Artificial Intelligence and the Changing Patterns of Crime in Nigeria: Implications for Social Control

Noah Lumun Abanyam[1*], Isa Hamza[2], David Francis (PhD)[3]

[123]Department of Sociology, Taraba State University, Jalingo, Taraba State

DOI: https://doi.org/10.47772/IJRISS.2026.101000697

Received: 28 October 2026; Accepted: 03 November 2026; Published: 16 November 2026

ABSTRACT

The increasing application of artificial intelligence (AI) is transforming criminal activities and creating emerging challenges for mechanisms of social control in Nigeria. This study examined the changing patterns of AI-assisted criminality and their implications for crime prevention, institutional regulation and social control. Anchored in Social Control Theory and Routine Activity Theory, the study adopted a qualitative integrative literature review and documentary analysis of scholarly publications, institutional reports, Nigerian legislation and relevant policy documents. The findings revealed that AI is reshaping existing forms of cybercrime through automated financial fraud, identity impersonation, deepfake-enabled deception, social engineering and transnational criminal operations. Available evidence further indicated that socioeconomic pressures, weakened informal social controls, institutional capacity limitations and inadequate technological guardianship contribute to vulnerabilities associated with emerging digital criminal activities. However, existing Nigerian cybercrime statistics do not sufficiently distinguish AI-enabled offences from conventional cybercrime, limiting accurate assessments of their prevalence and economic consequences. The study also identified challenges involving digital evidence authentication, cross-border jurisdiction, data protection and inter-agency coordination. It argued that effective responses require the integration of technological safeguards with formal and informal mechanisms of social control. The study recommended specialised digital forensic training, strengthened cybersecurity legislation, improved financial fraud detection, community-based digital literacy, institutional accountability and international cooperation. It concluded that addressing AI-assisted criminality in Nigeria requires a preventive, technologically responsive and socially inclusive approach that strengthens crime prevention while safeguarding fundamental human rights.

Keywords: Artificial Intelligence; Cybercrime; Criminal Behaviour; Social Control; Digital Criminology; Nigeria.

INTRODUCTION

The rapid advancement of artificial intelligence (AI) has introduced significant transformations in contemporary social organisation, economic activities, communication systems and institutional governance. Artificial intelligence increasingly influences how individuals access information, conduct financial transactions, establish interpersonal relationships and participate in digital environments. While these developments have created opportunities for innovation, economic productivity and improved public administration, they have also introduced vulnerabilities that can be exploited for criminal purposes. Schmitt and Flechais (2024) explain that generative artificial intelligence has transformed social engineering by facilitating realistic content creation, personalised deception and automated criminal communication. These capabilities suggest that technological innovation is increasingly influencing not only the methods through which crimes are committed but also the opportunities available to offenders and the effectiveness of conventional crime prevention mechanisms.

Historically, technological advancement has influenced the organisation and execution of criminal activities. The emergence of electronic banking, mobile communication and internet-based commercial transactions has transformed conventional offences such as fraud, forgery, theft and identity manipulation into increasingly complex forms of digitally mediated criminality. However, artificial intelligence introduces distinctive challenges because of its capacity to imitate human communication, generate convincing synthetic information

and automate activities previously requiring substantial individual effort. Heiding et al. (2026), in an experimental investigation involving 101 participants, found that fully AI-generated phishing messages achieved click-through rates comparable to those developed by human experts. Although the findings cannot be generalised directly to Nigerian criminal activities, they provide evidence that artificial intelligence can improve the effectiveness and accessibility of particular forms of digital deception.

Across Africa, the increasing adoption of digital technologies has been accompanied by growing concerns regarding cyber-enabled financial fraud, online extortion and transnational criminal networks. INTERPOL (2025) identified online scams, ransomware, business email compromise and digital sextortion among the principal cyberthreats confronting African countries. Its assessment also revealed significant institutional capacity limitations, with 90% of surveyed African countries reporting the need for substantial improvements in law enforcement or prosecutorial capabilities. More recently, INTERPOL (2026) reported that artificial intelligence was associated with approximately 55% of reported cybercrimes covered by its regional assessment involving 36 African member countries. Although this figure should not be interpreted as a Nigeria-specific prevalence estimate, it illustrates the increasing significance of AI-assisted criminality within Africa's evolving digital security environment.

Nigeria presents an important context for examining these developments because of its expanding digital economy and longstanding experience with cyber-enabled financial fraud. Criminal activities popularly described as *Yahoo-Yahoo* have evolved alongside technological changes, creating opportunities for identity manipulation, romance fraud, business email compromise and other forms of financial deception. Lazarus et al. (2022) demonstrate that cybercriminal behaviour in Nigeria cannot be understood exclusively through technological explanations because public perceptions of corruption, inequality and criminal legitimacy influence attitudes towards internet fraud. Similarly, Aborisade (2023) reveals that parental acceptance and moral justification may sometimes weaken informal mechanisms for discouraging cybercriminal involvement. These findings suggest that contemporary cybercrime operates within broader socioeconomic and cultural environments that influence criminal opportunities and social responses.

Artificial intelligence introduces additional complexities into these established criminal environments. Its capacity to generate persuasive messages, manipulate audiovisual information and automate deceptive communication may increase the sophistication of existing offences while creating new difficulties for victims, financial institutions and law enforcement agencies. Nevertheless, technological innovation does not independently explain criminal involvement. Button et al. (2025), drawing on 36 interviews involving stakeholders connected to Nigeria and Ghana, identify economic pressures, peer relationships, family attitudes and social expectations as important influences on participation in cyber-enabled fraud. Their findings reinforce the importance of examining technological criminality within the social structures that shape human behaviour.

Despite increasing scholarly attention to artificial intelligence and cybercrime, existing research frequently examines technological vulnerabilities, criminal motivations and institutional responses as separate concerns. Consequently, insufficient attention has been directed towards integrating these dimensions within a sociological explanation of changing mechanisms of social control in Nigeria.

The central argument of this article is that artificial intelligence is transforming criminal opportunities while simultaneously challenging the social relationships, institutional arrangements and technological safeguards through which criminal behaviour is regulated. Accordingly, the article examines emerging AI-assisted criminal activities in Nigeria, evaluates their implications for formal and informal social control, and proposes strategies for strengthening crime prevention within an increasingly digital society.

LITERATURE REVIEW AND CONCEPTUAL CLARIFICATION

Artificial Intelligence and Criminal Behaviour

Artificial intelligence refers broadly to computational systems capable of performing activities associated with human cognitive functions, including learning, prediction, language processing and decision-making. Contemporary applications include machine learning, natural language processing, biometric identification and

generative systems capable of producing written, visual and auditory content. Although these technologies support legitimate activities, their dual-use characteristics create opportunities for criminal exploitation.

Schmitt and Flechais (2024) identify realistic content generation, personalised targeting and automated attack infrastructure as important mechanisms through which generative AI can strengthen social engineering. These capabilities enable deceptive communication to become more convincing and potentially less dependent on offenders' technical expertise. However, the criminal consequences of artificial intelligence depend on how technological capabilities interact with offender motivations, available opportunities and institutional safeguards.

From a criminological perspective, artificial intelligence should therefore be understood as an enabling technology rather than an independent cause of criminal behaviour. Its significance lies in its capacity to alter existing criminal techniques, expand opportunities for offending and complicate mechanisms of detection and accountability.

Changing Patterns of Crime in Nigeria

Crime patterns in Nigeria have undergone significant changes alongside expanding internet connectivity, electronic financial services and digital communication. Traditional offences involving theft, deception and financial exploitation increasingly occur through online platforms that allow offenders and victims to interact without physical contact.

Lazarus et al. (2022) demonstrate that Nigerian cybercriminality is influenced by broader perceptions of corruption and moral justification. Their findings suggest that some social media participants rationalise internet fraud through comparisons between cybercriminals and political actors perceived as corrupt. Similarly, Button et al. (2025) identify economic pressures, peer influence, social recognition and weaknesses in formal social control as important factors associated with cyber-fraud involvement in West Africa.

These studies provide valuable sociological explanations of digital criminal behaviour. Nevertheless, they do not establish the extent to which artificial intelligence has been incorporated into specific Nigerian criminal operations. This distinction is important because the expansion of cybercrime cannot automatically be attributed to AI adoption.

Social Control in Contemporary Society

Social control refers to the processes through which society regulates behaviour, promotes conformity and discourages activities considered harmful or unacceptable. Formal social control operates through institutions such as the police, courts and regulatory agencies, while informal social control is exercised through families, educational institutions, religious organisations and community relationships.

Hirschi (1969) argues that conformity is strengthened through attachment, commitment, involvement and belief. These elements establish relationships between individuals and conventional institutions, thereby reducing the likelihood of criminal participation. Costello and Laub (2020) reaffirm the continuing significance of social bonding for understanding delinquency and conformity. However, technological development has expanded the institutions involved in regulating behaviour. Financial institutions, telecommunications operators and digital platforms increasingly employ automated systems to identify suspicious activities and enforce security standards. Gorwa et al. (2020) explain that algorithmic moderation has become an important component of digital platform governance, although its implementation raises concerns about transparency, institutional power and accountability. Consequently, contemporary social control increasingly involves interaction between conventional institutions and technologically mediated regulatory arrangements.

THEORETICAL FRAMEWORK

The article adopts Social Control Theory and Routine Activity Theory as complementary perspectives for exp-

laining the relationship between artificial intelligence, criminal behaviour and institutional regulation.

Social Control Theory

Social Control Theory was developed by Travis Hirschi (1969) to explain why individuals conform to social norms rather than engage in criminal behaviour. The theory identifies attachment, commitment, involvement and belief as essential elements of social bonding. Strong relationships with conventional institutions are expected to discourage deviant behaviour, while weakened social bonds may increase vulnerability to criminal involvement.

The theory is relevant to contemporary cybercriminality in Nigeria because criminal participation is influenced by family expectations, peer relationships and community attitudes towards illegitimate financial success. Aborisade (2023) demonstrates that some parents of cybercrime-involved youths rationalise or support their children's activities. Similarly, Button et al. (2025) identify social recognition, parental attitudes and cultural expectations as factors influencing involvement in cyber-enabled fraud.

These findings suggest that informal social control may become ineffective when criminal financial gains receive social approval. Nevertheless, Social Control Theory does not adequately explain the technological conditions that create emerging criminal opportunities. This limitation necessitates complementary theoretical interpretation.

Routine Activity Theory

Routine Activity Theory was developed by Cohen and Felson (1979). The theory proposes that criminal opportunities emerge through the convergence of motivated offenders, suitable targets and the absence of capable guardianship.

Within digital environments, artificial intelligence may influence criminal opportunities by facilitating target identification, identity impersonation and deceptive communication. Suitable targets include individuals, businesses and institutions exposed to technologically mediated fraud. Capable guardianship involves security awareness, reliable authentication systems, institutional monitoring and effective law enforcement.

Griffith et al. (2023) demonstrate the relevance of routine activity explanations to cybervictimisation, identifying relationships between online activities, exposure to potential offenders and protective behaviours.

The integration of both theories provides a comprehensive analytical perspective. Social Control Theory explains the social conditions influencing criminal participation, while Routine Activity Theory explains the opportunities through which criminal behaviour becomes possible. Together, the theories suggest that AI-assisted criminality may become more harmful where expanding technological opportunities intersect with weakened social regulation and inadequate institutional guardianship.

Integration of Social Control Theory and Routine Activity Theory into Digital Guardianship

The integration of Social Control Theory and Routine Activity Theory provides a comprehensive framework for understanding technological guardianship in the prevention of AI-enabled criminality in Nigeria. Hirschi's (1969) Social Control Theory emphasises the importance of social bonds, moral values and institutional attachments in discouraging criminal behaviour, while Cohen and Felson's (1979) Routine Activity Theory explains how crime occurs through the convergence of motivated offenders, suitable targets and the absence of capable guardianship. Within digital environments, technological guardianship involves the application of cybersecurity awareness, identity verification, fraud detection systems, digital forensic capabilities and institutional monitoring to reduce opportunities for criminal exploitation. These mechanisms complement informal social controls exercised through families, educational institutions, religious organisations and community relationships.

In Nigeria, effective technological guardianship requires collaboration among law enforcement agencies, financial institutions, telecommunications providers, educational institutions and local communities. Digital

literacy programmes can strengthen individuals' ability to recognise AI-generated deception, while secure authentication systems and coordinated incident reporting can reduce exposure to identity theft, financial fraud and automated social engineering. However, technological monitoring must operate within appropriate legal safeguards to protect personal privacy, prevent discriminatory surveillance and promote institutional accountability. Consequently, combining technological safeguards with strong social relationships and responsible institutional governance offers a more comprehensive approach to addressing emerging AI-assisted criminal activities (Gorwa et al., 2020; Griffith et al., 2023).

METHODOLOGY

This study adopted a qualitative integrative literature review and documentary analysis to examine the relationship between artificial intelligence, changing patterns of crime, and mechanisms of social control in Nigeria. The study was anchored in Social Control Theory (Hirschi, 1969) and Routine Activity Theory (Cohen & Felson, 1979). Data were obtained from secondary sources, including peer-reviewed journal articles, institutional reports, Nigerian legislation, and relevant policy documents published primarily between 2020 and October 2026. Particular attention was given to reports from INTERPOL, publications on electronic financial fraud in Nigeria, the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, as amended in 2024, the Nigeria Data Protection Act, 2023, and the National Artificial Intelligence Strategy, 2025. These sources provided theoretical, empirical, and institutional evidence for understanding emerging AI-assisted criminal activities within the Nigerian context.

The study employed thematic analysis to synthesise findings under major themes, including AI-assisted financial fraud, identity impersonation, deepfake-enabled deception, automated social engineering, transnational cybercrime, and implications for social control. Available Nigerian cybercrime statistics and documented institutional assessments were critically examined to strengthen empirical interpretation, while distinguishing confirmed criminal activities from emerging technological risks. The analysis further explored technological guardianship, digital literacy, institutional accountability, and cooperation among law enforcement agencies, financial institutions, and communities as mechanisms for preventing AI-enabled criminality. Although the study relied on secondary evidence without primary field investigations, the approach provided a theoretically grounded understanding of emerging crime patterns and their implications for social control in Nigeria.

Artificial Intelligence and the Changing Patterns of Crime in Nigeria

AI-Assisted Financial Fraud and Identity Theft

Financial fraud constitutes an important dimension of Nigeria's contemporary digital criminal environment. The expansion of electronic banking, mobile financial services and internet-based commercial transactions has created opportunities for economic participation while exposing individuals and institutions to increasingly sophisticated forms of financial deception.

Artificial intelligence may strengthen financial fraud through personalised phishing messages, synthetic identities and automated communication. Heiding et al. (2026) demonstrate that AI-generated phishing messages can perform comparably to human-developed attacks under experimental conditions. This finding indicates that artificial intelligence can reduce certain operational requirements associated with deceptive communication.

However, available Nigerian financial fraud statistics require careful interpretation. Ejalonibu et al. (2026), drawing on Nigeria Inter-Bank Settlement System data, report that losses from electronic payment fraud decreased from approximately ₦52.26 billion in 2024 to ₦25.85 billion in 2025. Reported fraud incidents also declined during the period. These developments demonstrate that technological sophistication does not necessarily produce continuous increases in recorded financial crime. More importantly, the statistics do not establish what proportion of reported offences involved artificial intelligence.

Therefore, the emerging concern is not simply the volume of financial fraud but the changing techniques through which criminal actors may exploit technological systems and human vulnerabilities.

Deepfakes, Impersonation and Digital Extortion

The emergence of generative artificial intelligence has increased the accessibility of synthetic audio, images and video that can imitate authentic human communication. Although these technologies have legitimate applications, their misuse creates opportunities for impersonation, reputational attacks, harassment and financial extortion.

Sandoval et al. (2024), in a systematic review examining deepfake threats to criminal justice, identify fraud, manipulated information and the falsification of digital evidence among important emerging concerns. Their findings suggest that synthetic media may undermine the reliability of audiovisual information and complicate investigative and judicial processes.

These developments have important implications for Nigeria, where social relationships increasingly depend on digital communication. Fraudulent audiovisual content may be used to imitate trusted individuals, exploit interpersonal relationships or threaten victims with reputational damage.

The consequences are particularly significant for victims of technology-facilitated sexual exploitation. Aborisade (2022), examining image-based sexual abuse in Nigeria, demonstrates that victims experience serious psychological and social consequences, including stigma, isolation and secondary victimisation.

Although this research does not specifically establish the prevalence of AI-generated sexual imagery, it provides a relevant foundation for understanding the potential social consequences of synthetic image abuse within culturally conservative environments. Consequently, AI-related criminality must be evaluated beyond financial losses to include psychological harm, reputational damage and the erosion of interpersonal trust.

Automation and Transnational Criminal Opportunities

Artificial intelligence is also changing criminal opportunities through the automation of activities previously requiring sustained individual participation. Generative AI systems can produce persuasive communication, process information and support interactions with multiple potential victims. Schmitt and Flechais (2024) explain that automated attack infrastructure constitutes an important dimension of AI-enabled social engineering. Such capabilities may enable offenders to increase the scale of deceptive operations while reducing certain operational costs. These developments also have implications for transnational criminality. Digitally mediated offences frequently involve victims, perpetrators and financial systems located across different jurisdictions. Artificial intelligence can further complicate these relationships by supporting multilingual communication and identity manipulation.

INTERPOL (2026) describes African cybercriminality as increasingly organised and transnational, highlighting the expansion of automated criminal techniques and limitations in international regulatory coordination. For Nigeria, these developments suggest that effective crime prevention cannot depend exclusively on territorially restricted policing arrangements. International cooperation, digital evidence preservation and collaboration between financial institutions and law enforcement agencies are increasingly necessary.

Nevertheless, the relationship between AI adoption and transnational criminal expansion requires further empirical investigation. Existing evidence establishes emerging technological capabilities but does not adequately quantify their specific contribution to Nigerian organised criminal networks.

Socioeconomic Conditions and the Normalisation of Cybercrime

The transformation of criminal techniques cannot be separated from the socioeconomic and cultural conditions influencing criminal behaviour. In Nigeria, unemployment, limited economic opportunities, social inequality and the pursuit of financial recognition have been identified as factors associated with participation in cyber-enabled fraud.

However, economic deprivation alone cannot sufficiently explain criminal involvement. Lazarus et al. (2022) demonstrate how perceptions of political corruption may influence the moral justification of cybercriminal activities. Their findings indicate that criminal conduct may become rationalised through comparisons with perceived wrongdoing among powerful social actors.

Similarly, Button et al. (2025) identify social recognition, peer relationships, family attitudes and cultural expectations as important influences on cyber-fraud participation. These findings suggest that the effectiveness of informal social control depends partly on the extent to which communities consistently discourage illegitimate financial success.

Artificial intelligence may intensify these challenges by making certain forms of deceptive communication more accessible. However, technological accessibility does not inevitably encourage criminal participation. Individuals' decisions remain influenced by their social relationships, perceived opportunities and moral expectations.

From a sociological perspective, therefore, reducing AI-related criminality requires more than restricting technological tools. It also requires addressing the social conditions that encourage offending and the institutional arrangements through which legitimate economic opportunities are created.

Empirical Evidence of Cybercrime and AI-Enabled Criminality in Nigeria

Empirical evidence indicates that cybercrime remains a significant challenge to Nigeria's financial security, although recorded losses have fluctuated. According to Ejalonibu et al. (2026), drawing on Nigeria Inter-Bank Settlement System (NIBSS) data, electronic payment fraud losses declined from ₦52.26 billion in 2024 to ₦25.85 billion in 2025, representing approximately a 51% reduction. The number of reported fraud incidents also decreased to approximately 67,515 in 2025. Despite this improvement, phishing, account compromise, identity theft and social engineering remain important threats to digital financial transactions. These findings suggest that technological improvements in financial security can reduce recorded losses even as criminal techniques continue to evolve. However, the available statistics do not establish the proportion of Nigerian financial fraud specifically facilitated by artificial intelligence.

NILDS+1

At the continental level, INTERPOL (2026) reported that artificial intelligence was associated with approximately 55% of reported cybercrimes across Africa, based on an assessment involving 36 African member countries. The report identified AI-assisted phishing, synthetic identity fraud, deepfake-enabled extortion and automated social engineering as emerging threats. These developments have implications for Nigeria, particularly given the country's exposure to electronic financial fraud and transnational cybercriminal activities. Nevertheless, the continental findings should not be interpreted as Nigeria-specific prevalence estimates. From the perspectives of Social Control Theory and Routine Activity Theory, the evidence highlights the importance of strengthening institutional guardianship, digital literacy, identity verification and cooperation among law enforcement agencies, financial institutions and technology providers.

Artificial Intelligence and Criminal Investigation

Although artificial intelligence can facilitate criminal activities, it also provides opportunities for improving criminal investigation and prevention. AI-assisted analytical systems can support suspicious transaction detection, digital evidence processing and the identification of patterns within large datasets.

Berk (2021) explains that artificial intelligence may improve particular aspects of policing and criminal justice risk assessment. Nevertheless, its application creates challenges concerning prediction accuracy, algorithmic bias, transparency and institutional accountability. These concerns are particularly important in developing institutional environments where limited technological infrastructure and inadequate oversight may influence investigative outcomes.

In Nigeria, the introduction of AI-assisted policing should therefore be accompanied by specialised training, appropriate legal safeguards and transparent mechanisms of accountability. Artificial intelligence should support professional investigation rather than replace human judgement, evidentiary standards or established legal procedures. The effectiveness of technological crime prevention ultimately depends on the institutional conditions under which these systems are developed, implemented and monitored.

Implications for Social Control in Nigeria

Challenges to Formal Social Control

The increasing sophistication of technologically mediated crime presents important challenges for formal social control institutions. Conventional policing arrangements depend on investigative procedures, available evidence and established legal jurisdictions. However, AI-assisted criminality introduces additional complexities involving synthetic identities, manipulated digital information and cross-border criminal networks.

Nigeria's Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, as amended in 2024, provides an important legal framework for addressing cyber-enabled criminal activities. Nevertheless, the existence of legislation does not automatically guarantee effective implementation. Institutional capacity, digital forensic expertise, international cooperation and reliable evidence management remain essential requirements. Consequently, formal social control must increasingly incorporate technological expertise without undermining procedural justice and individual rights.

Challenges to Informal Social Control

Informal social control remains important in regulating criminal behaviour, particularly through families, educational institutions, religious organisations and community relationships. However, evidence concerning the social acceptance of cybercrime among some Nigerian groups raises questions about the effectiveness of these institutions.

Aborisade (2023) demonstrates that parental acceptance of cybercriminal involvement can weaken family-based regulation. Button et al. (2025) similarly identify the importance of cultural expectations and social recognition in explaining participation in cyber-enabled fraud. These findings suggest that technological crime prevention must address the moral and social environments within which criminal behaviour develops. Where financial achievement is valued without adequate consideration of its legitimacy, informal mechanisms of social control may become less effective.

Digital Surveillance, Privacy and Institutional Accountability

The increasing use of artificial intelligence in crime prevention also raises concerns about surveillance, personal privacy and institutional accountability. Automated monitoring may support the identification of suspicious activities, but excessive or poorly regulated surveillance can undermine public confidence in criminal justice institutions.

Gorwa et al. (2020) demonstrate that algorithmic regulation involves important questions concerning institutional power, transparency and accountability. Similarly, Berk (2021) identifies fairness and explainability as central considerations in AI-assisted criminal justice. Nigeria's Data Protection Act, 2023, provides an important framework for safeguarding personal information, while the National Artificial Intelligence Strategy, 2025, emphasises responsible and ethical AI governance. Effective social control therefore requires a balance between public security and the protection of fundamental rights. Technological efficiency should not become a justification for arbitrary surveillance, discriminatory enforcement or unaccountable decision-making.

Towards Integrated Technological and Community-Based Social Control

The preceding analysis suggests that AI-assisted criminality cannot be adequately addressed through law

enforcement or technological surveillance alone. A more comprehensive response requires the integration of technological safeguards, institutional capacity, community participation and preventive education. This article proposes an integrated social control approach based on three interconnected dimensions.

- The first involves technological guardianship, including reliable identity verification, digital forensic capabilities, fraud detection systems and secure financial infrastructure.
- The second involves institutional accountability, encompassing appropriate legislation, transparent investigative procedures, independent oversight and cooperation among regulatory agencies.
- The third involves preventive socialisation, through which families, educational institutions, religious organisations and community structures promote ethical digital behaviour and discourage criminal participation.

The proposed framework contributes to sociological discussions by demonstrating that technological innovation, social relationships and institutional regulation should be examined as interconnected components of contemporary crime prevention.

Cross-Border Cybercrime, Legal Challenges and Institutional Cooperation

The transnational nature of AI-assisted cybercrime presents significant challenges to Nigeria's criminal justice system, particularly in establishing jurisdiction, obtaining electronic evidence and coordinating investigations across national boundaries. Criminal activities involving deepfake impersonation, automated financial fraud and identity theft may involve perpetrators, victims and digital infrastructure located in different countries, thereby complicating prosecution and enforcement. Nigeria's Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, as amended in 2024, provides a legal foundation for addressing cyber-enabled offences, including international cooperation through mutual legal assistance. Similarly, the Evidence Act, 2011, as amended in 2023, provides for the admissibility and authentication of electronic records. Nevertheless, AI-generated and manipulated digital materials introduce additional challenges concerning evidential authenticity, forensic reliability and the preservation of electronic evidence.

Addressing these challenges requires stronger collaboration among the Economic and Financial Crimes Commission (EFCC), Nigeria Police Force (NPF), Federal Ministry of Justice, financial institutions and international security organisations. The African Union Convention on Cyber Security and Personal Data Protection provides an important regional framework for strengthening cybersecurity governance and cooperation, while international cybercrime agreements offer additional opportunities for coordinated investigations and evidence sharing. Effective implementation should prioritise specialised digital forensic training, standardised electronic evidence preservation, timely cross-border information exchange and stronger institutional accountability. These measures should operate within appropriate legal safeguards to protect privacy, due process and fundamental human rights. Strengthening such cooperation would improve Nigeria's capacity to investigate AI-enabled criminal activities while addressing the jurisdictional limitations of conventional law enforcement.

POLICY IMPLICATIONS AND RECOMMENDATIONS

The findings of this study highlight the need for coordinated and technologically responsive policies to address the changing patterns of AI-assisted criminality in Nigeria. Effective crime prevention requires an integrated approach combining legal reforms, institutional capacity building, technological guardianship and community-based social control. Accordingly, the following recommendations are proposed:

1. Strengthening AI-Related Cybercrime Investigation: The Federal Government, through the Economic and Financial Crimes Commission (EFCC), Nigeria Police Force (NPF) and relevant cybersecurity institutions, should establish specialised training programmes in AI-assisted fraud detection, deepfake identification, digital forensics and electronic evidence management. These institutions should develop standard operating procedures for investigating AI-enabled offences, supported by periodic professional training and assessments of investigative capacity.

2. Enhancing Legal and Regulatory Frameworks: The Federal Ministry of Justice and National Assembly should periodically review the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, as amended in 2024, to address emerging challenges involving synthetic identity fraud, deepfake-enabled extortion and AI-generated evidence. Particular attention should be given to evidential authenticity, procedural safeguards, cross-border jurisdiction and the protection of personal data under the Nigeria Data Protection Act, 2023.
3. Promoting Technological Guardianship and Financial Security: The Central Bank of Nigeria (CBN), Nigeria Inter-Bank Settlement System (NIBSS), commercial banks and financial technology companies should strengthen fraud monitoring, identity verification, transaction authentication and suspicious-activity reporting. Regular assessments of these safeguards should be conducted to determine their effectiveness in reducing financial fraud and preventing AI-assisted impersonation.
4. Strengthening Digital Literacy and Community-Based Prevention: The Federal Ministry of Education, universities, civil society organisations and community leaders should integrate AI-related cybersecurity awareness into educational and public enlightenment programmes. Such initiatives should focus on recognising deepfake manipulation, phishing, fraudulent online identities and financial deception. Families, religious institutions and community organisations should also promote ethical digital behaviour and discourage the social acceptance of cybercrime, particularly among young people.
5. Improving Inter-Agency Coordination and International Cooperation: The EFCC, NPF, Federal Ministry of Justice and relevant cybersecurity institutions should establish coordinated mechanisms for cybercrime intelligence sharing, electronic evidence preservation and cross-border investigations. Cooperation with INTERPOL and relevant African regional institutions should be strengthened to facilitate lawful information exchange, mutual legal assistance and effective prosecution of transnational AI-enabled offences.
6. Promoting Data Protection and Institutional Accountability: The Nigeria Data Protection Commission and relevant regulatory institutions should strengthen oversight of AI-assisted surveillance, biometric identification and automated criminal investigation systems. These measures should ensure compliance with the Nigeria Data Protection Act, 2023, while promoting transparency, procedural fairness and protection against discriminatory enforcement.
7. Strengthening Research and Evidence-Based Policy Development: The Federal Government, through relevant research institutions, universities and security agencies, should encourage empirical investigations into the prevalence, methods and socioeconomic consequences of AI-enabled criminality in Nigeria. Standardised reporting mechanisms should distinguish confirmed AI-assisted offences from conventional cybercrime, enabling policymakers to evaluate emerging threats and measure the effectiveness of prevention strategies.

CONCLUSION

This study examined the changing patterns of crime associated with artificial intelligence and their implications for social control in Nigeria. The findings indicate that AI is reshaping existing criminal activities through automated financial fraud, identity impersonation, deepfake-enabled deception, social engineering and transnational cybercrime. Although available Nigerian cybercrime statistics do not adequately distinguish AI-enabled offences from conventional cybercriminal activities, emerging technological capabilities present significant challenges to crime prevention, criminal investigation and institutional accountability. Drawing on Social Control Theory and Routine Activity Theory, the study establishes that AI-assisted criminality cannot be explained by technological advancement alone but must be understood through the interaction of socioeconomic conditions, criminal opportunities, weakened social bonds and inadequate institutional guardianship.

The study concludes that addressing AI-enabled criminality in Nigeria requires an integrated approach combining technological guardianship, effective legislation, specialised law enforcement capacity, digital literacy and community-based crime prevention. Strengthening collaboration among security agencies, financial institutions, regulatory bodies and international organisations is essential for addressing cross-border criminal activities while safeguarding privacy and fundamental human rights. Furthermore, sustained empirical research and improved institutional reporting are necessary to establish the prevalence and characteristics of

AI-assisted offences in Nigeria. Ultimately, effective social control in an increasingly digital society depends on Nigeria's ability to develop preventive, technologically responsive, socially inclusive and institutionally accountable mechanisms of crime prevention.

REFERENCES

1. Aborisade, R. A. (2022). Image-based sexual abuse in a culturally conservative Nigerian society: Female victims' narratives of psychosocial costs. *Sexuality Research and Social Policy, 19*, 220–232. doi:10.1007/s13178-021-00536-3
2. Aborisade, R. A. (2023). Yahoo boys, Yahoo parents? An explorative and qualitative study of parents' disposition towards children's involvement in cybercrimes. *Deviant Behavior, 44*(7), 1102–1120. doi:10.1080/01639625.2022.2144779
3. African Union. (2014). African Union Convention on Cyber Security and Personal Data Protection. https://www.au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection
4. Berk, R. A. (2021). Artificial intelligence, predictive policing, and risk assessment for law enforcement. *Annual Review of Criminology, 4*, 209–237. doi:10.1146/annurev-criminol-051520-012342
5. Button, M., Lazarus, S., Hock, B., Sabia, J. B., Pandey, D. S., & Gilmour, P. (2025). Factors influencing involvement in cyber-frauds in West Africa and the implications for policy. *European Journal on Criminal Policy and Research*. Advance online publication. doi:10.1007/s10610-025-09649-6
6. Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608. doi:10.2307/2094589
7. Costello, B. J., & Laub, J. H. (2020). Social control theory: The legacy of Travis Hirschi's *Causes of Delinquency*. *Annual Review of Criminology, 3*, 21–41. doi:10.1146/annurev-criminol-011419-041527
8. Ejalonibu, G., Obot, E., & Nandi, L. (2026). *Electronic payment fraud trends in Nigeria's banking sector—2025 data, emerging risks, and legislative imperatives*. National Institute for Legislative and Democratic Studies.
9. Federal Ministry of Communications, Innovation and Digital Economy. (2025). *National artificial intelligence strategy*. Federal Republic of Nigeria.
10. Federal Republic of Nigeria. (2015). *Cybercrimes (Prohibition, Prevention, etc.) Act, 2015*.
11. Federal Republic of Nigeria. (2023). Evidence (Amendment) Act, 2023.
12. Federal Republic of Nigeria. (2024). *Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024*.
13. Gorwa, R., Binns, R., & Katzenbach, C. (2020). Algorithmic content moderation: Technical and political challenges in the automation of platform governance. *Big Data & Society, 7*(1). doi:10.1177/2053951719897945
14. Griffith, C. E., Tetzlaff-Bemiller, M., & Hunter, L. Y. (2023). Understanding the cyber-victimization of young people: A test of routine activities theory. *Telematics and Informatics Reports, 9*, Article 100042. doi:10.1016/j.teler.2023.100042
15. Heiding, F., Lermen, S., Kao, A., Verdun, C. M., Schneier, B., & Vishwanath, A. (2026). Evaluating large language models' ability to automate spear phishing. *Expert Systems with Applications, 314*, Article 131546. doi:10.1016/j.eswa.2026.131546
16. Hirschi, T. (1969). *Causes of delinquency*. University of California Press.
17. INTERPOL. (2025). *INTERPOL Africa cyberthreat assessment report 2025*.
18. INTERPOL. (2026). African cyberthreat assessment report 2026. Official report announcement
19. Lazarus, S., Button, M., & Adogame, A. (2022). Advantageous comparison: Using Twitter responses to understand similarities between cybercriminals ("Yahoo Boys") and politicians ("Yahoo men"). *Heliyon, 8*(11), Article e11142. doi:10.1016/j.heliyon.2022.e11142
20. Sandoval, M.-P., de Almeida Vau, M., Solaas, J., & Rodrigues, L. (2024). Threat of deepfakes to the criminal justice system: A systematic review. *Crime Science, 13*, Article 41. doi:10.1186/s40163-024-00239-1
21. Schmitt, M., & Flechais, I. (2024). Digital deception: Generative artificial intelligence in social engineering and phishing. *Artificial Intelligence Review, 57*, Article 324. doi:10.1007/s10462-024-10973-2