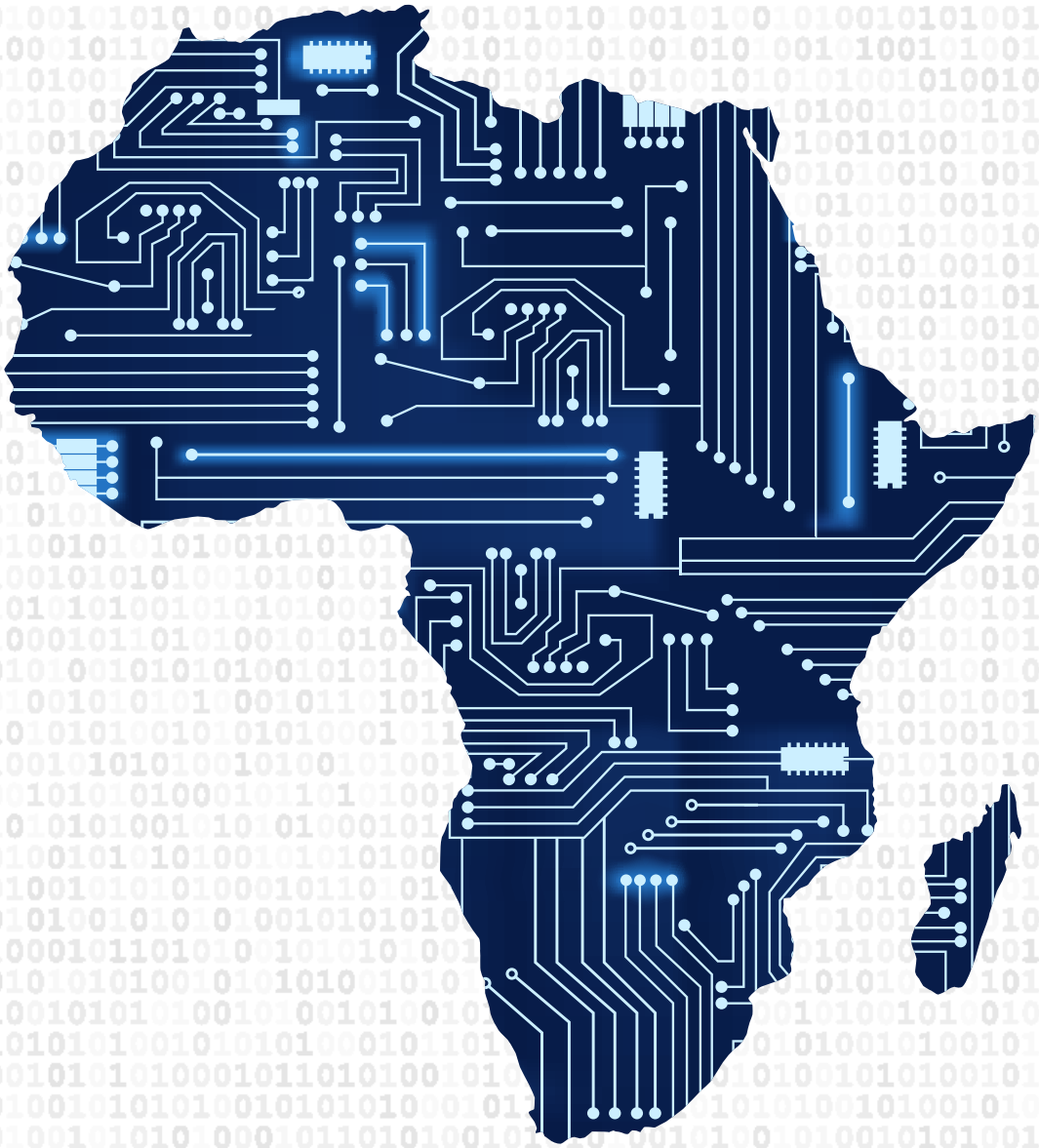
INTERPOL

INTERPOL AFRICAN CYBERTHREAT ASSESSMENT REPORT 2026



JUNE 2026

DISCLAIMER

This report must not be reproduced in whole or in part and in any form without special permission from the copyright holder. When the right to reproduce this report is granted, INTERPOL would appreciate receiving a copy of any publication that uses it as a source.

This report has not been formally edited. The content of this report does not necessarily reflect the views or policies of INTERPOL, its member countries, its governing bodies or contributory organizations, nor does it imply any endorsement.

The boundaries and names shown, and the designations used on any maps, do not imply official endorsement or acceptance by INTERPOL. The designations employed and the presentation of the material in this report do not imply the expression of any opinion whatsoever on the part of INTERPOL concerning the legal status of any country, territory, city, or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Any reference to third-party names is for appropriate acknowledgement of their ownership and does not constitute a sponsorship or endorsement of such owner. INTERPOL does not endorse or recommend any commercial product, process, or service.

All reasonable precautions have been taken by INTERPOL to verify the information contained in this report. However, the published material is being distributed without warranty of any kind, either expressed or implied. The responsibility for the interpretation and use of the material lies with the reader. In no event shall INTERPOL be liable for damages arising from its use.

INTERPOL takes no responsibility for the continued accuracy of the information or for the content of any external website. Any links to external websites do not constitute an endorsement by INTERPOL and are only provided as a convenience. It is the responsibility of the reader to evaluate the content and usefulness of information obtained from other sites. INTERPOL has the right to alter, limit, or discontinue the content of this report.

INTERPOL General Secretariat
200, quai Charles de Gaulle
69006 Lyon
France
Telephone + 33 4 72 44 70 00
Fax + 33 4 72 44 71 63
Web: www.INTERPOL.int
E-mail: info@INTERPOL.int

CONTENTS

FOREWORD

Cybercrime now poses a growing and systemic threat to the economic security, public confidence, and institutional resilience of African countries. As this **INTERPOL African Cyberthreat Assessment Report 2026** makes clear, we are witnessing a defining shift: cyber-criminality has evolved from isolated incidents into an industrialized, borderless ecosystem.

Drawing on critical intelligence from law enforcement in 36 African member countries, and reinforced by insights from INTERPOL's private sector partners, this report reveals a threat landscape defined by speed, scale, and constant adaptation. Traditional cyberthreats such as ransomware, business e-mail compromise, data breaches, and online scams remain deeply damaging, with offenders continuously refining their methods and tools. At the same time, a new tier of threats is expanding the reach and sophistication of criminal networks. The growth of AI-enabled phishing, AI-driven sextortion, deepfake-based deception, and cybercrime-as-a-service reflects a dangerous evolution in both capability and intent.

Of particular concern is the way these threats intersect with broader structural vulnerabilities. In many parts of the continent, cybercrime flourishes where digital adoption outpaces legislation, technical capacity, and law enforcement's ability to access and act on digital evidence. Scam centres linked to human trafficking and coercion, fraud schemes targeting vulnerable communities, and attacks against essential services and critical infrastructure all point to the same reality: cybercrime is not only a technical problem. It is a defining issue for economic development, public safety, and human security.

Given the scale of the challenge, our response must be collective, coordinated, and operational. No country can address these threats in isolation, and no single institution can match the agility of criminal networks operating across borders. Through the Africa Joint Operation against Cybercrime (AFJOC), and in close partnership with member countries and trusted private sector stakeholders, INTERPOL is strengthening the mechanisms that make coordinated enforcement possible – from intelligence exchange and operational planning to technical support and targeted disruption.

This report highlights clear grounds for optimism. Across Africa, law enforcement agencies are strengthening specialized capabilities, enhancing legislative frameworks, and deepening cross-border cooperation. Operational successes in 2025 show that when countries work together, cybercriminal infrastructure can be identified, disrupted, and dismantled. But this progress must now be matched by stronger cooperation mechanisms, sustained investment in cybersecurity, and a collective commitment to capacity building.

I extend my sincere appreciation to my team in the African Cybercrime Operations Desk, our member countries, all the partners who contributed to this assessment, and to the United Kingdom's Foreign, Commonwealth & Development Office (FCDO) who have funded and supported these efforts. This teamwork reflects a shared determination to confront cybercrime with clarity, professionalism, and resolve. By acting together, we can strengthen trust in Africa's digital future and better protect the communities, institutions, and economies that depend on it.

Neal Jetton
Director, Cybercrime
INTERPOL

ABBREVIATIONS AND ACRONYMS

ACRONYM	FULL TITLE
AFJOC	African Joint Operation against Cybercrime
AFRIPOL	African Union Mechanism for Police Cooperation
AU	African Union
BEC	Business E-mail Compromise
CaaS	Cybercrime-as-a-Service
CERT	Computer Emergency Response Team
CIRT	Computer Incident Response Team
DDoS	Distributed Denial-of-Service
ENCVR	École Nationale de Cybersécurité à Vocation Régionale
EAPCCO	Eastern Africa Police Chiefs Cooperation Organization
ECOWAS	Economic Community of West African States
FCDO	Foreign, Commonwealth and Development Office (United Kingdom)
GLACY-e	Global Action on Cybercrime Enhanced
ICT	Information and Communication Technology
I-24/7	INTERPOL's secure global communication system
ITU	International Telecommunication Union
KYC	Know Your Customer
MLAT	Mutual Legal Assistance Treaty
MoU	Memorandum of Understanding
NBS	Nigerian Bureau of Statistics
NIN-SIM	National Identification Number – Subscriber Identity Module
OIBSA	Online Image-Based Sexual Abuse
PPP	Public-Private Partnership
SAWS	South African Weather Service
SADC	Southern African Development Community
SIM	Subscriber Identity Module
SOW	Secure Our World (South African public awareness campaign)
TTPs	Tactics, Techniques, and Procedures
US	United States of America
VASP	Virtual Asset Service Provider

ACKNOWLEDGEMENTS

This report was developed by the INTERPOL Africa Cybercrime Operations Desk in close coordination with the African Joint Operation against Cybercrime (AFJOC), under the funding and strategic support of the United Kingdom's Foreign, Commonwealth & Development Office (FCDO). The analysis is the product of a comprehensive, multi-source intelligence synthesis process, incorporating quantitative and qualitative data from 36 African member countries that completed the INTERPOL Africa Cyberthreat Assessment Survey in 2025.

Additional analytical depth was derived from telemetry feeds and threat intelligence shared by INTERPOL's private sector partners – including Fortinet, Mastercard, the Shadowserver Foundation, S2W, and TrendAI – as well as operational insights from INTERPOL's own cyber intelligence and operational units. The report also draws upon open-source reporting, verified through cross-referencing with law enforcement cases.

We extend our sincere gratitude to the national law enforcement agencies, cybersecurity units, judicial authorities, and telecommunications regulators across Africa who contributed their time, expertise, and operational experience to this assessment. Their collaboration remains the foundation of any meaningful progress against transnational cybercrime.

EXECUTIVE SUMMARY

Cybercrime continues to evolve as a transnational and systemic threat across Africa, undermining economic stability, eroding public trust in digital services, and compromising the integrity of critical infrastructure. In 2025, the region experienced an intensification of cyberthreats driven by rapid digital transformation, persistent capacity deficits, and the increasing exploitation of emerging technologies — particularly artificial intelligence (AI). These developments have created an environment in which criminal actors operate with greater speed, scale, and sophistication, often exploiting jurisdictional fragmentation and institutional gaps to evade detection and prosecution.

Law enforcement capacity across the continent remains unevenly distributed. While several member countries have established dedicated cybercrime units and begun investing in digital forensic laboratories, secure communications infrastructure, and specialized training programmes, many others continue to operate with severe constraints. These include insufficient staffing, outdated or non-interoperable tools, and a shortage of certified cybercrime investigators. As a result, national units often lack the technical capability to conduct timely forensic analysis, preserve digital evidence in accordance with international standards, or respond effectively to incidents involving encrypted platforms, cryptocurrency transactions, or AI-generated content.

Legal and policy frameworks have expanded at the national level, with several member countries adopting comprehensive cybercrime legislation aligned with the African Union's (AU) Malabo Convention on Cyber Security and Personal Data Protection. However, significant disparities persist in implementation, enforcement, and harmonization. In many jurisdictions, laws face challenges related to outdated provisions, resource constraints, or inconsistent application. Mutual legal assistance (MLA) processes can sometimes experience delays due to administrative complexities, unclear points of contact, and varying levels of familiarity with international legal frameworks. The absence of a unified regional framework for digital evidence exchange further impedes transnational investigations, particularly in cases involving cross-border ransomware attacks, business e-mail compromise (BEC), and online image-based sexual abuse (OIBSA).

Cross-border cooperation is further complicated by jurisdictional obstacles, divergent data protection regulations, and the absence of formalized information-sharing protocols between national cybercrime units. The fragmentation of legislative approaches, from definitions of cybercrime to the admissibility of electronic evidence, enables criminal networks to exploit legal vacuums and relocate operations rapidly across borders. This is compounded by under-resourced regional bodies, which lack the authority, funding, and technical infrastructure to coordinate sustained operational responses.

The proliferation of AI has fundamentally altered the threat landscape. Cybercriminals are now deploying AI-powered tools to automate phishing campaigns, generate convincing deepfakes for identity fraud and social engineering, create synthetic identities for financial fraud, and evade detection by traditional signature-based security systems. AI-driven ransomware variants, such as those associated with the Qilin and Akira groups, are increasingly targeting healthcare systems, power utilities, and educational institutions, disrupting essential services and extorting payments in cryptocurrency. The availability of Cybercrime-as-a-Service (CaaS) platforms on the dark web has further democratized access to advanced attack tools, allowing even low-skill actors to conduct high-impact operations with minimal technical expertise.

This report synthesizes operational trends, threat indicators, and systemic challenges observed across 36 African member countries during 2025. It draws on data collected through INTERPOL's Africa Cyberthreat Assessment Survey (hereafter referred to as the INTERPOL member country survey), national incident reports, data from private cybersecurity vendors, and regional law enforcement agencies. The findings are not intended as a general overview, but as a targeted intelligence assessment to inform strategic decision-making by national authorities, regional bodies, and international partners.

The report concludes with a series of evidence-based recommendations aimed at strengthening cyber resilience through legal harmonization, interoperable technical capacity, sustained operational coordination, and the institutionalization of investigative practices. Addressing these challenges requires more than technological investment and demands a unified, rules-based, and cooperative approach to cybercrime, anchored in the principles of sovereignty and collective security.

INTRODUCTION

Africa's digital transformation continues at an accelerating pace. With more than 1.1 billion mobile subscriptions and more than USD 1.1 trillion in digital transactions recorded in 2025, the continent has become a critical node in the global digital economy.[1] More than 570 million Internet users now rely on digital platforms for financial services, government access, healthcare, and education. This rapid adoption, while economically empowering, has outpaced the development of cybersecurity infrastructure, regulatory frameworks, and institutional capacity, creating a high-risk environment for cybercriminal exploitation.

In response, INTERPOL conducted a comprehensive survey among 49 African member countries, with 36 responses or 73 per cent response rate (Central Africa: 63 per cent; East Africa: 56 per cent; S. Africa: 85 per cent; West Africa: 94 per cent), gathering high-level insights from law enforcement agencies, national cybersecurity units, and judicial authorities. The findings were cross-referenced with telemetry data from private sector partners, including Fortinet, TrendAI, the Shadowserver Foundation, Mastercard, and S2W, to validate trends and eliminate reporting bias. This multi-source methodology ensured the accuracy of observed patterns, particularly in regions with limited incident reporting.

This report focuses exclusively on cybercrime trends observed between January and December 2025. It does not speculate beyond the data provided, projections, or unverified claims. Its purpose is to deliver a clear, evidence-based, and actionable intelligence assessment – one that reflects the realities faced by African nations on the frontlines of cybercrime.

This report aims to highlight the major contemporary cybercriminal trends facing Africa at both the continental and regional levels. Each section is grounded in a comprehensive analysis of information and responses provided by African member countries, incident and trend data provided by INTERPOL's private partners, and referenced open-source information from high-fidelity sources. These data points have been collated and synthesized to produce actionable insights and recommendations for strategic-level decision makers within national-level law-enforcement, national-level cybersecurity agencies, and regional cybersecurity organizations.

1 GSMA The Mobile Economy Africa 2025 (https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2025/10/GSMA_AFRICA_ME2025_R_Web-3.pdf) (January 2026).

THE CONTEMPORARY AFRICAN CYBERTHREAT LANDSCAPE

Africa's digital economy continues to expand at an unprecedented scale, underpinned by rapid technological adoption, mobile connectivity growth, and the digitalization of core public and private sector services. In 2025, the continent recorded more than 1.1 billion mobile subscriptions and facilitated more than USD 1.1 trillion in digital transactions,[2] reinforcing its position as a critical node in the global digital ecosystem. With approximately 570 million Internet users, critical infrastructure sectors including financial services, healthcare, government administration, and telecommunications have become increasingly exposed to systemic cyberthreats.[3]

The proliferation of emerging technologies, including AI, the Internet of Things (IoT), and blockchain technology, has introduced new vectors for exploitation. While these innovations drive efficiency and inclusion, they have also been weaponized by cybercriminal actors to conduct scalable, automated, and highly targeted attacks. Ransomware, supply-chain compromises, and data breaches remain persistent and escalating threats. A high volume of data breaches was observed, relating to users and organizations originating from South Sudan, South Africa, Nigeria, and Namibia, between January 2024 and September 2025.[4] Ransomware incidents were similarly prevalent across South Africa, Nigeria, Namibia, Senegal, and Zambia, with attackers increasingly targeting healthcare institutions, utility providers, and public service portals to maximize disruption and extortion potential.[5]

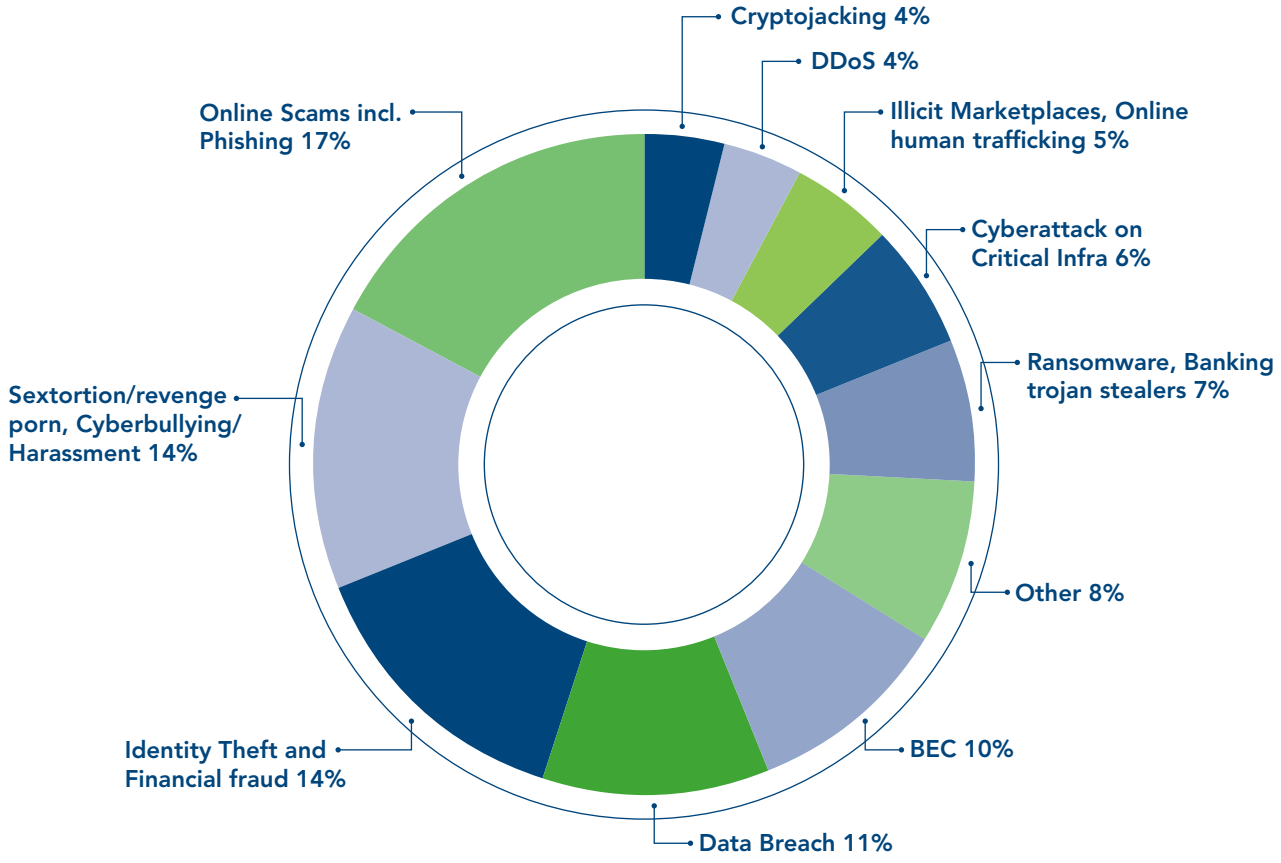


Figure 1: Reported cybercrime cases by type in 2025 (Source: INTERPOL member country survey).

2 GSMA The Mobile Economy Africa 2025 (https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2025/10/GSMA_AFRICA_ME2025_R_Web-3.pdf) (January 2026).

3 Serianu Limited Africa Cybersecurity Report – Kenya 2024/2025 (https://www.serianu.com/downloads/Africa%20Cybersecurity%20Report%20-%20Kenya.pdf) (January 2026).

4 SOCRadar Africa Threat Landscape 2025 (https://socradar.io/wp-content/uploads/2025/09/Africa-Threat-Report.pdf) (December 2025).

5 SOCRadar Africa Threat Landscape 2025 (https://socradar.io/wp-content/uploads/2025/09/Africa-Threat-Report.pdf) (December 2025).

Cybersecurity capacity across the continent remains uneven, characterized by diverging legal frameworks, insufficient investment in digital defence infrastructure, and persistent gaps in digital literacy and institutional awareness. These weaknesses are amplified by the pace of digital adoption, which often outpaces the development of protective mechanisms. As a result, cybercrime has emerged as one of the most significant criminal threats to the region. Member countries across West and Southern Africa who responded to the INTERPOL member country survey estimate that cybercrime now likely accounts for more than 30 per cent of all recorded crimes. This represents a marked increase from the previous year and reflects the growing operational sophistication of criminal networks due to the inclusion of Southern Africa; the region only accounted for between 10 to 30 per cent of reported cybercrime in 2024.

Online scams remain the most frequently reported cybercrime type across the region, often serving as the initial entry vector for identity theft and subsequent financial fraud. These incidents form a cascading threat chain: compromised credentials lead to unauthorized access to financial accounts, digital wallets, and government services, enabling large-scale monetary extraction. BEC continues to be the most financially damaging attack vector and a more frequent outcome attack (21 per cent) driven by identity compromise in 2025.[6] Digital sextortion and online harassment, often facilitated by AI-generated deepfakes and synthetic media, remain pervasive, particularly affecting vulnerable populations and undermining trust in digital communication channels.

The financial toll of cybercrime in Africa has intensified dramatically. Between 2024 and 2025, reported cybercrime-related losses more than doubled, rising from USD 192 million to USD 484 million.[7] The number of identified victims increased from 35,000 to 87,000, driven primarily by AI-facilitated scams, credential harvesting, and automated social engineering campaigns. While comprehensive national data on financial losses remain inconsistent due to underreporting and divergent reporting methodologies, aggregated estimates suggest that cybercrime inflicted at least USD 5 billion in direct economic damage across Africa in 2025, as compared to the region's total cybersecurity expenditure of USD 15.3 billion.[8] This imbalance underscores a critical strategic vulnerability: **whilst defensive investment has grown, the scale and velocity of offensive operations continue to increase.**

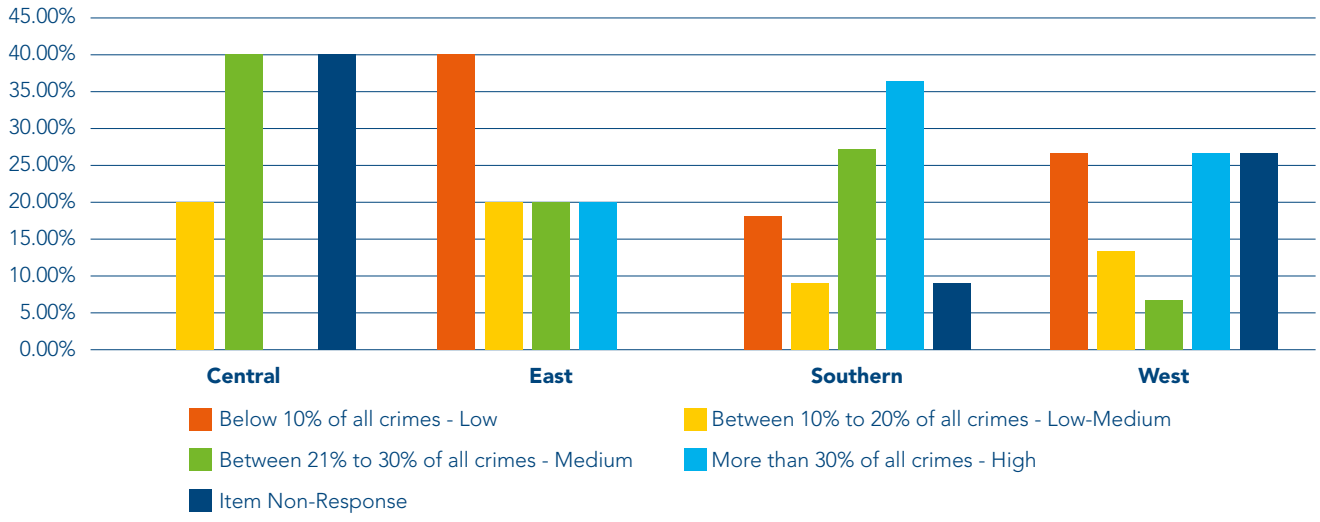


Figure 2: Perceived level of cybercrime as a percentage of all reported crime across Africa region-by-region in 2025 (Source: INTERPOL member country survey).

6 Microsoft Digital Defense Report 2025 (https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf) (December 2025).

7 Microsoft Digital Defense Report 2025 (https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf) (December 2025).

8 Serianu Limited Africa Cybersecurity Report – Kenya 2024/2025 (https://www.serianu.com/downloads/Africa%20Cybersecurity%20Report%20-%20Kenya.pdf) (January 2026).

The sectors most affected remain financial services, telecommunications, and government institutions, all of which serve as central nodes in the digital economy.[9] Ransomware attacks on public utilities and healthcare systems have disrupted essential services, while data breaches have exposed sensitive personal and biometric information, including national identification numbers (NIN) and subscriber identity module (SIM) linkages, enabling large-scale identity fraud. The widespread use of mobile money platforms, while enhancing financial inclusion, has also created new attack surfaces, particularly in countries where Know Your Customer (KYC) protocols are weak or inconsistently enforced.

The African cyberthreat landscape is no longer defined by isolated incidents conducted by threat actors, but by a coordinated, transnational criminal ecosystem. Cybercriminal networks operate across borders with minimal friction, leveraging diverging legal jurisdictions, under-resourced law enforcement, and limited cross-border information-sharing mechanisms. Effective prosecution is often complex due to the diverse application of mutual legal assistance treaty (MLAT)[10] procedures and differing technical capacity among National Central Bureaus (NCBs) present ongoing challenges for investigation. Despite these challenges, member countries are demonstrating increasing resilience through enhanced national capabilities and regional coordination mechanisms.

REGIONAL CYBERTHREAT TRENDS AND INSIGHTS ACROSS AFRICA

The cyberthreat landscape in Africa is not monolithic. Regional disparities in digital maturity, economic development, legal infrastructure, and institutional capacity have produced distinct threat clusters, each with its own dominant threat vectors, actor profiles, and operational patterns. The data reveal four primary threat ecosystems: the Southern region, characterized by high connectivity and high-impact incidents; the West, where fraud and scam cases are most frequently reported; and the East, driven by mobile money platforms, with Central Africa emerging as a zone of underreported but escalating social engineering and botnet activity.

Malware detection statistics also demonstrate regional differences in the distribution of the types of malware being used. The Southern region sees prominent use of trojan-spy, or infostealer malware, trojans, and backdoor malware, which are potentially used as smokescreens to deploy ransomware. Ransomware and cryptocurrency mining threats remain prevalent in the Western region, while multi-mutating worms, grayware, and viruses are prevalent. The Eastern region is minimally affected by trojans and high in virus detections, possibly indicating that perpetrators are keen on mobile-money fraud schemes rather than malware-centric attacks. The Central region is affected by trojans, backdoors, worms, and viruses.

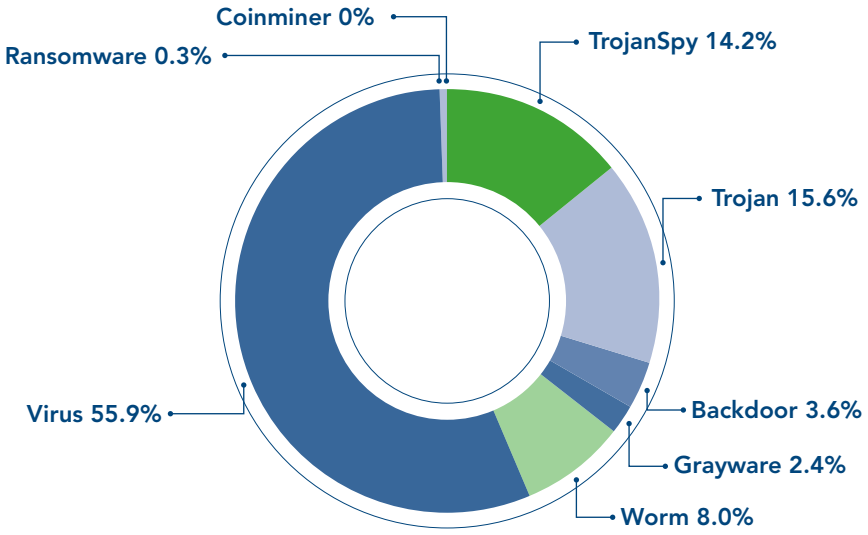


Figure 3: 2025 malware detections by type in Africa (Source: TrendAI).

9 Serianu Limited Africa Cybersecurity Report – Kenya 2024/2025 (https://www.serianu.com/downloads/Africa%20Cybersecurity%20Report%20-%20Kenya.pdf) (January 2026).

10 Chatham House The AU can help African countries adopt the UN cybercrime convention. But the challenges are significant 2025 (https://www.chathamhouse.org/2025/10/au-can-help-african-countries-adopt-un-cybercrime-convention-challenges-are-significant) (April 2026).

CENTRAL AFRICA

Central and West Africa experienced the highest rates of human-related incidents compared to other regions, with up to 75 per cent linked to employee behaviour.[11] BEC and romance scams proliferated, often delivered through French-language phishing lures targeting both corporate and individual victims. Mobile credit application fraud became more prevalent in Côte d'Ivoire, while Cameroon and Chad have also been identified as areas of potential vulnerability. This is because the countries faced challenges related to unauthorized lending practices, including the use of non-standard debt recovery tactics such as public exposure threats and SIM lockouts.[12]

Over the course of 2025, an increase in the use of synthetic identities generated using AI to bypass KYC protocols was observed.[13] FortiGuard Labs' telemetry confirmed Cameroon as the second-highest botnet detection hub in Africa, with 40.5 million incidents in 2025, indicative of widespread device compromise used for credential harvesting and ransomware delivery.

Ransomware activity remained relatively low in absolute numbers, but this is likely a result of underreporting rather than absence. The region's minimal distributed denial-of-service (DDoS) activity and moderate vulnerability exposure suggest that threat actors prioritize stealth over disruption, focusing on long-term access and data exfiltration rather than immediate extortion. Gabon and the Republic of the Congo have the highest vulnerability detections in Central Africa, underscoring the region's growing exposure as digital services expand without commensurate security investment, based on statistics provided by FortiGuard Labs.

The absence of coordinated computer emergency response team (CERT) responses and limited inter-agency communication have allowed these threats to operate with minimal interference. The lack of public awareness campaigns in the predominantly French-speaking countries has further entrenched vulnerability among non-urban populations.

EAST AFRICA

East Africa emerged as a hub of mobile money fraud and infrastructure-targeted ransomware. Kenya recorded more than 46,786 DDoS attacks in the first half of 2025 targeting telecoms,[14] and was included in SOCRadar's top phishing detection in September 2025. The Communications Authority of Kenya reported hundreds of millions of intrusion attempts against government and information and communication technology (ICT) infrastructure[15] between July and September 2025, primarily via brute-force and system exploitation vectors.

Uganda's Electricity Transmission Company Limited (UETCL) experienced a suspected ransomware incident in August 2025, marking a case involving a national power grid.[16] The incident highlighted potential areas for improvement in critical infrastructure resilience and incident response coordination. In 2025, SIM swap fraud surged by 327 per cent in Kenya, with more than 123,000 fraudulent SIMs issued and an estimated USD 3.8 million drained from mobile wallets.[17] Tanzania and Rwanda reported similar patterns, with telecom providers struggling to implement real-time biometric verification.

Ethiopia ranked fifth across the entire continent in vulnerability detections by Shadowserver, while Seychelles faced a targeted breach of its central bank's customer data, indicating that even small, high-income nations are not immune. The region's rapid digital adoption has outpaced its ability to secure it. Kenya and Tanzania made strides in legal reform – Kenya's Computer Misuse and Cybercrimes (Amendment) Bill 2024[18] specifically targets SIM swaps and scam calls. The absence of a unified regional cybercrime response mechanism has allowed criminal networks to exploit jurisdictional boundaries between nations.

11 KnowBe4 Africa Human Risk Management Report 2025 (https://www.knowbe4.com/hubfs/African%20Human%20Risk%20Management%20Report.pdf) (January 2026).

12 Facebook Plcc- Plateforme de Lutte Contre la Cybercriminalité's Post 2025 (https://www.facebook.com/plcc.ditt/posts/quand-les-prêts-en-ligne-deviennent-un-piège-les-prêts-usuraires-sont-caractéris/1239563941546395/) (December 2025).

13 Sumsub Identity Fraud Report 2025-2026 (https://sumsub.com/files/Sumsub_Fraud_Report_2025_2026.pdf) (December 2025).

14 NETSCOUT DDoS Threat Intelligence Report 2025 (https://www.netscout.com/threatreport/country-analysis/) (January 2026).

15 Communications Authority of Kenya Cybersecurity Report 39th Edition 2025 (https://www.ca.go.ke/sites/default/files/2025-10/Cyber%20Security%20Report%20Q1%202025-2026.pdf) (February 2026).

16 Ransomware.live Uganda Electricity Transmission Company Limited 2025 (https://www.ransomware.live/id/VWdhbmRhIEVsZWN0cmljaXR5IFRyYW5zbWlzc2lvbiBDb21wYW55IExpbWl0ZWRAcWlsaW4=) (January 2026).

17 Capital FM Kenya Top StorySafaricom SIM swap fraud investigations up 327pc 2025 (https://www.capitalfm.co.ke/business/2025/10/safaricom-sim-swap-fraud-investigations-up-327pc/) (January 2026).

18 CM Advocates LLP Kenya's New Cybercrimes Law: Progress or Overreach? 2025 (https://cmadvocates.com/blog/kenyas-new-cybercrimes-law-progress-or-overreach-a-deep-dive-into-the-computer-misuse-and-cybercrimes-amendment-act-2024/) (February 2026).

WEST AFRICA

West Africa is observed as the most active region for BEC detections.[19] Ransomware detections in 2025 provided by TrendAI reached record levels in Cabo Verde, with 16,997 detections, the second highest in Africa, while Nigeria recorded 5,822, reflecting the country's dual role as an origin and target of cybercrime. Côte d'Ivoire is in ransomware detections of other countries and ranks third in sextortion IP senders, with 64,111 detections provided by TrendAI. Mali recorded the highest sextortion detections in West Africa, with 3,494 incidents, suggesting a growing infrastructure for automated blackmail campaigns. DDoS attacks, which had been prevalent in 2024, declined in the first half of 2025, although Mali registered 4,145 attacks,[20] indicating a strategic pivot toward more profitable, less detectable vectors like BEC and crypto scams.

Mobile money fraud and crypto-related scams, including Ponzi schemes and romance baiting, were widespread, often linked to scam centres operating under the guise of fintech startups. The region's high volume of French-language scams and the presence of cross-border money laundering networks underscore its position as a nexus between African and global criminal ecosystems. The Nigerian Bureau of Statistics (NBS) website was compromised in 2025, highlighting the vulnerability of key national institutions to cyber intrusion.[21] The attack disrupted economic data collection and fuelled disinformation campaigns, demonstrating the strategic value of targeting public data infrastructure.

SOUTHERN AFRICA

Southern Africa remains the continent's most digitally advanced and most heavily targeted region. South Africa accounted for 92 per cent of all ransomware detections in Africa by TrendAI, with incidents affecting critical infrastructure such as the South African Weather Service, South African Airways, and Namibia's Paratus Telecom.[22] The region's ultra-high connectivity, anchored by subsea cable landings and dense data centre networks, makes it a magnet for global threat actors seeking maximum disruption.

DDoS attacks peaked in the region, with South Africa alone recording 213,523 attacks, a single incident reaching 312 Gbps – dwarfing all other regions. Mauritius and Angola also surged in DDoS attacks,[23] reflecting the concentration of high-value digital infrastructure. Phishing was rampant, with South Africa accounting for almost 40 per cent of all African phishing detections, followed by Mauritius at 22 per cent, according to SOCRadar.[24] BEC activity originating from the region targeted global enterprises, particularly in the United States and Europe, based on TrendAI data. Angola recorded the highest FortiGuard Labs botnet detection volume in the region, while Namibia's national telecom breach exposed nearly 500,000 records[25] – a direct consequence of unpatched vulnerabilities.

Despite having the most mature regulatory frameworks, including South Africa's Cybersecurity Act and Mauritius' Digital Transformation Blueprint, the region's institutions remain vulnerable to the speed and scale of AI-enabled attacks. The presence of scam centres in Zambia[26] and the prevalence of sextortion with potential deepfake usage, based on TrendAI data, originating from South Africa underscore a troubling trend: advanced infrastructure coexists with systemic exploitation. The region's challenge is not a lack of policy, but gaps in implementation, particularly in cross-border coordination and real-time threat intelligence sharing between national CERTs and private sector partners.

19 Microsoft Digital Defense Report 2025 (https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf) (December 2025).

20 NETSCOUT DDoS Threat Intelligence Report 2025 (https://www.netscout.com/threatreport/country-analysis/) (January 2026).

21 Business Insider Hackers intensify attacks on Nigerian government websites, seize NBS platform 2024 (https://africa.businessinsider.com/local/lifestyle/hackers-intensify-attacks-on-nigerian-government-websites-seize-nbs-platform/0zdk4gl) (January 2026).

22 Radiowave Paratus Confirms Akira Ransomware Attack 2025 (https://radiowave.com.na/paratus-confirms-akira-ransomware-attack/) (January 2026).

23 NETSCOUT DDoS Threat Intelligence Report 2025 (https://www.netscout.com/threatreport/country-analysis/) (January 2026).

24 SOCRadar Africa Threat Landscape 2025 (https://socradar.io/wp-content/uploads/2025/09/Africa-Threat-Report.pdf) (December 2025).

25 BBC Sensitive data leaked after Namibia ransomware hack 2024 (https://www.bbc.com/news/articles/ce3l509e6x7o) (January 2026).

26 INTERPOL Major operation in Africa targeting online scams nets 651 arrests, recovers USD 4.3 million 2025 (https://www.interpol.int/en/News-and-Events/News/2026/Major-operation-in-Africa-targeting-online-scams-nets-651-arrests-recovers-USD-4.3-million) (March 2026).

KEY CYBERCRIMINAL THREATS – MAJOR ATTACK TYPES TARGETING AFRICA

RANSOMWARE: FROM OPPORTUNISTIC ATTACKS TO INFRASTRUCTURE SABOTAGE

Ransomware in 2025 evolved from a tool of financial extortion into a mechanism of systemic disruption, with threat actors increasingly targeting public services and critical infrastructure to maximize leverage. The most significant incidents were concentrated in Southern and West Africa, where digital infrastructure, while advanced, remained vulnerable due to outdated systems, underfunded cybersecurity units, and a pattern of underreporting.

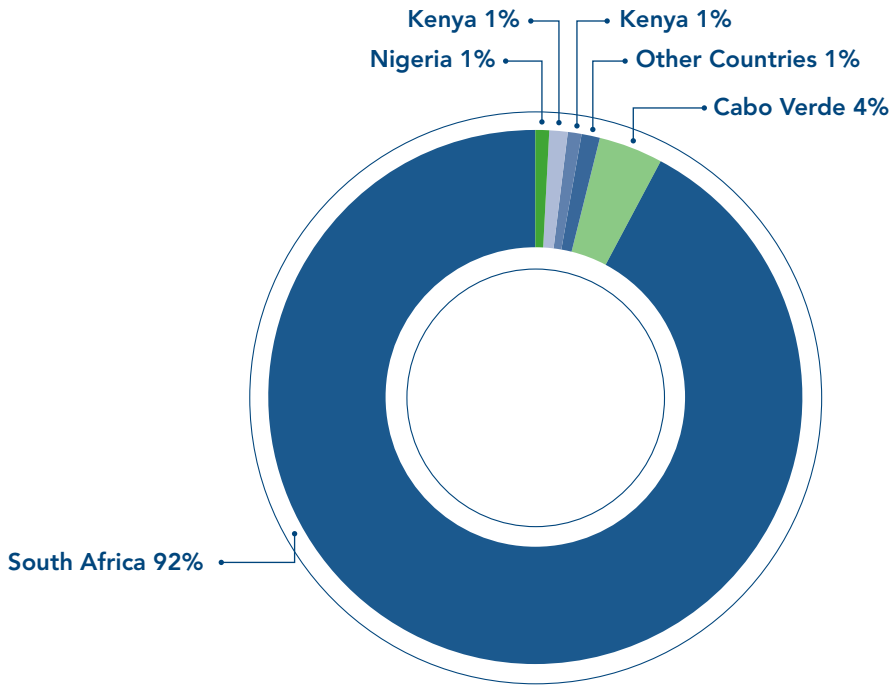


Figure 4: Ransomware detections by country in 2025 (Source: TrendAI).

South Africa accounted for 92 per cent of all ransomware detections in Africa, according to TrendAI data, with incidents affecting key public institutions such as the suspected attack against the South African Weather Service (SAWS) in January 2025.[27] The incident resulted in the corruption of critical meteorological data systems, leading to disruptions in aviation routing and maritime navigation services. Similarly, in August 2025, Nigeria's Customs Service was targeted by a ransomware variant[28] that paralyzed cargo clearance operations at the country's major ports, resulting in an estimated USD 18 million in storage fees and significant delays in import timelines.

In Uganda, the Electricity Transmission Company Limited (UETCL) experienced a suspected ransomware incident[29] in August 2025, compromising monitoring systems for the national power grid. While service was restored via backup protocols, the incident underscored the vulnerability of essential utilities to cyber disruption. In Namibia, two separate ransomware incidents were reported: a threat actor associated with the group Hunters International compromised the national telecommunications provider's customer database in December 2024,[30] while another actor, reportedly linked to the Akira group, targeted Paratus Telecom, disrupting core network functions.[31]

27 ITWeb Cyber attack derails SA Weather Service's performance 2025 (https://www.itweb.co.za/article/cyber-attack-derails-sa-weather-services-performance/o1Jr5MxPAXlMKdWL) (February 2026).

28 Vanguard News Cyber attack hits Customs, disrupts cargo clearance 2025 (https://www.vanguardngr.com/2025/08/cyber-attack-hits-customs-disrupts-cargo-clearance/) (January 2026).

29 Ransomware.live Uganda Electricity Transmission Company Limited 2025 (https://www.ransomware.live/id/VWdhbmRhIEVsZWN0cmljaXR5IFRyYW5zbWlzc2lvbiBDb21wYW55IExpbWl0ZWRAcWlsaW4=) (January 2026).

30 BBC Sensitive data leaked after Namibia ransomware hack 2024 (https://www.bbc.com/news/articles/ce3l509e6x7o) (January 2026).

31 Radiowave Paratus Confirms Akira Ransomware Attack 2025 (https://radiowave.com.na/paratus-confirms-akira-ransomware-attack/) (January 2026).

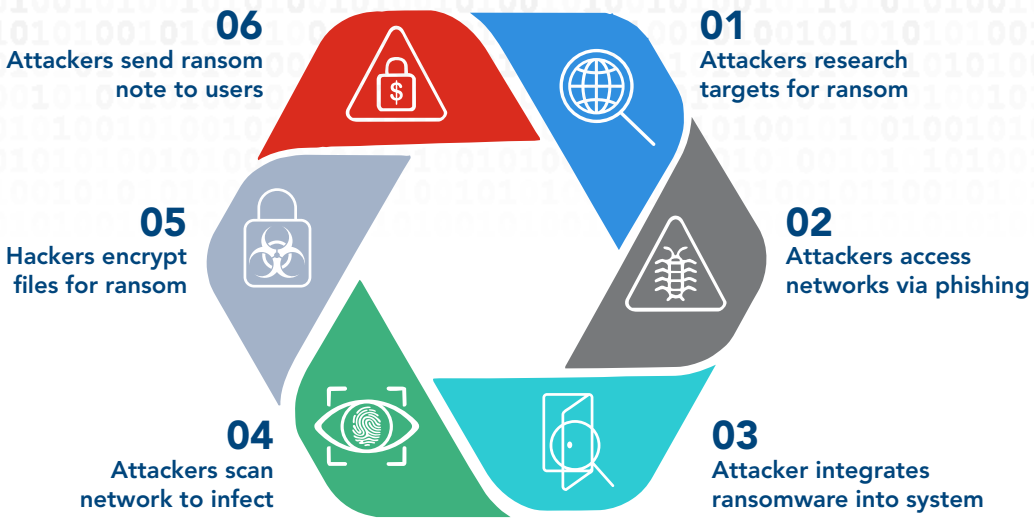


Figure 5: Six stages of the ransomware attack chain (Source: Fortinet).

FortiGuard Labs telemetry revealed that threat actors are deploying automated reconnaissance tools capable of scanning tens of thousands of systems per second, leveraging machine learning to identify exploitable vulnerabilities in routers, outdated software, and misconfigured cloud services. The use of botnets as delivery mechanisms has also intensified, with the Sliver C2 framework, an open-source, widely available tool, being weaponized to deploy novel ransomware strains.

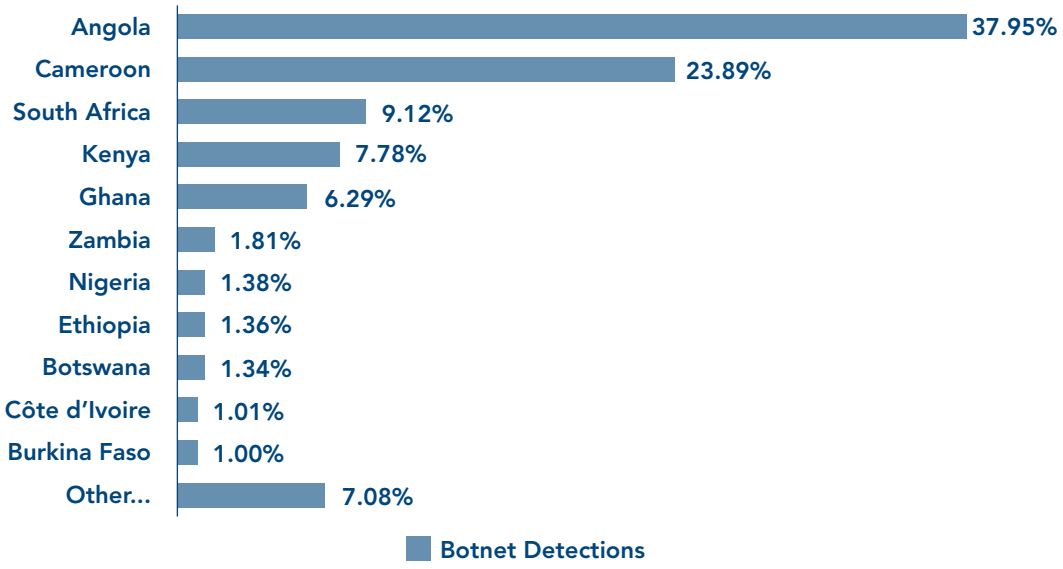


Figure 6: 2025 Botnet detections in Africa by country (Source: FortiGuard Labs).

Cameroon recorded 40.5 million botnet detections in 2025, the second highest in Africa. Angola also demonstrated high levels of botnet activity, suggesting a growing network of compromised devices used to launch coordinated attacks.

Botnets are infected machines controlled by cybercriminals due to malware and can be a prime delivery mechanism of ransomware. Based on FortiGuard Labs' botnet detection in 2025, the Sliver botnet – an open-source command-and-control (C2) framework often abused by threat actors to facilitate ransomware attacks such as the novel 01flip ransomware[32] – remains widespread in Africa (see Figure 7).

32 Unit 42 01flip: Multi-Platform Ransomware Written in Rust 2025 (https://unit42.paloaltonetworks.com/new-ransomware-01flip-written-in-rust/) (February 2026).

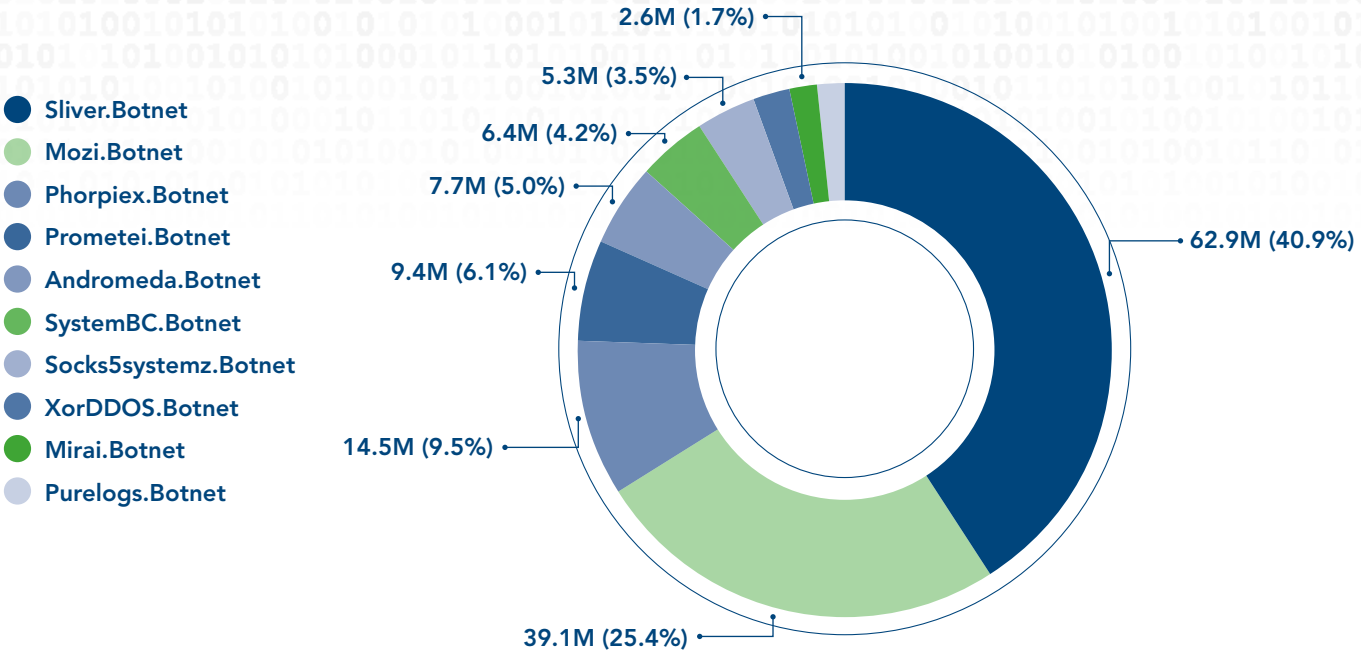


Figure 7: Botnet detections in Africa in 2025 by malware family (Source: FortiGuard Labs).

Despite the scale of these incidents, according to 89 per cent of the respondents of the INTERPOL member country survey, underreporting remains a pervasive challenge – with countries citing no formal incident reporting mechanisms, fear of reputational damage, lack of forensic capability, and uncertainty over legal obligations as some of the major challenges. Only Nigeria, Kenya, South Africa, and Mauritius mandate disclosure within 72 hours; Ghana requires reporting within 24 hours of detection, reflecting a fragmented regulatory landscape.[33]

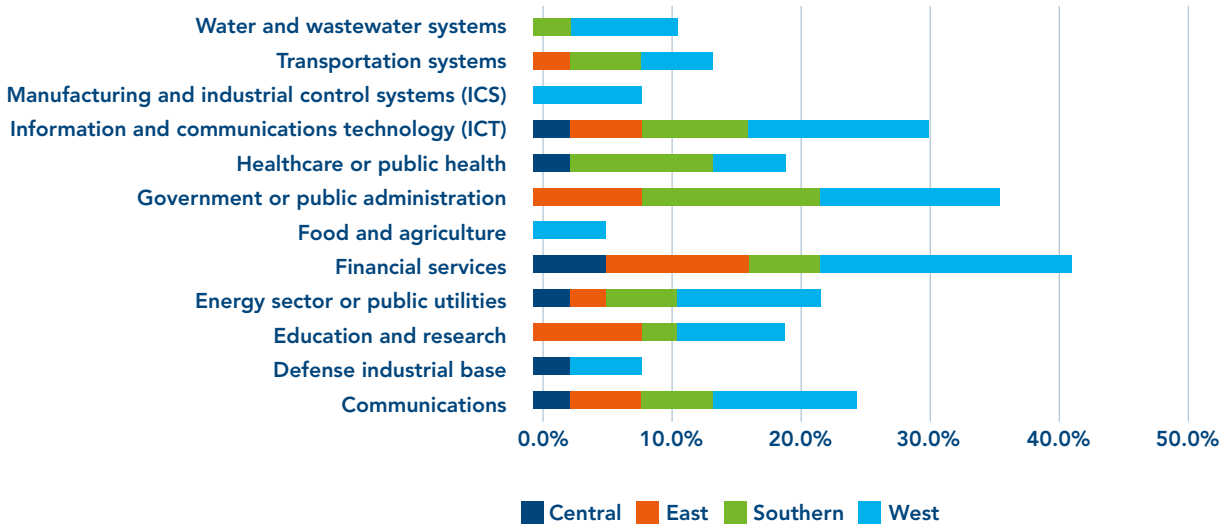


Figure 8: Critical infrastructure sectors affected by ransomware in 2025 (Source: INTERPOL member country survey).

33 Mondaq Africa Guide Data Protection 2025 (https://www.mondaq.com/pdf/1661282.pdf) (January 2026).

Most agencies lack the tools, personnel, or international coordination to conduct timely decryption or attribution. While **INTERPOL's Operation Sentinel** successfully decrypted 30 terabytes of ransomware-encrypted data in Ghana, such successes remain exceptional.[34] The strategic implication is clear: ransomware is no longer a criminal nuisance, it is a weapon of economic coercion used to destabilize public services and extract maximum value from systemic vulnerabilities. Without mandatory reporting, sector-wide cyber audits, and robust backup protocols, Africa's critical infrastructure will remain perpetually exposed.

BUSINESS E-MAIL COMPROMISE: THE FINANCIAL ENGINE OF TRANSNATIONAL CYBERCRIME

BEC, unlike ransomware which targets systems, exploits trust, manipulating human behaviour to bypass technical controls. The sophistication of these campaigns has increased dramatically, with AI now used to generate highly convincing e-mail correspondence that mimics executive tone, internal jargon, and signature styles with near-perfect fidelity.

In 2025, TrendAI data indicated that 70 per cent of BEC detections originated in South Africa and 29 per cent from Nigeria. Microsoft-identified threat actors based in South Africa, active since 2017, primarily target US-based enterprises and use compromised e-mail accounts and money mule networks to divert funds to offshore accounts. In addition, threat actors based in Nigeria, active since 2021, have become central to international money laundering operations, routing illicit proceeds through crypto exchanges, shell companies, and mobile payment platforms.[35]

A key case identified during INTERPOL's Operation Sentinel involved a Senegalese-based BEC attempt targeting a petroleum company, seeking to divert USD 7.9 million. Authorities successfully froze the destination account, but the operation revealed the transnational nature of these schemes, with threat actors based in Africa orchestrating fraud against targets in Europe and North America using infrastructure located in multiple jurisdictions.

The attack vector remains consistent: initial reconnaissance to identify payroll or procurement personnel, followed by account compromise via phishing or credential stuffing. AI-generated e-mails are then sent to finance departments, impersonating senior executives, often with urgent requests to "correct" payment details. The use of free e-mail services (Gmail, Outlook) to bypass domain spoofing detection has rendered traditional e-mail security measures increasingly ineffective.

The financial impact is compounded by the lack of coordinated financial intelligence sharing. While banks and fintech's have improved fraud detection, cross-border collaboration between financial institutions, telecoms, and law enforcement remains slow and bureaucratic. Money mule networks, often recruited through job fraud scams, operate with impunity in countries with limited anti-money laundering (AML) enforcement. The strategic vulnerability lies in the intersection of digital trust and human behaviour. As AI continues to refine the realism of impersonation, the human element remains the weakest link – and the most difficult to defend.

34 INTERPOL 574 arrests and USD 3 million recovered in coordinated cybercrime operation across Africa 2025 (https://www.interpol.int/en/News-and-Events/News/2025/574-arrests-and-USD-3-million-recovered-in-coordinated-cybercrime-operation-across-Africa) (January 2026).

35 Microsoft Digital Defense Report 2025 (https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf) (December 2025).

ONLINE SCAMS: THE GROWING THREAT OF SCAM CENTRES

Online scams in 2025 transitioned from isolated phishing incidents to highly organized, industrialized criminal enterprises – often operating from centralized scam centres linked to human trafficking and transnational organized crime.[36] These operations leverage mobile money platforms, social media, and AI to target vulnerable populations across Africa and beyond, generating billions in illicit revenue.

Mobile money fraud emerged as the most prevalent scam, reported by 97 per cent of countries who responded to the INTERPOL member country survey. Kenya alone detected 123,000 fraudulent SIM cards in 2025,[37] enabling attackers to conduct SIM swap attacks and drain mobile wallets. Ghanian citizens lost USD 1.3 million in the first quarter of the year,[38] while Tanzania reported a 19 per cent reduction in attempts following stricter SIM registration enforcement.[39] The root cause remains inconsistent KYC protocols, particularly in countries where telecom providers lack the technical capacity to verify identity in real time.

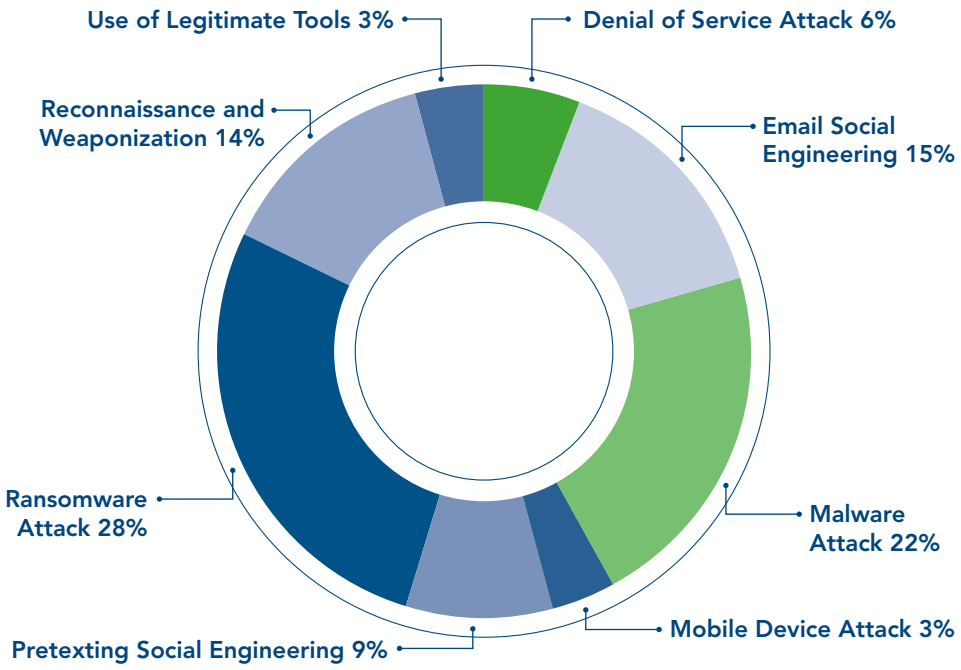


Figure 9: Africa cyberthreat events by attack vector in 2025 (Source: Mastercard).

36 SOCRadar Africa Threat Landscape 2025 (https://socradar.io/wp-content/uploads/2025/09/Africa-Threat-Report.pdf) (December 2025).

37 Capital FM Kenya Top StorySafaricom SIM swap fraud investigations up 327pc 2025 (https://www.capitalfm.co.ke/business/2025/10/safaricom-sim-swap-fraud-investigations-up-327pc/) (January 2026).

38 The Fourth Estate Mobile money robberies: Inside Ghana's rising cybercrime wave 2025 (https://thefourthestategh.com/2025/10/mobile-money-robberies-inside-ghanas-rising-cybercrime-wave/) (March 2026).

39 The Guardian News Mobile fraud attempts drop as awareness and reporting improve 2025 (https://www.ippmedia.com/the-guardian/news/local-news/read/mobile-fraud-attempts-drop-as-awareness-and-reporting-improve-2025-07-27-104409) (February 2026).

Loan and microcredit scams proliferated in West and Central Africa, particularly among French-speaking populations. Unlicensed fintech apps, some even listed on the Google Play Store, were used to harvest personal data under the guise of offering small loans.[40] Victims were then harassed with automated voice calls and threats of public exposure if repayments were not made. In Côte d'Ivoire, authorities shut down platforms such as "Wave Prêt" and "Crédit Max" after investigations revealed abusive interest rates and extortion tactics.[41]

The crypto economy in the region was valued at USD 205 billion in transactions between July 2024 and July 2025 and became a magnet for fraud. Nigeria accounted for USD 92 billion of this total, while South Africa's regulatory clarity attracted both legitimate investors and criminal actors.[42] Scams such as the CryptoBridge Exchange (CBEX) falsely claimed US licensing to defraud African investors,[43] while "Optcoin" and "AfriQuantumX" used deepfake videos of national leaders and social media influencers to promote fake AI trading platforms.[44] INTERPOL's Operation Serengeti 2.0 dismantled a Zambia-based network responsible for USD 300 million in losses and 60,000 victims, leading to 15 arrests.[45]

Romance baiting, a hybrid of emotional manipulation and investment fraud, became increasingly industrialized.[46] Victims, often recruited via Facebook, were moved to WhatsApp for video calls, where they were coerced into sending money under false pretences. Many of these operations were linked to scam centres, facilities where victims are held against their will and forced to participate in fraud.

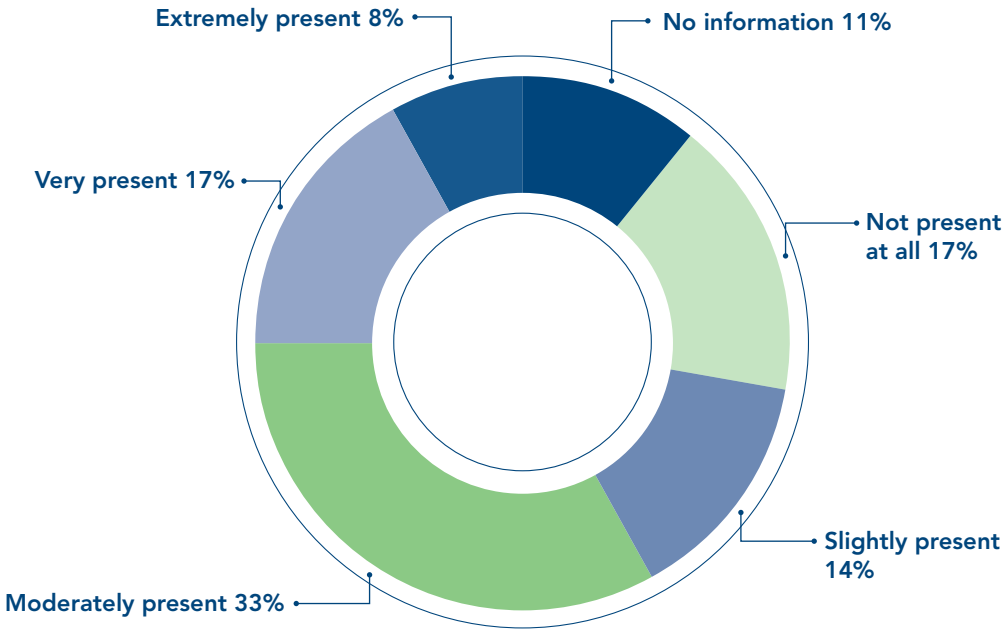


Figure 10: The perceived presence of scam centre operations in Africa member countries in 2025 (Source: INTERPOL member country survey).

40 News du Camer Illegal fintechs: express loans, abusive rates. The hidden excesses of microcredit applications 2025 (https://www.newsducamer.com/fintechs-illegales-prets-express-taux-abusifs-les-derives-cachees-des-applications-de-microcredit/) (January 2025).

41 Facebook Plcc- Plateforme de Lutte Contre la Cybercriminalité's Post 2025 (https://www.facebook.com/plcc.ditt/posts/quand-les-prêts-en-ligne-deviennent-un-piège-les-prêts-usuraires-sont-caractéris/1239563941546395/) (December 2025).

42 Chainalysis Sub-Saharan Africa Emerges as Third-Fastest Growing Crypto Region with Strong Retail Activity 2025 (https://www.chainalysis.com/blog/subsaharan-africa-crypto-adoption-2025/) (March 2026).

43 The Jakarta Post CBEX crypto scam: AI-hyped Ponzi scheme defrauds African investors 2025 (https://www.thejakartapost.com/business/2025/07/01/cbex-crypto-scam-ai-hyped-ponzi-scheme-defrauds-african-investors.html) (January 2026).

44 Money254 Scams That Saw Kenyans Lose Money in 2025 And How They Worked 2025 (https://www.money254.co.ke/post/scams-that-saw-kenyans-lose-money-in-2025-and-how-they-worked-info) (January 2026).

45 INTERPOL African authorities dismantle massive cybercrime and fraud networks, recover millions 2025 (https://www.interpol.int/en/News-and-Events/News/2025/African-authorities-dismantle-massive-cybercrime-and-fraud-networks-recover-millions) (March 2026).

46 Elliptic The state of crypto scams 2025 (https://info.elliptic.co/hubfs/The%20state%20of%20crypto%20scams%202025/The%20State%20of%20Crypto%20Scams%202025%20-%20Elliptic.pdf) (February 2026).

The scale of these operations is alarming. INTERPOL's member country survey found that 72 per cent of African countries reported the presence of scam centres, with the highest concentration in Southern and West Africa. These are not random actors; they are organized criminal enterprises with supply chains for recruitment, technology, laundering, and evasion.[47]

The response has been fragmented. While some governments have cracked down on unlicensed fintechs, the lack of cross-border coordination and digital evidence-sharing has allowed these networks to persist. The integration of AI into scam operations, generating personalized lures, voice clones, and fake testimonials, has made detection increasingly difficult for both platforms and victims.

DIGITAL SEXTORTION: AI-POWERED ATTACK METHODS FUEL WEAPONIZED CONTENT

Digital sextortion, a form of online image-based sexual abuse (OIBSA), surged in 2025 based on the INTERPOL member country survey, likely because of AI's ability to generate highly realistic synthetic media. Unlike traditional scams, sextortion does not primarily seek financial gain; it seeks psychological control, leveraging shame, fear, and coercion to extract ongoing payments. TrendAI recorded 600,000 sextortion detections in Africa in 2025, with the majority originating from South Africa (30 per cent), Kenya (13 per cent), Côte d'Ivoire (11 per cent), Ethiopia (8 per cent), and Angola (4 per cent). These campaigns were predominantly delivered via the Phorpiex botnet,[48] which sent mass e-mails demanding cryptocurrency payments under the threat of releasing intimate content.

A significant shift occurred in the targeting of minors. Meta removed 635,000 accounts on Instagram and Facebook in 2025 for exploiting children,[49] a tenfold increase from 2023. In Côte d'Ivoire, four suspects were arrested in connection with a 2022 case involving the sextortion of a US teenager,[50] marking one of the first transnational prosecutions of its kind in Africa. Adult victims were increasingly targeted through social media romance scams. Attackers would establish fake relationships on Facebook, then move victims to WhatsApp for video calls, capturing explicit content to later demand payments via mainstream mobile money wallets such as M-Pesa or MTN Mobile Money (MoMo). In Ghana, financial losses among teen victims (18–24) increased fivefold in 2025, largely due to the use of deepfake technology to fabricate compromising images of victims based on their social media photos.[51]

TRM Labs confirmed that AI-driven tools now allow criminals to generate photorealistic explicit imagery[52] from a single photograph, a development that has rendered traditional verification methods obsolete. The psychological toll is immense, with victims suffering from depression, anxiety, and social isolation, yet underreporting remains high due to stigma and lack of support services. While the African Union,[53] the African Telecommunications Union, and initiatives such as Child Online Africa (COA) and Africa Week for Action for Child Online Protection (AWA4COP)[54] have raised awareness, there remains a critical gap in law enforcement capacity to investigate and prosecute these cases, particularly when perpetrators operate across borders using anonymized infrastructure. Most agencies lack specialized units trained in digital sexual abuse, forensic analysis of deepfakes, or victim support protocols. The absence of harmonized legal definitions for non-consensual intimate imagery further complicates prosecution.

The strategic trajectory is alarming: sextortion is no longer a crime of opportunity; it is becoming a scalable, automated, and psychologically devastating business model, enabled by accessible AI tools and the global reach of social media platforms. Without dedicated investigative units, cross-border legal cooperation, and robust victim protection frameworks, this threat will continue to grow in both scale and severity.

47 Al Jazeera 'I invested in a Ponzi scheme': Nigerians fall victim to crypto scams 2025 (https://www.aljazeera.com/features/2025/6/11/i-invested-in-a-ponzi-scheme-nigerians-fall-victim-to-crypto-scams) (February 2026).

48 Sophos Phorpiex Continues to Deliver Sextortion Spam 2024 (https://www.sophos.com/en-us/blog/phorpiex-continues-to-deliver-sextortion-spam) (December 2026).

49 Facebook Expanding Teen Account Protections and Child Safety Features 2025 (https://about.fb.com/news/2025/07/expanding-teen-account-protections-child-safety-features/) (December 2025).

50 LA Times 'Sextortion' scam linked to California teen's suicide leads to 4 arrests in West Africa 2025 (https://www.latimes.com/california/story/2025-05-12/sextortion-scam-teen-suicide) (December 2025).

51 Graphic Online Sextortion: Rising threats, hidden victims, urgent action 2025 (https://www.graphic.com.gh/features/opinion/ghana-news-sextortion-rising-threats-hidden-victims-urgent-action.html) (January 2026).

52 Conflict International Deepfake Sextortion: The Next Phase of Digital Blackmail 2025 (https://conflictinternational.com/news/deepfake-sextortion-the-next-phase-of-digital-blackmail) (February 2026).

53 Dark Reading Afripol Focuses on Regional Cyber Challenges, Deepening Cooperation 2025 (https://www.darkreading.com/cybersecurity-operations/afripol-focuses-regional-cyber-challenges-deepening-cooperation) (December 2025).

54 Child Online Africa Launches Africa Week for Action for Child Online Protection (AWA4COP) to Support Global Push Against Online Child Sexual Exploitation 2025 (https://childonlineafrica.org/press-releases/child-online-africa-launches-africa-week-for-action-for-child-online-protection-awa4cop-to-support-global-push-against-online-child-sexual-exploitation/57) (December 2025).

DATA BREACH: THE FOUNDATION THAT DRIVES CYBERCRIME AT SCALE

Data breaches in 2025 were not isolated events; they were the foundational layer upon which nearly every other major cybercrime vector was built. While ranked third in reported incidence in the INTERPOL member country survey, the cascading impact of compromised data was felt across ransomware, BEC, identity theft, and mobile fraud ecosystems.

The Shadowserver Foundation identified more than 6,000 exploitable vulnerabilities across Africa in 2025, with the highest concentrations in South Africa, Kenya, and Nigeria, the same countries with the largest Internet user bases.[55] The most targeted systems included outdated and unpatched routers, vulnerable Virtual Private Networks (VPNs), and misconfigured web-based document management platforms. These vulnerabilities were not exotic or novel; they were well-documented, publicly known, and easily exploitable. Their persistence reflects ongoing challenges in cyber hygiene, resource allocation, and patch management across both the public and private sectors. These vulnerabilities are leveraged by threat actors to gain initial entry into vulnerable networks and systems, which result in many of the data breaches observed.

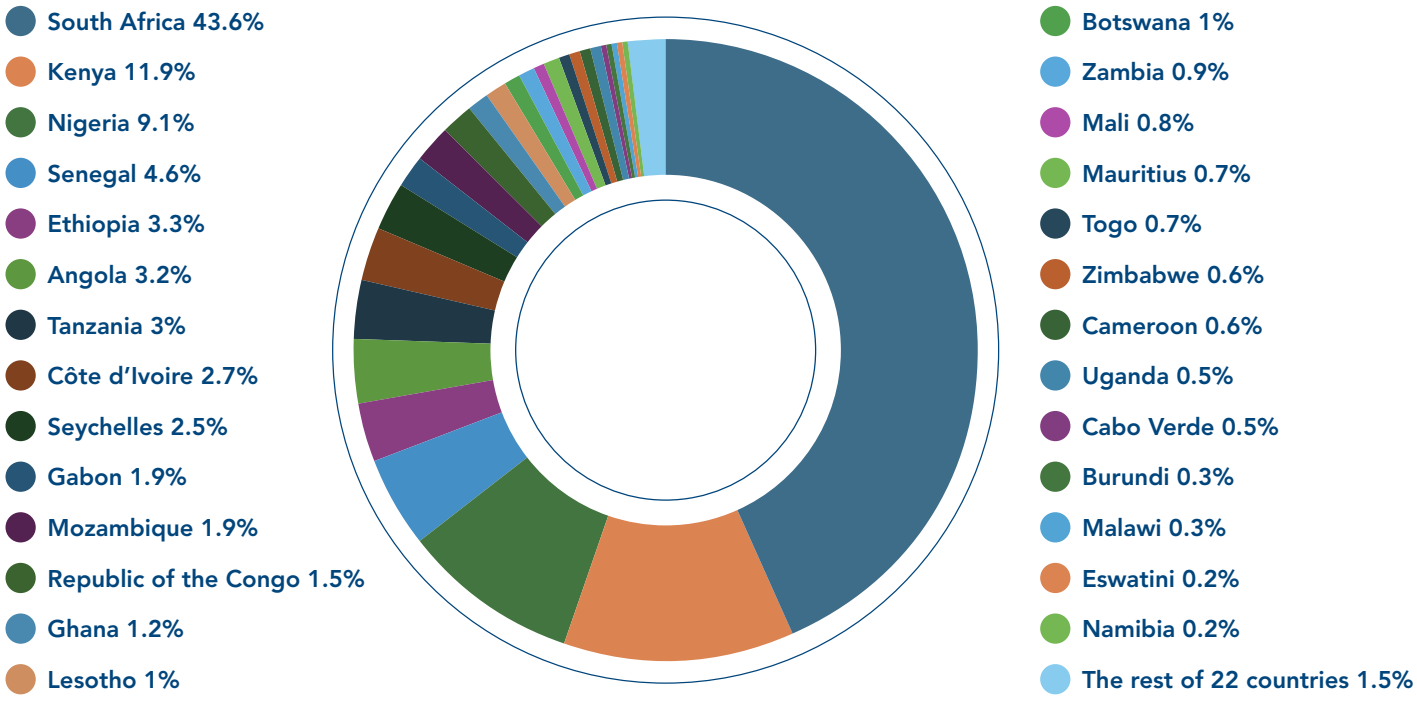


Figure 11: Detection of vulnerabilities by country in Africa in 2025 (Source: Shadowserver Foundation).

55 Statista Number of Internet users in Africa as of October 2025, by country (https://www.statista.com/statistics/505883/number-of-internet-users-in-african-countries/) (January 2026).

One of the most significant incidents occurred in December 2024, when Namibia's national telecommunications[56] provider suffered a breach exposing 500,000 personal and financial records. The breach was not attributed to a sophisticated attack, but rather to an unsecured administrative portal left accessible to the public Internet. The consequences were immediate: stolen identities could potentially sold on the dark web, used to open fraudulent mobile money accounts, and deployed in BEC campaigns targeting government procurement departments.

In Seychelles, a central bank customer database was reportedly held for ransom, with attackers demanding payment in cryptocurrency to prevent public disclosure.[57] In Tanzania, government-linked social media accounts were compromised during the pre-election period, leading to coordinated disinformation campaigns and attempts to disrupt digital civic engagement.[58] Somalia's e-visa platform also experienced a confirmed breach, underscoring the vulnerability of even nascent digital services.[59]

The dark web became a primary marketplace for stolen African-origin data. S2W data provided to INTERPOL showed a 62 per cent year-over-year increase in African-origin content on dark web forums – primarily consisting of identity documents, SIM card PINs, banking credentials, and mobile money account details. Much of this data was sourced from previous breaches, phishing campaigns, and compromised mobile apps.

The strategic implication is clear: data breaches are not a technical failure – they are a corporate governance failure. Until data protection is treated as a national security imperative, with enforceable standards, independent oversight, and mandatory reporting, every digital service in Africa will remain a potential entry point for criminal exploitation.

FINANCIAL FRAUD: LEAKED DATA FUELLING IDENTITY THEFT CRISIS

Identity theft in 2025 evolved from the theft of existing credentials to the creation of entirely synthetic identities, digital personas fabricated using AI to bypass even advanced biometric verification systems. This shift marked a fundamental erosion of trust in digital authentication mechanisms across the continent. While Nigeria's National Identification Number-SIM (NIN-SIM) policy significantly reduced fraud in 2024 by linking mobile registrations to national ID databases,[60] cybercriminals adapted rapidly. In 2025, fraud hotspots shifted to Cameroon, Mali, and Tanzania, where attackers exploited gaps in KYC enforcement, particularly in rural areas and informal financial systems.[61] AI-generated synthetic identities, created by combining real personal data with fabricated elements, were used to open bank accounts, secure mobile loans, and register SIM cards under false names.

The rise of "money muling" as a widespread phenomenon further complicated the landscape. A 2025 survey found that almost 77 per cent of fraud-exposed individuals in Africa[62] were aware of money muling, the practice of receiving and transferring illicit funds through personal bank accounts, yet only 12 per cent understood its legal consequences or recognized it as a form of criminal complicity. Many were recruited through fake job postings, often posing as "financial agents" or "remote transaction officers," and were unaware they were laundering proceeds from BEC, ransomware, or crypto scams. The ease with which attackers could hijack a SIM card, often through social engineering of telecom customer service representatives, allowed them to gain instant access to victims' financial ecosystems. In Kenya, the 327 per cent increase in SIM swap fraud demonstrated the fragility of telecom-based authentication.[63]

56 Radiowave Paratus Confirms Akira Ransomware Attack 2025 (https://radiowave.com.na/paratus-confirms-akira-ransomware-attack/) (January 2026).

57 SC Media Cyber intrusion contained by Seychelles Commercial Bank 2025 (https://www.scworld.com/brief/cyber-intrusion-contained-by-seychelles-commercial-bank) (February 2026).

58 Africanews Tanzania blocks access to X following cyberattacks on government accounts 2025 (https://www.africanews.com/2025/05/22/tanzania-blocks-access-to-x-following-cyberattacks-on-government-accounts/) (February 2026).

59 BBC US and UK warn of major e-visa data breach in Somalia 2025 (https://www.bbc.com/news/articles/c620e43z2q5o) (January 2026).

60 Punch Newspapers NIN–SIM policy erased 59.7m phone lines — NCC 2025 (https://punchng.com/nin-sim-policy-erased-59-7m-phone-lines-ncc) (February 2026).

61 Sumsub Identity Fraud Report 2025-2026 (https://sumsub.com/files/Sumsub_Fraud_Report_2025_2026.pdf) (December 2025).

62 Sumsub Identity Fraud Report 2025-2026 (https://sumsub.com/files/Sumsub_Fraud_Report_2025_2026.pdf) (December 2025).

63 Capital FM Kenya Top StorySafaricom SIM swap fraud investigations up 327pc 2025 (https://www.capitalfm.co.ke/business/2025/10/safaricom-sim-swap-fraud-investigations-up-327pc/) (January 2026).

The absence of real-time, inter-agency data sharing between banks, telecoms, and law enforcement created a dangerous blind spot. While financial institutions could detect suspicious transactions, they lacked the legal authority or technical channels to block SIM swaps or freeze accounts without court orders, a process that often took weeks to months. The strategic vulnerability lies in the fragmentation of identity verification. No single, interoperable, and secure digital identity system exists across Africa. Each country operates its own framework, often with incompatible standards. This fragmentation allows criminals to exploit jurisdictional gaps, stealing an identity in one country, using it to open an account in another, and laundering funds through a third.

Without a continental digital identity framework, built on interoperable standards, biometric verification, and real-time fraud detection, Africa's financial inclusion gains are at risk of being reversed by the very technologies designed to empower them.

ARTIFICIAL INTELLIGENCE (AI) – SCALING AND SIMPLIFYING CRIMINAL CAMPAIGNS

The year 2025 marked the definitive transition from AI as a supporting tool to AI as the core operational driver of cybercrime in Africa. Generative AI tools, once the domain of researchers and developers, are now freely available, commodified, and weaponized by criminal actors with minimal technical expertise. According to INTERPOL's member country survey, 55 per cent of cybercrime cases in 2025 involved AI in some capacity, 47 per cent occasionally, 8 per cent frequently. This represents a dramatic increase from previous years and reflects a fundamental shift in criminal methodology. AI is now used to automate every stage of the attack lifecycle: from reconnaissance and phishing to extortion and evasion.

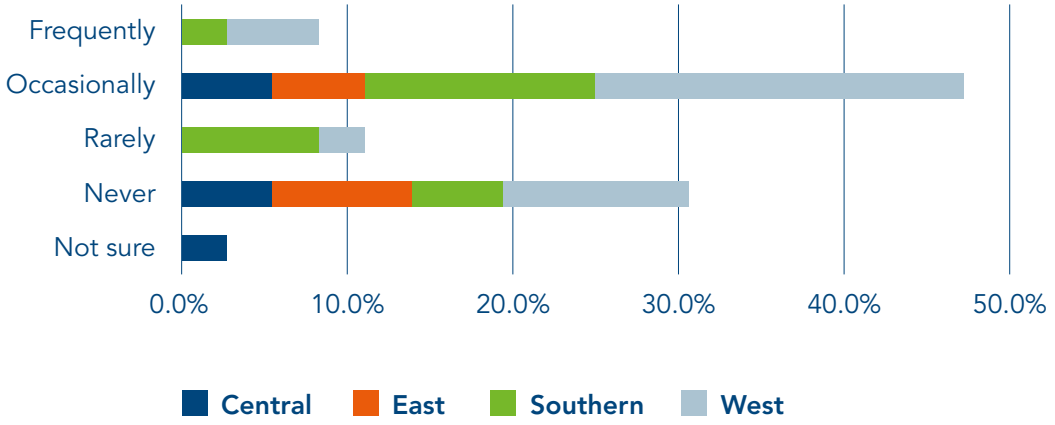


Figure 12: Cybercrime cases observed utilizing AI technology (Source: INTERPOL member country survey).

Deepfakes became the most visible manifestation of this trend. Between Q2 and Q4 2024, deepfake incidents increased sevenfold throughout Africa,[64] with AI-generated audio and video used to impersonate government officials, corporate executives, and even family members. In Uganda, a deepfake video of a prominent public figure was circulated to promote a fraudulent investment scheme, resulting in more than USD 2 million in losses before authorities intervened.[65]

AI was also used to generate synthetic identities that bypassed KYC checks, craft hyper-personalized phishing lures tailored to individual victims, and produce AI-driven malware capable of evading signature-based detection. One emerging strain, named PromptLock ransomware, uses generative AI to autonomously write, adapt, and execute its own malicious code, a level of customization previously only possible through human labour. [66]

64 Smile ID Digital Identity Fraud in Africa Report 2025 (https://cms.media.usesmileid.com/Smile-ID-2025-Fraud-Report.pdf) (January 2026).

65 CEO East Africa Ugandan billionaire, Dr. Sudhir Ruparelia Warns Public of Deepfake AI Scam Misusing His Image to Promote a Fraudulent Financial Platform 2025 (https://www.ceo.co.ug/ugandan-billionaire-dr-sudhir-ruparelia-warns-public-of-deepfake-ai-scam-misusing-his-image-to-promote-a-fraudulent-financial-platform/) (January 2026).

66 ESET First known AI-powered ransomware uncovered by ESET Research 2025 (https://www.welivesecurity.com/en/ransomware/first-known-ai-powered-ransomware-uncovered-eset-research) (December 2025).

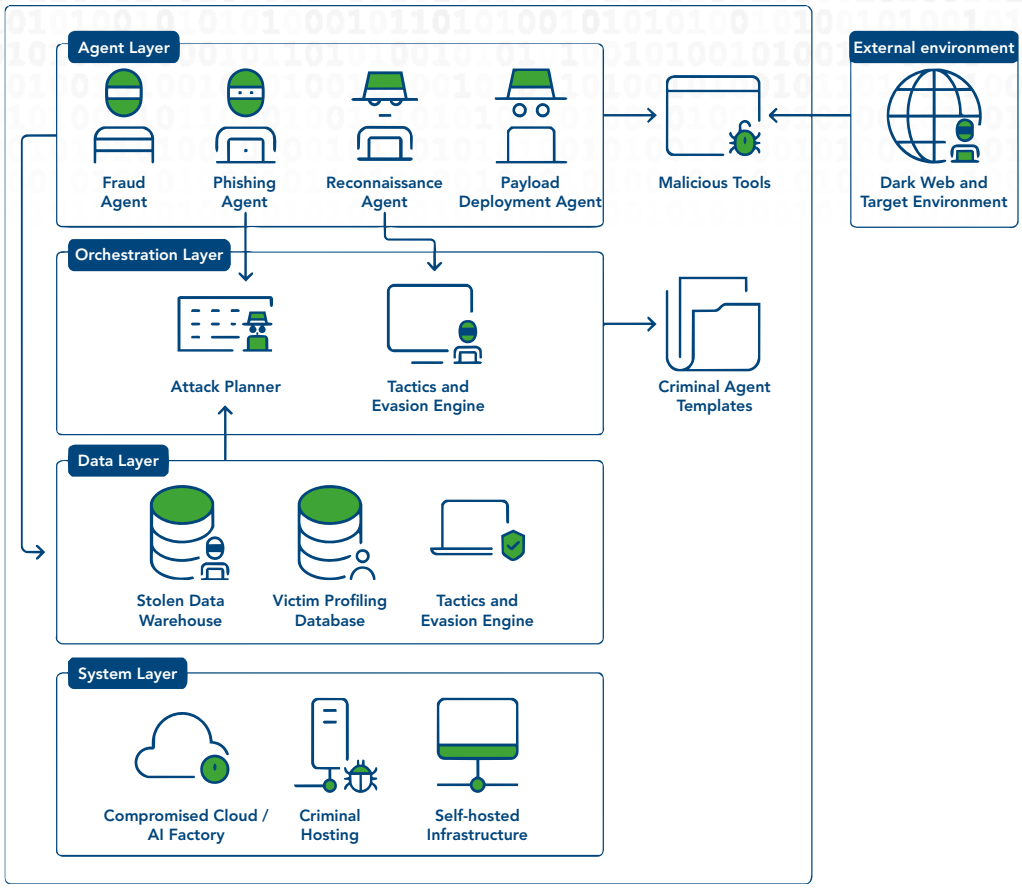


Figure 13: The layers of criminal agentic AI usage (Source: TrendAI).

The response from law enforcement has been uneven. While 33 per cent of agencies reported using AI for threat detection and 31 per cent for digital forensics and OSINT analytics, the majority still rely on manual processes. Only 8 per cent of intelligence analysts possess advanced AI expertise, and 92 per cent of agencies cite a lack of technical expertise as the primary barrier to adopting AI tools, according to the INTERPOL member country survey.

The most critical gap is not technological, but rather a gap in training and skills. Most frontline officers and investigators have not been trained to recognize or respond to AI-generated content. The ability to distinguish between authentic and synthetic media, whether it is a voice call, a video, or an e-mail, is now a fundamental skill in cyber investigations. Yet, training programmes remain sparse, underfunded, and inconsistent across the continent.

The implications are profound. Criminals are now operating at machine speed, with AI enabling attacks that are faster, more scalable, and more difficult to attribute. Law enforcement, by contrast, remains constrained by legal processes, bureaucratic delays, and a lack of technical capacity. While the gap is widening in cybersecurity, by prioritizing focused investment in AI literacy, specialized forensic tools, and cross-border coordination, Africa can bridge the divide and keep pace with the rapidly evolving tactics of cybercriminals.

CHALLENGES IN COMBATING CYBERCRIME IN AFRICA

DIVERGING LEGAL AND POLICY FRAMEWORKS

Cybercrime legislation across Africa remains fragmented, with 83 per cent of countries who responded to INTERPOL's member country survey possessing dedicated cybercrime laws, while 17 per cent indicated that they rely on outdated general provisions or are in the process of drafting legislation. Although regional instruments such as the African Union's Malabo Convention and the United Nations' new Convention against Cybercrime, signed in Hanoi in October 2025, offer a path toward harmonization, implementation lags significantly.

Only 13 African nations have ratified the Budapest Convention on Cybercrime, and even among those, the operationalization of Article 35 (24/7 international assistance) and Article 26 (spontaneous information sharing) remains inconsistent. Regarding the UN Convention against Cybercrime (Hanoi Convention), there is a total of 21 African nations who signed the treaty at the time of drafting this report. Definitions of cybercrime vary widely: some jurisdictions exclude cryptojacking, cyberstalking, deepfake creation, and online human trafficking from legal definitions, creating safe havens for transnational actors.

The absence of standardized legal terminology impedes mutual legal assistance, delays evidence sharing, and allows criminals to exploit jurisdictional arbitrage. While 61 per cent of surveyed countries rated their legal frameworks as satisfactory to excellent, 31 per cent explicitly called for urgent reform, particularly in areas of digital evidence preservation, cross-border data access, and the criminalization of AI-facilitated fraud.

CAPACITY AND CAPABILITY CONCERNS

Law enforcement agencies across Africa operate under severe constraints. According to the INTERPOL member country survey, 94 per cent of agencies reported insufficient digital forensics tools, while 78 per cent cited inadequate budgets, response vehicles, international mobile subscriber identity (IMSI) catchers to track location data of mobile phone users, and specialized personnel. Only 17 per cent of countries maintain cybercrime units with more than 100 personnel; many operate with fewer than 10. Technical expertise is unevenly distributed. While digital forensics and incident response (DFIR) skills are relatively uncommon, expertise in network security, penetration testing, crypto-asset tracing, and malware analysis remains even more in-demand.

AI readiness is alarmingly low. Only 22 per cent of digital forensic units possess working knowledge of AI-driven threats, and just 8 per cent of intelligence analysts have advanced expertise. Frontline officers and leadership generally possess only basic awareness, leaving them ill-equipped to identify AI-generated deepfakes, synthetic identities, or automated phishing campaigns. Operational constraints compound these challenges: 72 per cent of respondents reported slow data exchange between agencies, while 89 per cent identified cross-border cooperation as the most significant barrier to successful investigations. The result is a system where evidence is lost, leads go cold, and perpetrators operate with near-total impunity.

EMERGING THREATS AND EVOLVING TACTICS

The rapid evolution of AI-driven threats has outpaced law enforcement's ability to respond. Deepfakes, synthetic media, and AI-enhanced phishing now dominate the threat landscape, with attackers leveraging public trust to amplify disinformation campaigns. The identification of PromptLock ransomware,[67] the first known strain to generate dynamic, context-aware ransom notes using AI, signals a new era in which attacks are no longer static, but adaptive and personalized. Whilst this strain remains a concept created in academia, it demonstrates that the AI-powered ransomware technology now exists and it is only a matter of time before threat actors leverage similar technology, at scale and "in-the-wild".

Online scam investigations face unique hurdles: anonymized infrastructure, jurisdictional fragmentation, and delayed access to telecom and social media data. Legal gaps in evidence collection procedures, coupled with a shortage of trained investigators and forensic tools, mean that even when victims report crimes, cases often collapse before trial. Ransomware remains a persistent challenge, with 66 per cent of agencies reporting that victims are unable to recover encrypted files due to lack of decryption tools, insufficient VASP support, and delays in international collaboration. The emergence of AI-powered malware that evades signature-based detection further complicates attribution and defence.

The speed and scale of these attacks demand a shift from reactive, jurisdiction-bound responses to proactive, intelligence-led, and cross-border operations – a transition that most African agencies are not yet prepared to make.

CROSS-BORDER COOPERATION AND INFORMATION SHARING GAPS

Cross-border cybercrime investigations face complexities within established legal frameworks, highlighting an opportunity to streamline and harmonize procedures to achieve a more desirable outcome.

Half of all surveyed countries reported significant challenges in multi-jurisdictional cases, citing inconsistent definitions of cybercrime, missing urgent response protocols, and disparate data retention policies. While INTERPOL channels remain the primary mechanism for cooperation, they are often overwhelmed, under-resourced, and unable to bypass national legal barriers.

Based on the INTERPOL member country survey, subregional collaboration is uneven: East Africa demonstrates high CERT-to-CERT coordination, West Africa shows moderate cooperation, Southern Africa's efforts are mixed, and Central Africa's level of collaboration remains underdeveloped. The absence of standardized operating procedures between law enforcement and national cybersecurity agencies further impedes joint operations.

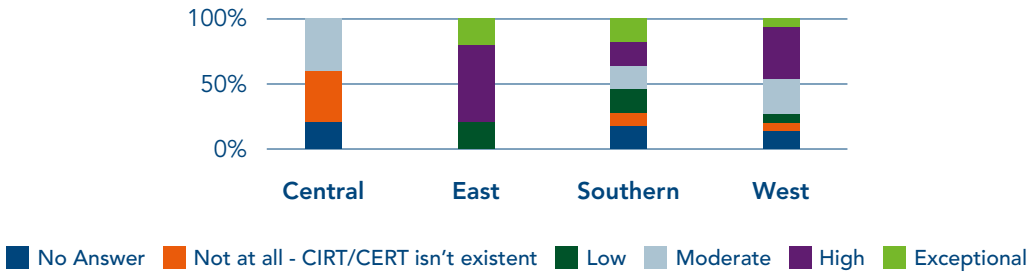


Figure 14: Rating or perception from member countries on LE and CERT/CSIRT/NCA collaboration (Source: INTERPOL member country survey).

67 ESET First known AI-powered ransomware uncovered by ESET Research 2025 (https://www.welivesecurity.com/en/ransomware/first-known-ai-powered-ransomware-uncovered-eset-research) (December 2025).

PUBLIC-PRIVATE PARTNERSHIPS AND PLATFORM ACCOUNTABILITY HURDLES

Public-private partnerships (PPPs) are essential to effective cybercrime response, yet they remain underdeveloped across Africa. While 44 per cent of countries now report "significant or some improvement" in PPP engagement, down from 89 per cent in prior assessments, barriers persist, according to the INTERPOL member country survey. Law enforcement lacks clear, lawful channels to request data from Meta, TikTok, and other social media platforms. Data retention policies conflict with privacy regulations, and telecom providers often refuse to share SIM swap logs without court orders – a process that can take weeks.

Fintechs and mobile money operators have yet to integrate real-time fraud alerts with national law enforcement systems. While Memoranda of Understanding (MoUs) exist, few agencies possess the technical or legal capacity to execute them effectively. The result is a system where vital evidence – IP logs, transaction trails, and account metadata – is siloed, inaccessible, or delayed. Without structured, trust-based, and legally grounded partnerships, the private sector remains a passive observer rather than an active participant in the fight against cybercrime.

REGIONAL EFFORTS TO COMBAT EMERGING CYBERCRIMINAL THREATS

PROGRESS IN COMBATTING CYBERCRIME IN AFRICA

As Africa's cybersecurity landscape substantially progresses in response to investigation and legal frameworks, cybercrime continues to intensify, accounting for more than 30 per cent of reported crime in the Western and Southern regions of Africa, according to the INTERPOL member country survey. To strengthen the ability to fight cybercrime, a multi-pronged strategy is imperative to sustain initiatives. The survey, which reflects ongoing efforts to outpace the speed of cybercrime, has uncovered positive developments for 2025 (see Figure 15).

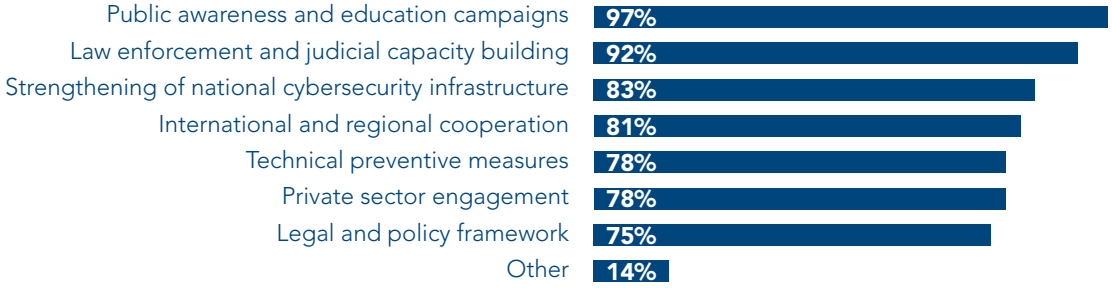


Figure 15: Key initiatives implemented by member countries in 2025 (Source: INTERPOL member country survey).

NATIONAL CYBERCRIME FRAMEWORK INITIATIVES

In 2025, seventeen countries enacted or amended cybercrime laws, signalling a growing recognition of cyberthreats as national security issues. Burkina Faso launched the "Alerte-BCLCC" reporting platform and adopted a National Cybercrime Strategy (2025-2029). Côte d'Ivoire's National Assembly passed the Digital Security Bill 2025, aligning its framework with international standards. Zambia enforced its Cyber Crime Act 2025, establishing clear definitions for online harassment, data protection, and digital fraud.

Mauritius unveiled its Digital Transformation Blueprint (2025-2029), creating a National Cyber-Resilience and Cybersecurity Agency. Kenya advanced its Computer Misuse and Cybercrimes (Amendment) Bill 2024 to target SIM swap and scam calls. South Sudan passed its Cybercrime and Computer Misuse Bill 2025, establishing a dedicated National Cybercrime Department.

Angola approved a National Cybersecurity Strategy and established a National Cybersecurity Centre with regulatory authority. Senegal launched "digital sovereignty," allocating USD 24 million to modernize platforms and combat cyber harassment, while also deploying a national platform to protect children online.

These legislative strides reflect a growing realization of cyber risk, but implementation remains the next critical step. Several countries showed signs of dedication to digital security in 2025 by amending or advancing legal frameworks on cybercrime (see Figure 16).

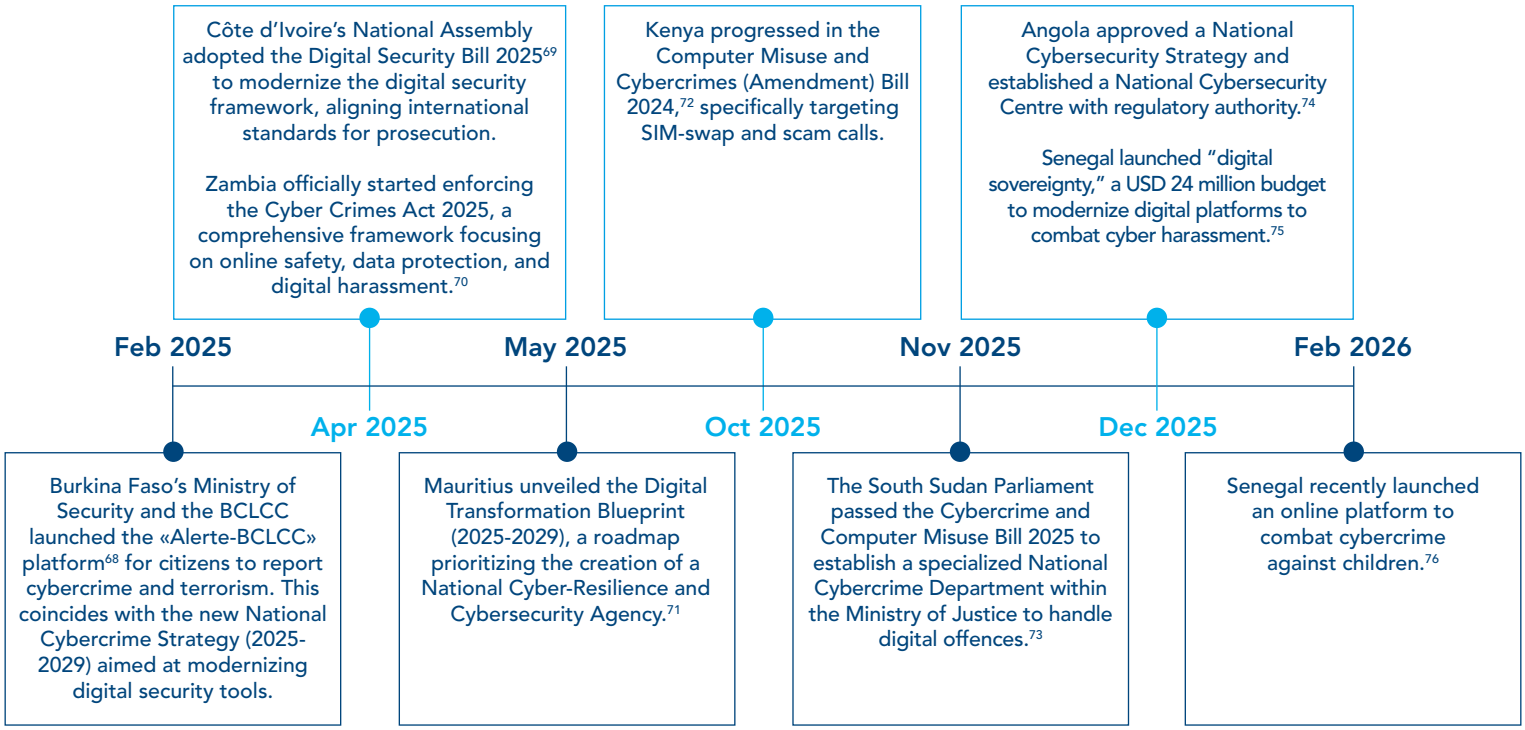


Figure 16: Notable updates to legal frameworks pertaining to cybercrime in Africa in 2025.

68 APAnews Burkina Faso launches new platform for reporting Cybercrimes 2025 (https://apanews.net/burkina-faso-launches-new-platform-for-reporting-cybercrimes/) (January 2026).

69 WeAreTech Côte d'Ivoire Approves New Digital Security Framework 2025 (https://www.wearetech.africa/en/fils-uk/news/tech/cote-d-ivoire-approves-new-digital-security-framework) (January 2026).

70 ZambiaLII Cyber Crimes Act, 2025 (https://zambialii.org/akn/zm/act/2025/4/eng@2025-04-15) (December 2025).

71 Ministry of Information Technology, Communication and Innovation A Blueprint for Mauritius a Bridge to the Future 2025 (https://mitci.govmu.org/mitci/wp-content/uploads/2025/05/Blueprint-for-Mauritius-2025.pdf) (December 2025).

72 Parliament of Kenya The Computer Misuse and Cybercrimes (Amendment) Bill, 2024 (https://parliament.go.ke/sites/default/files/2024-09/THE%20COMPUTER%20MISUSE%20AND%20CYBERCRIME%20%28AMENDMENT%29%20BILL%2C2024.pdf) (January 2026).

73 ICT & Postal Services REVITALIZED NAT'L LEGISLATIVE ASSEMBLY PASSED CYBERSECURITY AND COMPUTER MISUSE BILL 2025 (https://mictps.gov.ss/revitalized-natl-legislative-assembly-passed-cybersecurity-and-computer-misuse-bill/) (January 2026).

74 360 Mozambique Angola: Government Establishes National Cybersecurity Centre to Strengthen the Fight Against Digital Crime 2025 (https://360mozambique.com/world/angola/angola-government-establishes-national-cybersecurity-centre-to-strengthen-the-fight-against-digital-crime/) (January 2026).

75 Ecofin Agency Senegal Allocates $24 Million to Modernise Communications Sector in 2026 2025 (https://www.ecofinagency.com/news-digital/1212-51335-senegal-allocates-24-million-to-modernise-communications-sector-in-2026) (January 2026).

76 TechAfrica News Senegal Launches Online Platform to Combat Cybercrime Against Children 2026 (https://techafricanews.com/2026/02/13/senegal-launches-online-platform-to-combat-cybercrime-against-children/) (March 2026).

TRAINING, UPSKILLING, AND TECHNICAL CAPABILITIES

The Third African Forum on Cybercrime and Electronic Evidence in Nairobi brought together more than 300 experts from 31 nations, focusing on practical training in digital forensics and cross-border evidence handling. **Global Action on Cybercrime Extended (GLACY+),** a joint EU-Council of Europe initiative, supported capacity development in Benin, Burkina Faso, Cabo Verde, Ghana, Mauritius, Morocco, Nigeria, and Senegal, delivering training in cybercrime legislation, electronic evidence handling, and international cooperation. **Cyber4Dev,** funded by the European Union, strengthened national cybersecurity policies and incident response capacities in Botswana, Mauritius, Rwanda, and expanded training to Gambia, Malawi, Mozambique, Congo, and Seychelles.

The **Africa Joint Operation against Cybercrime (AFJOC),** implemented by INTERPOL's Africa Cybercrime Operations Desk and funded by the UK FCDO, delivered targeted capacity-building initiatives across the continent. These included the first-ever Mobile Forensic Workshop in Harare, Zimbabwe in December 2025, equipping investigators with tools to extract and analyse evidence from smartphones – a critical capability given the centrality of mobile devices in African cybercrime.

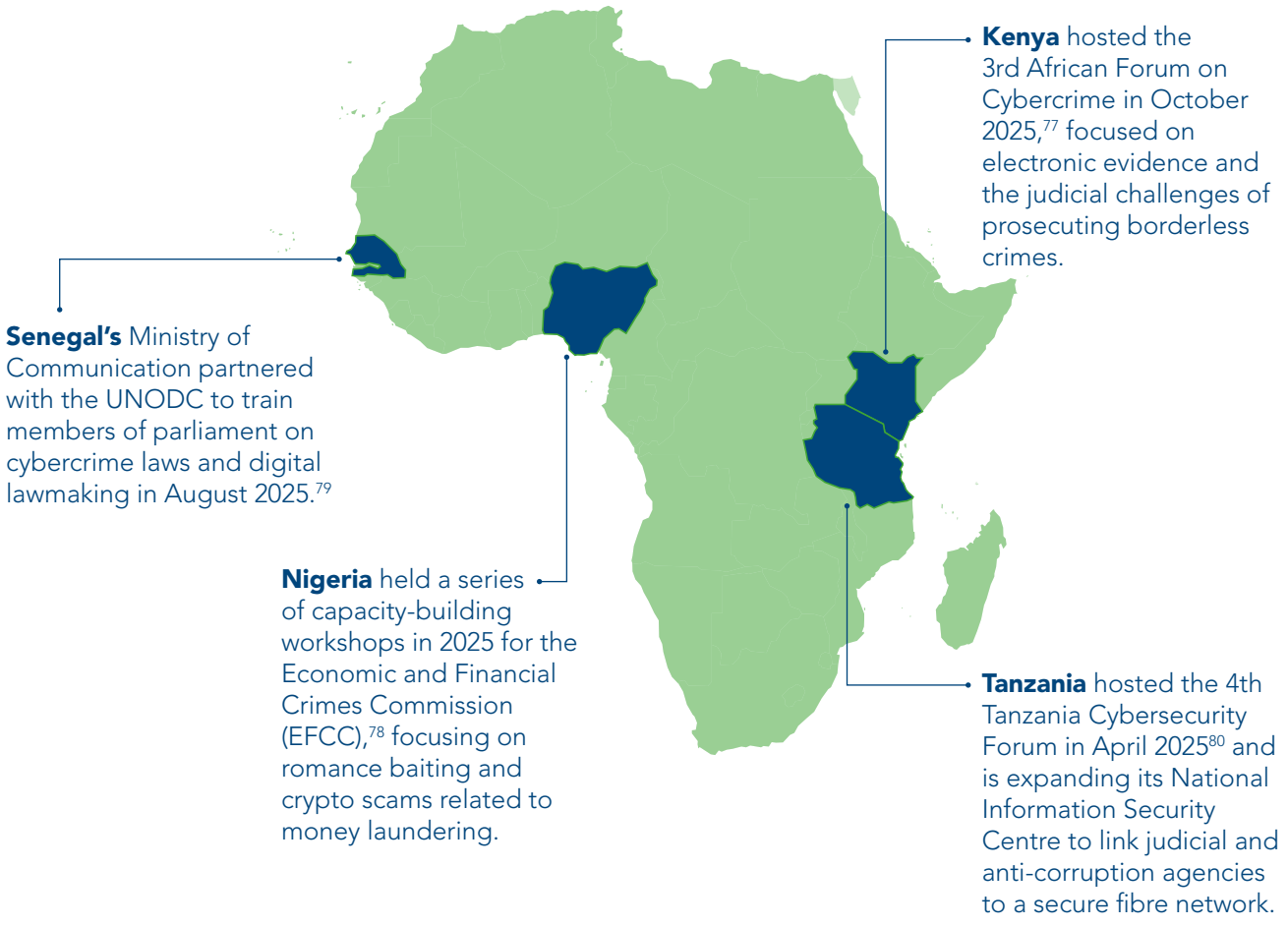


Figure 17: Notable upskilling initiatives on fighting cybercrime in African countries in 2025.

77 The Council of Europe Third African Forum on Cybercrime and Electronic Evidence 2025 (https://www.coe.int/en/web/cybercrime/3afcybercrime) (January 2026).

78 EFCC Opens Three-Day Workshop on AML/ CFT Enforcement in Nigeria 2025 (https://www.facebook.com/officialefcc/posts/efcc-opens-three-day-workshop-on-aml-cft-enforcement-in-nigeriathe-economic-and-/1385046840325182/) (January 2026).

79 TechAfrica News Senegal Trains Lawmakers on Digital Transformation and Cybersecurity 2025 (https://techafricanews.com/2025/08/29/senegal-trains-lawmakers-on-digital-transformation-and-cybersecurity/) (January 2026).

80 ICT Commission TANZANIA CYBER SECURITY FORUM 2025 (https://www.youtube.com/watch?v=2U1OBB4Svxc&t=6363s) (January 2026).

The International Telecommunications Union (ITU-INTERPOL) Cyber Drill, held in Brazzaville, Congo in July 2025, simulated large-scale cyber incidents across multiple sectors, testing CERT coordination and national response protocols. A Cryptocurrency Investigations Workshop in September 2025 trained police from the **Eastern Africa Police Chiefs Cooperation Organization (EAPCCO)** in blockchain analysis, wallet tracing, and asset recovery.

The *École Nationale de Cybersécurité à Vocation Régionale* (ENCVR) in Dakar, Senegal hosted a Cybercrime Investigation Workshop in December 2025, integrating regional law enforcement units into a structured, curriculum-based training model designed to foster sustained skill development and cross-border operational synergy.

These initiatives reflect a strategic shift: from ad hoc interventions to institutionalized, scalable, and regionally coordinated capacity building, a necessary foundation for long-term cyber resilience.

Mobile Forensic Workshop, including tools, held in Harare, Zimbabwe in December 2025.

ITU-INTERPOL Cyber Drill for Africa held in Brazzaville, Congo in July 2025.

Cryptocurrency investigation workshop in September 2025 for Eastern Africa Police Chiefs Cooperation Organization (EAPCCO) countries.

Cybercrime investigation workshop in December 2025 via the École Nationale De Cybersécurité À Vocation Régionale (ENCVR) Dakar School in Senegal.

Figure 18: INTERPOL's AFJOC initiatives in upskilling and capacity building of member countries in 2025.

EDUCATIONAL CAMPAIGNS TO ELEVATE CYBER RESILIENCE

Observations of public awareness campaigns in 2025 ranged from generic "stay safe online" messaging to highly targeted, culturally resonant initiatives designed to combat the most prevalent and damaging threats.

Ghana's National Cybersecurity Awareness Month (NCSAM) 2025[81] promoted accountability under the Cybersecurity Act 2020, introducing professional licensing for cybersecurity practitioners and launching mobile cyber-alert vans that demonstrated smartphone security practices nationwide, emphasizing the "4 P's": Passwords, Phishing, Privacy, and Patching. **South Africa's "Secure Our World" (SOW) 2025 campaign**[82] promoted safer online practices, and with the help of Digify Africa's Kitso WhatsApp learning bot, it guided the public with ease-of-content access and practical application. **Kenya's "Kaa Chonjo!" campaign,**[83] Swahili for "Don't Give It!", directly addressed SIM swap and ID-based loan fraud, instructing citizens never to share one-time passwords (OTPs) or personal identification numbers (PINs) via phone or message. **Rwanda's national initiative "Tekana Online"**[84] continued in 2025, and is a month-long campaign focused on protecting young people, parents, and educators, and informing the wider public on how to create a safer digital environment for young users, as well as educating young people.

LAW ENFORCEMENT COLLABORATION AND COORDINATION FOR SUCCESSFUL OPERATIONS

2025 witnessed an unprecedented level of coordinated, multinational cybercrime operations led by INTERPOL, resulting in tangible disruptions to transnational criminal networks. **Operation Serengeti 2.0,** conducted in early 2025, targeted illegal cryptocurrency mining operations, scam centres, and ransomware infrastructure across Angola, South Africa, and Uganda. The operation led to the dismantling of more than 1,200 malicious servers, the seizure of 1,800 devices, and the arrest of 120 individuals, disrupting networks responsible for USD 300 million in losses.[85]

Operation Contender 3.0 (July-August 2025) focused on romance scams and digital sextortion across 14 African countries. It resulted in 260 arrests, the seizure of more than 1,200 devices, and the identification of 1,500 victims, dismantling 81 online crime networks and recovering an estimated USD 2.8 million in illicit proceeds. **Operation Sentinel (October-November 2025)** was the largest coordinated cybercrime crackdown in African history, spanning 19 nations and targeting BEC, digital extortion, and ransomware. It led to 574 arrests, the recovery of approximately USD 3 million, the takedown of more than 6,000 malicious links, and the decryption of six ransomware variants, disrupting networks tied to more than USD 21 million in estimated losses.

Operation Red Card 2.0 (December 2025-January 2026) targeted high-yield investment fraud, mobile money scams, and fake loan applications across 16 African countries. The operation resulted in 651 arrests, the recovery of more than USD 4.3 million, the seizure of 2,341 devices, and the takedown of 1,442 malicious IPs and domains, uncovering scams responsible for USD 45 million in losses affecting 1,247 victims across Africa and beyond.

These operations were made possible through the integration of INTERPOL's I-24/7 secure communication system, and real-time intelligence sharing with private sector partners. Additionally, INTERPOL's collaboration with the Dutch National Police and the **International Cyber Offender Prevention Network (InterCOP)** has begun pilot programmes to rehabilitate young cyber offenders, recognizing that not all actors are hardened criminals; many are exploited youths recruited through online scams. The partnership with the ENCVR Dakar School has further institutionalized training as a pillar of operational readiness, embedding cybercrime investigation as a core competency within regional law enforcement academies.

81 Ghana Ministry of Communication, Digital Technology and Innovations Minister Launches 2025 National Cyber Security Awareness Month and Calls for Safer, More Accountable Digital Space (https://moc.gov.gh/2025/09/03/minister-launches-2025-national-cyber-security-awareness-month-and-calls-for-safer-more-accountable-digital-space/) (March 2026).

82 The Citizen Cybersecurity Awareness Month: How South Africans can stay secure online 2025 (https://www.citizen.co.za/germiston-city-news/news-headlines/local-news/2025/10/05/south-africans-urged-to-boost-online-safety-during-cybersecurity-awareness-month/) (April 2026).

83 Branch Kenya Facebook Ka Chongo 2025 (https://www.facebook.com/branchkenya/posts/kaa-chonjo-dont-save-your-bank-passwords-on-your-phone-or-browser-your-moneys-sa/1104854315136130/) (January 2026).

84 Rwanda National Cyber Security Authority The Tekana Online Campaign aims to protect youth online 2025 (https://cyber.gov.rw/updates/article/the-2025-tekana-online-campaign-aims-to-protect-youth-online/) (January 2026).

85 INTERPOL African authorities dismantle massive cybercrime and fraud networks, recover millions 2025 (https://www.interpol.int/en/News-and-Events/News/2025/African-authorities-dismantle-massive-cybercrime-and-fraud-networks-recover-millions) (March 2026).

RECOMMENDATIONS AND CONCLUSIONS

The cyberthreat landscape in Africa in 2025 presents a complex, evolving, and deeply entrenched challenge – one that cannot be addressed through isolated initiatives, reactive policing, or fragmented legal frameworks. The data are unequivocal: cybercrime is no longer a peripheral concern but a central pillar of transnational organized crime, enabled by AI, amplified by digital adoption, and exacerbated by institutional weakness.

However, the progress observed in 2025, legislative reform, operational coordination, public awareness, and capacity building, demonstrates that the foundations for a resilient cyber future are being laid. The critical imperative now is to scale, synchronize, and sustain these efforts through strategic, system-wide action.

CONCLUSION

The cyberthreat environment in Africa in 2025 remained complex, persistent, and evolving. Cybercrime continues to be a primary driver of financial loss, institutional disruption, and public distrust, with ransomware, business e-mail compromise (BEC), AI-facilitated scams, and digital identity fraud representing the most prevalent and damaging trends. These threats are increasingly transnational, automated, and enabled by accessible technologies, including generative AI and Cybercrime-as-a-Service (CaaS) platforms.

While national capacity has improved, with 17 countries enacting or amending cybercrime legislation, INTERPOL-coordinated operations resulting in more than 1,500 arrests, and regional training initiatives expanding forensic and crypto-investigation skills, significant gaps persist. Legal harmonization remains incomplete. Cross-border data sharing is often delayed by bureaucratic and procedural barriers. Technical capabilities are unevenly distributed, with many units lacking access to modern digital forensics tools, AI-detection systems, or secure communication infrastructure.

The operational reality is clear: cyber investigations require speed, standardization, and sustained coordination. Investigations that take months to initiate often lose critical evidence. Cases that rely on manual evidence collection struggle to keep pace with AI-driven attacks. Jurisdictional fragmentation continues to enable criminal mobility.

To national cyber investigative leaders, we recommend the following priorities:

1. **Standardize core capabilities.** Ensure all units have access to baseline digital forensic tools, including mobile device extraction, memory analysis, and cryptocurrency transaction tracing. Prioritize interoperability with regional and international systems such as INTERPOL's I-24/7.
2. **Strengthen legal and operational coordination.** Advocate for clear, binding protocols for cross-border data requests, especially for time-sensitive cases involving BEC, ransomware, or deepfake fraud.
3. **Invest in AI literacy, not just tools.** Train investigators to recognize and respond to AI-generated content – not merely to use AI tools, but to understand how adversaries deploy them. This includes identifying synthetic voices, forged identities, and automated phishing patterns. Basic AI-awareness is now a core investigative skill.
4. **Formalize public-private engagement.** Establish formal, lawful channels for information-sharing with telecoms, fintechs, and financial institutions. Ensure these partnerships are grounded in clear MoUs, defined data retention requirements, and mutual accountability, not ad-hoc requests.
5. **Measure and report impact.** Track and report outcomes: number of cases resolved, assets recovered, infrastructure disrupted, and evidence successfully admitted in court. This builds institutional credibility and informs resource allocation at the national level.

The challenges are not new, but the pace and scale of the threat are increasing. Success will not come from isolated efforts or reactive operations. It will come from sustained, coordinated, and professionalized cyber investigation, led by national units that are equipped, empowered, and integrated into a regional and global framework.

STRATEGIC RECOMMENDATIONS

BRIDGE THE RESOURCE, TECHNOLOGY, AND LEGAL GAPS TO UPSCALE CAPABILITY AND CAPACITY

- **Invest in technical capabilities:** Equip all national cybercrime units with standardized digital forensics toolkits, malware analysis platforms, and AI-powered threat detection systems. Prioritize mobile forensics, cryptocurrency tracing, and deepfake identification tools.
- **Develop specialized teams:** Establish dedicated national units for AI threat analysis, crypto-asset investigations, and cyber-enabled human trafficking. Train personnel in adversarial AI, behavioural profiling of cybercriminals, and automated evidence correlation.
- **Enhance resources and infrastructure:** Allocate minimum national budgets for cybercrime units, including secure communication devices, IMSI catchers, and forensic labs. Establish regional cyber forensic centres to serve under-resourced nations.
- **Strengthen cross-border cooperation:** Harmonize definitions of cybercrime across African jurisdictions and adopt standardized protocols for evidence preservation, data sharing, and 24/7 emergency response. Expand the use of MLATs and MoUs with binding timelines and enforcement mechanisms.
- **Expand training and awareness:** Mandate annual AI threat literacy training for all law enforcement officers, prosecutors, and judiciary members.
- **Improve reporting and detection:** Implement a centralized, real-time African cybercrime reporting portal, integrated with national CERTs, financial institutions, and telecom providers to enable immediate incident logging, threat correlation, and automated alerting.

STRENGTHEN LEGAL AND POLICY FRAMEWORKS THROUGH REGIONAL AND GLOBAL COLLABORATION

- **Accelerate adoption of dedicated cybercrime laws:** Many African countries continue to develop or update legal frameworks to address cybercrime, and further alignment with instruments such as the UN Cybercrime Convention and the AU Malabo Convention may support consistency across jurisdictions.
- **Harmonize regional and international standards:** Efforts to harmonize national with international approaches, including those under the Budapest Convention or UN Cybercrime Convention on electronic evidence, data preservation, and cross-border access could help improve coordination. A regional mechanism through AFRIPOL may further support these efforts.
- **Enhance cross-border cooperation:** Establish a 24/7 contact network to facilitate the secure and timely exchange of digital evidence across borders. A regional coordination hub featuring designated liaison officers from the respective member countries could be set up to facilitate expeditious information exchange during major incidents.
- **Strengthen and harmonize legal frameworks:** Expand MLATs to include expedited procedures for urgent data requests related to ransomware, BEC, and deepfake crimes. Standardize data retention policies across telecoms and fintechs to ensure evidence is preserved.
- **Establish urgent protocols:** Create an Incident Response Protocol at a regional level to govern the rapid sharing of IOCs, threat intelligence, and suspect information between national agencies and INTERPOL.

CLOSE CROSS-BORDER GAPS AND STRENGTHEN PUBLIC-PRIVATE PARTNERSHIPS

- **Strengthen cooperation:** Leverage existing agencies such the Southern African Development Community (SADC), Economic Community of West African States (ECOWAS), and AFRIPOL to institutionalize joint cyber operations, training exchanges, and intelligence fusion centres.
- **Enhance police & CERT collaboration:** Formalize Standard Operating Procedures (SOPs) between law enforcement and national CERTs/Computer Incident Response Team (CIRTs) for evidence handover, joint investigations, and coordinated incident response.
- **Improve response protocols:** Mandate real-time data retention by telecoms and fintechs for fraud-related investigations. Establish a regional cyber-data-sharing trust framework with technical safeguards and audit mechanisms.
- **Accelerate telecom and fintech collaboration:** Require all mobile money platforms and fintechs to integrate real-time fraud alerts with national cybercrime units. Mandate biometric verification at point of SIM registration and KYC onboarding.
- **Promote public engagement:** Sustain and scale national awareness campaigns. Integrate cyber resilience into school curricula and public service messaging. Establish anonymous, multilingual reporting hotlines for victims of sextortion and scams.

STAY ABREAST OF EMERGING TECHNOLOGIES AND AI ADOPTION TO COMBAT CYBERCRIME

- **Reinforce online scam and ransomware response:** Establish dedicated crypto-investigation units within national financial intelligence units. Require VASPs to report suspicious transactions.
- **Build AI-ready capabilities:** Equip law enforcement with AI-assisted tools for deepfake detection, voice authentication, and anomaly detection in communication patterns. Train investigators to use AI as an investigative force multiplier – not a replacement for human judgment.
- **Adopt proactive, intelligence-led strategies:** Shift from reactive incident response to predictive threat hunting. Deploy AI-driven threat intelligence platforms that correlate global and regional indicators to anticipate attacks before they occur.
- **Enhance public trust and response:** Develop and deploy open-source tools for the public to verify the authenticity of videos, audio, and messages, particularly during elections or public emergencies.
- **Counter ransomware operators:** Coordinate regional intelligence-sharing on threat actors such as Qilin, RansomHub, and Devman. Mandate sector-wide cyber audits for critical infrastructure. Enforce mandatory backup and recovery standards for all public institutions.
- **Support international cooperation:** Strengthen ties with international law-enforcement agencies such as INTERPOL, Europol, and AFRIPOL to share threat intelligence, train investigators, and coordinate transnational operations. Seek technical assistance from global cybersecurity firms to build local capacity, not dependency.

ABOUT INTERPOL

INTERPOL's role is to enable police in our 196 member countries to work together to fight transnational crime and make the world a safer place. We maintain global databases containing police information on criminals and crime, and we provide operational and forensic support, analysis services and training. These policing capabilities are delivered worldwide and support four global programmes: financial crime and corruption; counter-terrorism; cybercrime; and organized and emerging crime.

OUR VISION: "CONNECTING POLICE FOR A SAFER WORLD"

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

ABOUT THE INTERPOL CYBERCRIME PROGRAMME

In a dynamic digital age, where more than half the global population is at potential risk from cybercrime, the INTERPOL Cybercrime Directorate 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.

For any further information, please contact the INTERPOL Cybercrime Directorate at the following e-mail address:

EDPS-CD@interpol.int

ABOUT THE INTERPOL AFRICA JOINT OPERATION AGAINST CYBERCRIME (AFJOC)

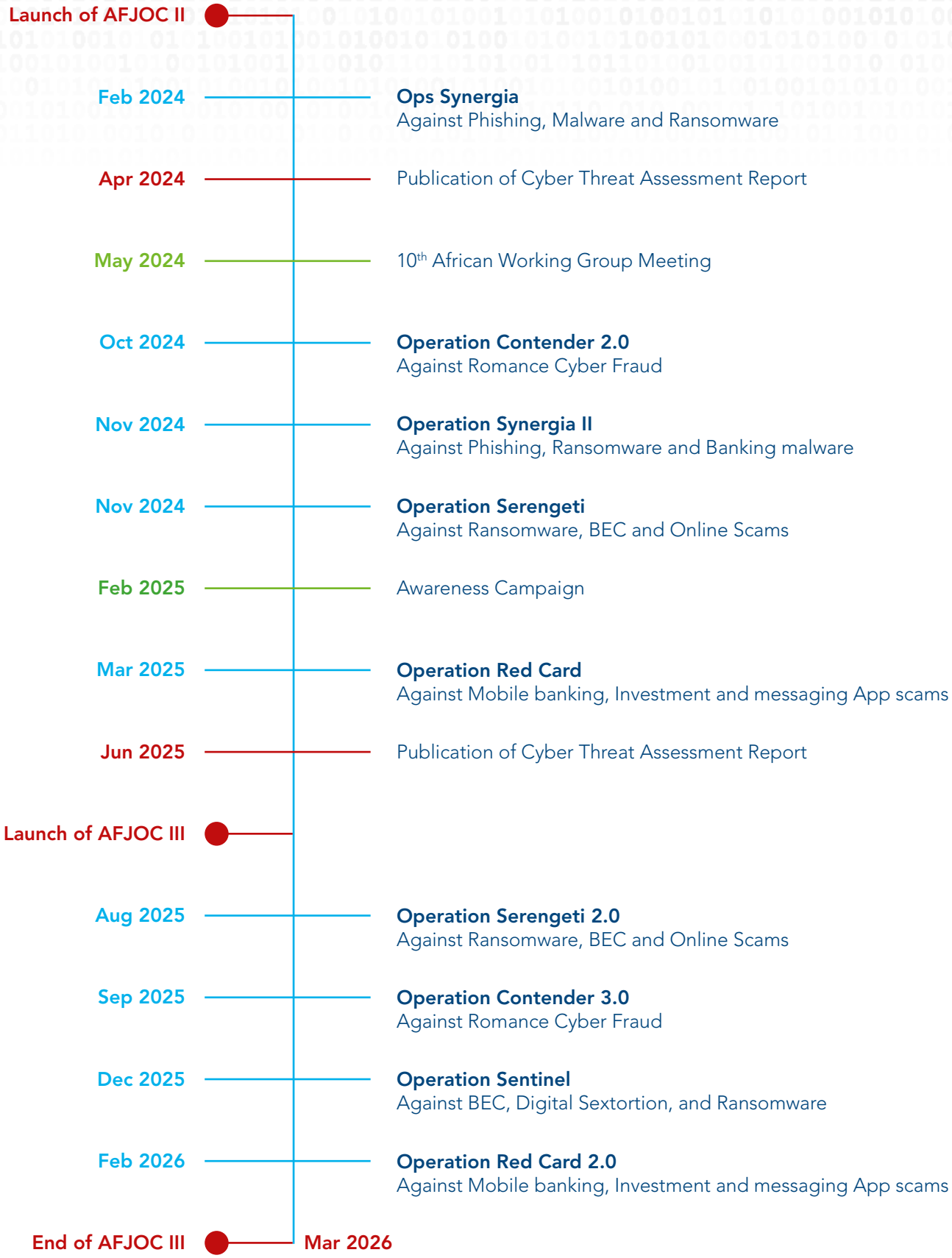
AFJOC is an INTERPOL initiative aimed at strengthening the capability of African national law enforcement agencies to prevent, detect, investigate, and disrupt cybercrime. This is achieved by:

- Gathering and analysing information on cybercriminal activity
- Carrying out intelligence-led, coordinated action
- Promoting cooperation and best practice amongst African member countries.

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 communications 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.


Launch of AFJOC II
Feb 2024
Ops Synergia
Against Phishing, Malware and Ransomware
Apr 2024
Publication of Cyber Threat Assessment Report
May 2024
10th African Working Group Meeting
Oct 2024
Operation Contender 2.0
Against Romance Cyber Fraud
Nov 2024
Operation Synergia II
Against Phishing, Ransomware and Banking malware
Nov 2024
Operation Serengeti
Against Ransomware, BEC and Online Scams
Feb 2025
Awareness Campaign
Mar 2025
Operation Red Card
Against Mobile banking, Investment and messaging App scams
Jun 2025
Publication of Cyber Threat Assessment Report
Launch of AFJOC III
Aug 2025
Operation Serengeti 2.0
Against Ransomware, BEC and Online Scams
Sep 2025
Operation Contender 3.0
Against Romance Cyber Fraud
Dec 2025
Operation Sentinel
Against BEC, Digital Sextortion, and Ransomware
Feb 2026
Operation Red Card 2.0
Against Mobile banking, Investment and messaging App scams
End of AFJOC III
Mar 2026

INTERPOL