



Third African Forum on Cybercrime and Electronic Evidence

Nairobi, Kenya
25 – 27 November 2025



**Third African Forum on Cybercrime
and Electronic Evidence**

Nairobi, Kenya | 25-27 November 2025

IMPACT OF ARTIFICIAL INTELLIGENCE ON CYBERCRIME

DR IFEOMA E. NWAFOR



Introduction

- There is an evolving intersection between artificial intelligence (AI) and cybercrime in Africa and globally.
- Cybercriminals are leveraging advanced technologies to escalate various cybercrime activities. There has been an alarming increase in AI-enabled cybercrime in Africa, including voice cloning, phishing, Business Email Compromise (BEC), deepfakes, AI-crafted text, misinformation, synthetic identity fraud and romance scams. AI has amplified the scale of cybercrime, making it easier, faster, and cheaper to target vulnerable people.
- Deep learning models can clone voices, mimicking vocal tone, pitch and cadence with high fidelity, facilitating impersonation scams.

- The INTERPOL Africa Cyberthreat Assessment Report 2025 underlines a drastic increase in cybercrime incidents across Africa.
- The Report highlights that the illegitimate use of AI, mobile-enabled fraud schemes and synthetic media is limiting the capacity of law enforcement to investigate and prosecute AI-facilitated cybercrime in Africa.



SURVEY

A report from Microsoft highlights that in Africa, AI-generated content and synthetic identities are increasingly used to bypass verification, enabling attacks such as BEC, malware with autonomous movement, etc.

The report found that although BEC made up just 2% of observed threats, it was the **outcome in 21% of successful breaches**, surpassing ransomware (16%) in the African region.



Real life case scenarios: Africa

- A British widow lost **over £ 150,000** after believing she was chatting with a U.S. Army general on Instagram; the scammer used the generative AI tool ChatGPT to craft messages, as well as a voice-cloning app to mimic an American accent. The scammer was later traced to Lagos, Nigeria.
- A 53-year-old French woman, identified as Anne, was defrauded of 830,000 Euros (\$850,000) by scammers posing as the Hollywood actor, Brad Pitt. The scammers employed AI-generated images and videos to establish trust, and Anne believed she was in a relationship with Brad.

- 
- There are multiple cases of AI- generated deepfake videos used to blackmail corporate executives in Africa.
 - Misinformation- AI enables the creation of sophisticated disinformation in Africa. Countries like Tanzania, Uganda and Kenya have experienced significant issues with AI-generated electoral misinformation.
- 



Can AI serve as a valuable ally in combating, detecting and investigating AI-related cybercrime?

- There is an ongoing debate about how AI can enable defenders to detect, predict, and respond effectively to cyber threats using AI technologies.
 - However, AI tools are laced with human rights, legal and ethical concerns.
 - Puzzle- Balancing ethical AI usage, transparency, accountability, privacy, human rights and security
- 

Empirical research: Nigeria as Case Study

- Empirical research titled “Accountable Predictive Policing: Insights from Nigerian Law enforcement” sought to determine if AI technologies, particularly predictive policing tools can be effectively applied to mitigate cybercrime in Nigeria despite the ethical, legal and human rights concerns entrenched in such AI- driven tools across all domains of their usage.
- Methodology: questionnaires and in-depth interviews with officers from the Cybercrime Units of the Nigerian Economic and Financial Crimes Commission.



Results of the criminological analysis that are noteworthy include:

- 80% of survey participants state that AI-driven cybercrime make investigation challenging.
 - 73.3% believe that there are cybercrime patterns that make predictive policing suitable to mitigate cybercrime in Nigeria.
 - 74% of the participants are unaware of the ethical challenges surrounding AI.
 - This indicates a readiness and capacity Gap.
- 

Limitations

- **Lack of dedicated AI regulation-** the absence of a dedicated AI regulation in some Africa countries that stipulates the legal status, oversight of risk and compliance management of AI technologies cripples the fight against AI-driven cybercrime in the region. Outdated laws and the lack of clear guidelines on AI use in investigations and evidence handling and preservation. This may lead to unethical AI usage that affects fundamental rights.
- **Skills gap-** limited AI expertise and inconsistent infrastructure remain hurdles in effective regional AI cyber threat management. Inadequate database and algorithmic bias risks unfair profiling, discrimination, etc. Most law enforcement agencies in Africa lack the technological infrastructure and a comprehensive cybercrime database needed for accountable, effective datasets for AI training.



Limitations

- **Cross-border challenges for regulation-** global AI cybercrime complicates jurisdiction and enforcement, especially in regions with limited cyber law frameworks.
 - **Insufficient funding** for advancing cybercrime units of law enforcements agencies impacts investigative capabilities and training.
 - **Balancing transparency, privacy, human rights and security-** law enforcement must navigate and balance transparency, privacy and human rights laws while employing AI surveillance and biometrics to avoid overreach.
- 

Conclusion

Based on the insights from Nigerian law enforcement, although there are potential benefits and cybercrime patterns that make AI technologies suitable to mitigate AI-facilitated cybercrime, there is an urgent need for **legal clarity, ethical safeguards, institutional readiness, formal measurement or oversight of compliance and risk management of AI usage and better design of capacity-building** to address the limitations discussed and the dual challenges of AI and cybercrime and ensure African countries can leverage AI's transformative potential while mitigating its associated risks.