforts, INTERPOL recommends:

- launching targeted public awareness campaigns, particularly for high-risk groups such as youth, women, Small and Medium Enterprises (SMEs), and first-time Internet users;
- integrating cybersecurity education into school curricula, vocational training, and adult learning programmes;
- promoting basic cyber hygiene practices, such as strong password use, multi-factor authentication, and reporting of suspicious messages;
- encouraging victims to report incidents, by strengthening trust in law enforcement and ensuring confidentiality, especially in cases of sextortion or online fraud;
- engaging local civil society organizations, including women's groups and youth networks, to help disseminate prevention messages in culturally relevant ways.

By empowering individuals and communities with the knowledge to recognize and avoid cyberthreats, countries can reduce victimization, shrink the cybercriminal target pool, and ease the investigative burden on law enforcement.

6.5 Deepening Public-Private Partnerships

Cybercrime investigations often depend on data, infrastructure, and insights held by private sector entities - including telecommunications providers, financial institutions, social media platforms, and cybersecurity firms. Yet law enforcement across Africa continues to face barriers in accessing timely information and technical support from these actors.

To build a more collaborative ecosystem, INTERPOL recommends:

- formalizing channels of cooperation between law enforcement and key private sector stakeholders, including frameworks for secure and lawful data sharing;
- establishing and joining national and regional cybercrime coordination forums (e.g. the INTERPOL Cybercrime Expert Group), bringing together regulators, investigators, prosecutors, and private sector actors to align priorities and share intelligence;
- facilitating timely access to digital evidence from global platforms, through improved legal agreements, technical protocols, and trusted communication channels;
- leveraging private sector expertise and infrastructure in areas such as threat intelligence, malware analysis, and incident response;
- encouraging private sector contributions to capacity-building initiatives, including training, toolkits, and mentorship programmes for public sector personnel.

By fostering trust and operational alignment between the public and private sectors, countries can unlock critical capabilities and accelerate the disruption of cybercriminal networks.

6.6 Leveraging Emerging Technologies for Cybercrime Prevention

As cyberthreats evolve, so must the tools and strategies used to combat them. Artificial intelligence, machine learning, data analytics, and automation present new opportunities for law enforcement to anticipate, detect, and disrupt cybercriminal activity at scale. However, adoption of these technologies remains uneven across African countries.

To promote more proactive and data-driven enforcement, INTERPOL recommends:

- exploring the use of AI and machine learning tools for phishing detection, anomaly detection, and digital evidence triage;
- developing national and regional data analytics capabilities to track cybercrime patterns and support real-time threat monitoring;
- investing in secure cloud-based infrastructure for case management, digital forensics, and cross-border information exchange;
- •testing automation tools for evidence collection, incident response, and network monitoring within law enforcement agencies;
- building ethical and legal frameworks for the responsible use of emerging technologies in cybercrime investigations, taking inspiration from INTERPOL's Innovation Centre (IC) initiatives on artificial intelligence.

Emerging technologies offer a path to faster, smarter, and more scalable enforcement - but only if deployed cautiously and with the necessary safeguards.

ABOUT INTERPOL

INTERPOL is the world's largest international police organization. Its role is to assist law enforcement agencies in the Organization's 196 member countries to combat all forms of transnational crime. It works to help police across the world meet the growing challenges of crime in the 21st century by providing a high-tech infrastructure of technical and operational support. The Organization's services include targeted training, expert investigative support, specialized databases, and secure police communications channels.

INTERPOL'S VISION: CONNECTING POLICE FOR A SAFER WORLD

INTERPOL's vision is that of a world where each and every law enforcement professional will be able to use the Organization to securely communicate, share, and access vital police information whenever and wherever needed, to ensure the safety of the world's citizens. INTERPOL constantly provides and promotes innovative and cutting-edge solutions to global challenges in policing and security.

ABOUT THE INTERPOL CYBERCRIME PROGRAMME

In a dynamic digital age, where over half the global population is at potential risk from cybercrime, the INTERPOL Global Cybercrime Programme stands in support of the international law enforcement community. We are dedicated to developing and leading a global response to prevent, detect, investigate, and disrupt cybercrime with the ultimate goal of helping member countries combat transnational cybercrime more effectively.

The INTERPOL Global Cybercrime Strategy focuses on four main objectives:

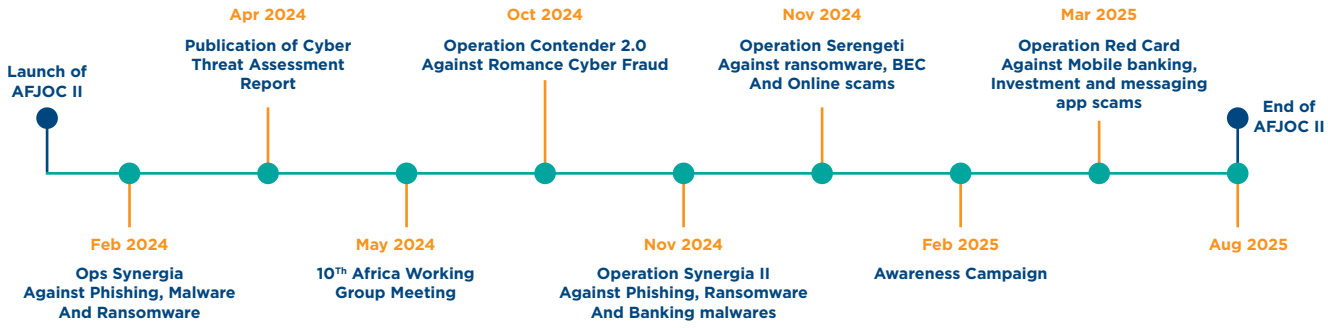
- Enabling a proactive and agile approach to the prevention and disruption of cybercrime by developing an in-depth understanding of the cybercrime threat landscape through information sharing and intelligence analysis.
- Effectively preventing, detecting, investigating, and disrupting cybercrime that causes significant harm on a national, regional, and global scale by leading, coordinating, and supporting member countries in transnational operational activities.
- Supporting the development of member countries' strategies and capabilities for combating cybercrime by cultivating open, inclusive, and diverse partnerships and building trust in the global cybersecurity ecosystem.
- Promoting INTERPOL's role and capabilities in shaping global security by participating in international forums in the field of cybercrime.

We implement our Strategy and objectives via a simple and constructive delivery model, which consists of three core pillars:

- Cybercrime Threat Response: Addressing immediate and emerging cyberthreats with a rapid and coordinated response;
- Cybercrime Operations: Implementing coordinated regional and global operational strategies to combat cybercrime effectively;
- Cyber Capabilities Development: Enhancing strategies and capabilities through innovative projects and platforms.

Underpinning these pillars is our extensive network of public-private partnerships, which fosters collaboration and leverages collective expertise to fight cybercrime.

For any further information, please contact the INTERPOL Cybercrime Directorate at the following email address: EDPS-CD@interpol.int



ABOUT THE INTERPOL AFRICA JOINT OPERATION AGAINST CYBERCRIME

AFJOC is an INTERPOL initiative aimed at strengthening the capability of African national law enforcement agencies to prevent, detect, investigate, and disrupt cybercrime. This is achieved by:

- gathering and analysing information on cybercriminal activity;
- carrying out intelligence-led, coordinated action;
- promoting cooperation and best practice amongst African member countries.

Phase 1 of the initiative was funded by the United Kingdom Foreign, Commonwealth & Development Office, and ran from 2021 to 2023. The second phase, still supported by the UK FCDO, is building upon the achievements of the first, and aims to further enhance the capabilities of national law enforcement agencies in Africa.

Project Activities

- Analytical support and intelligence - timely and accurate intelligence is vital in any effective law enforcement response to cybercrime. Our Cyber Activity Reports are important resources, providing insight on cyberthreats targeting specific countries or regions.
- Developing regional capacity and capabilities to combat cybercrime - collaborative platforms such as the Cybercrime Collaborative Platform and the Cyber Fusion Platform allow for secure communication and the exchange of data on operations.
- Joint Operational Framework - this addresses cybercrime threats through collaboration between law enforcement agencies, the private sector, and other international/ intergovernmental organizations.
- Operational support and coordination - our operations help dismantle the criminal networks behind cybercrime.
- Awareness-raising campaigns - promoting good cyber practices among individuals and businesses in Africa.
- Working group meetings for heads of units - bringing together representatives from nearly all African countries to address regional cybercrime challenges and strengthen operational collaboration through side meetings and strategic discussions.

The INTERPOL African Cybercrime Operations Desk is responsible for implementing the AFJOC project. It works in close partnership with key regional stakeholders, in particular the African Union mechanism for police cooperation, AFRIPOL, law enforcement communities, and the private sector.

Contact

Africa Cybercrime Operations Desk
AfricaDesk@interpol.int

INTERPOL

INTERPOL HQ

@INTERPOL_HQ

INTERPOL

INTERPOL HQ

INTERPOL_HQ