Vol. 9, No. 1, June (2026)
JOURNAL OF ENVIRONMENTAL AND TOURISM EDUCATION
ISSN: 2659-0794 (PRINT) ISSN:2659-0808(ONLINE)
Content Available at: **https://jeate.k-injo.com/index.php/Jete**

Globalization and Cyber Security: Implications for Ai-Driven Policing in Nigeria

JOHN FIDELIS INAKU barrjohninaku@gmail.com 0009-0004-9802-3311	Faculty of Law University of Calabar, Calabar, Nigeria
ESSIEN SAVIOUR OKOKON saviouressien83@gmail.com 0009-0006-1184-004X	Department of Criminology and Security Studies University of Calabar, Calabar, Nigeria
FELIX ONAH ODEY **odeyfelixh@gmail.com** **009-0006-3547-6537**	Department of criminology and security studies Alex Ewueme Federal University, Ndufu Alike, Nigeria

Keywords

Correspondence Email:
barrjohninaku@gmail.com

https://doi.org/10.60787/jete.vol9no1.436-445

Abstract

This study examined the implications of globalization and cyber security for AI-driven policing in Nigeria. Using a qualitative documentary research design, the study synthesized evidence from peer-reviewed literature, policy documents, government publications, and reports from relevant national and international institutions. Data were analyzed through thematic content analysis and interpreted within the framework of Systems Theory and Securitization Theory. Findings revealed that globalization has intensified cyber threats, including cyber fraud, identity theft, online financial crimes, cyber extortion, and attacks on critical digital infrastructure. The study further established that artificial intelligence enhances intelligence gathering, predictive policing, digital surveillance, crime detection, and inter-agency information sharing, thereby improving the efficiency of security operations. However, inadequate technological infrastructure, shortage of technical expertise, weak institutional coordination, corruption, poor funding, and concerns over privacy and data protection continue to constrain effective AI-driven policing in Nigeria. The study concludes that while AI offers significant prospects for strengthening cyber security governance, its effectiveness depends on robust institutional reforms, ethical governance frameworks, technological modernization, and sustained investment in digital security infrastructure. The paper recommends enhanced inter-agency collaboration, capacity building, responsible AI governance, and improved investment in cyber security technologies to strengthen national security.

1.0 Introduction

The unprecedented expansion of Information and Communication Technology (ICT) has fundamentally transformed contemporary societies by reshaping communication, commerce, governance, financial transactions, education, and social interaction. Across both developed and developing countries, digital technologies have improved productivity, expanded access to information, and enhanced socioeconomic development. However, these technological advancements have simultaneously created new opportunities for cyber-enabled criminal activities, making cybercrime one of the fastest-growing security threats worldwide (Wall, 2021; Yar, 2022; Interpol, 2023). The increasing dependence of governments, businesses, financial institutions, and individuals on digital technologies has widened the attack surface for cybercriminals, whose operations have become increasingly sophisticated, transnational, and difficult to detect. Globally, cybercrime has evolved beyond conventional hacking into a complex ecosystem involving phishing, ransomware, identity theft, business email compromise, cryptocurrency fraud, malware deployment, online financial scams, cyberstalking, and unauthorized access to digital systems (UNODC, 2023; Europol, 2023). Advances in artificial intelligence, cloud computing, mobile technologies, and encrypted communication have further increased the technical capabilities of cybercriminals while simultaneously complicating cybersecurity governance and digital law enforcement (Interpol, 2023). Consequently, scholars and policymakers increasingly acknowledge that cybercrime constitutes not only a technological challenge but also a socioeconomic, legal, and criminological concern requiring multidisciplinary intervention (Brenner, 2022; Wall, 2021).

Nigeria has experienced rapid digital transformation over the past decade through increased internet penetration, widespread smartphone ownership, expansion of electronic banking, digital commerce, social media utilization, and mobile financial services. According to the Nigerian Communications Commission (2024), internet subscriptions continue to rise annually, while digital payment platforms have significantly expanded financial inclusion. Although these developments have stimulated economic growth and technological innovation, they have equally exposed individuals, businesses, and government institutions to unprecedented cyber threats. Reports by the Economic and Financial Crimes Commission (EFCC, 2023), Nigeria Inter-Bank Settlement System (NIBSS, 2024), and the Nigeria Computer Emergency Response Team (ngCERT, 2024) indicate persistent increases in online financial fraud, phishing attacks, identity theft, ransomware incidents, account compromise, and other forms of cyber-enabled offences. These crimes have resulted in substantial financial losses, erosion of public trust in digital platforms, and increasing pressure on law enforcement agencies to strengthen cybersecurity governance. Central to the growing incidence of cybercrime is the widespread availability and misuse of ICT tools. While personal computers, smartphones, Virtual Private Networks (VPNs), and phishing kits were originally designed to facilitate communication, information sharing, data protection, and legitimate digital interaction, they are increasingly exploited to perpetrate sophisticated cyber offences. Personal computers remain the primary platforms for malware creation, hacking operations, unauthorized system access, and financial fraud. Smartphones have equally expanded opportunities for cybercrime through mobile banking fraud, identity theft, fraudulent social media activities, and malicious applications because of their portability and continuous internet connectivity. VPN technology, though developed to enhance online privacy and secure communication, is frequently misused by cybercriminals to conceal identities, bypass security controls, and evade digital surveillance. Similarly, phishing kits have significantly

lowered the technical barriers to cybercrime by enabling even individuals with limited programming expertise to execute phishing campaigns, credential theft, and online financial scams (Europol, 2023; UNODC, 2023).

The situation has become increasingly evident in Cross River South Senatorial District, where expanding internet access, electronic commerce, digital financial services, and social media participation have transformed patterns of communication and economic activity. While these technologies have enhanced socioeconomic opportunities, they have also increased exposure to cyber-enabled crimes such as online fraud, impersonation, account compromise, phishing attacks, and electronic financial theft. Security agencies continue to express concern over the growing sophistication of cybercriminal operations and the misuse of readily available ICT facilities by offenders. These developments underscore the need to understand how specific ICT tools contribute to cybercriminal activities within the local context. Existing literature has examined cybercrime from legal, technological, cybersecurity, and criminological perspectives, with considerable attention devoted to cybersecurity awareness, digital fraud, cyber victimization, and crime prevention strategies (Wall, 2021; Yar, 2022; Brenner, 2022). However, comparatively limited empirical attention has been given to the relationship between commonly accessible ICT tools—particularly personal computers, smartphones, VPNs, and phishing kits—and cybercriminal activities within Cross River South Senatorial District. This gap is significant because understanding the technological instruments facilitating cybercrime is essential for developing effective cybersecurity policies, strengthening law enforcement capacity, improving public awareness, and promoting the responsible utilization of digital technologies. It is against this backdrop that this study investigates the relationship between ICT tools and cybercriminal activities in Cross River South Senatorial District, Nigeria.

2.0 Statement of the Problem

The rapid expansion of digital technologies has transformed socioeconomic activities in Nigeria by improving communication, financial transactions, electronic commerce, and access to information. However, the same technologies that facilitate development have also become major instruments for cybercriminal activities. Despite increased investments in cybersecurity, public awareness campaigns, and digital crime legislation, cybercrime continues to increase in frequency, sophistication, and financial impact across the country (EFCC, 2023; Interpol, 2023). Reports from national security agencies consistently indicate rising cases of phishing, identity theft, online financial fraud, hacking, and other technology-enabled offences that undermine public confidence in digital systems and threaten national security. Although previous studies have extensively examined cybercrime from legal, technical, and cybersecurity perspectives, relatively few have specifically investigated the contribution of commonly accessible ICT tools including personal computers, smartphones, VPNs, and phishing kits to cybercriminal activities, particularly within Cross River South Senatorial District. This omission limits empirical understanding of the technological mechanisms through which cybercrime is perpetrated and constrains the development of targeted intervention strategies.

The problem is further compounded by increasing internet penetration, widespread smartphone ownership, expanding digital financial services, and limited cybersecurity awareness among users. While these developments have accelerated digital inclusion, they have equally expanded opportunities for cybercriminal exploitation. Law enforcement agencies continue to experience challenges in identifying offenders who exploit anonymity technologies such as VPNs,

while phishing kits and automated cybercrime tools have significantly lowered the technical expertise required to commit digital offences. Without adequate empirical evidence on the relationship between ICT tools and cybercriminal activities within the study area, efforts aimed at strengthening cybersecurity policies, improving digital literacy, enhancing law enforcement strategies, and promoting responsible ICT utilization may remain ineffective. Consequently, this study seeks to examine how selected ICT tools influence cybercriminal activities in Cross River South Senatorial District, Nigeria, with a view to providing evidence-based recommendations for strengthening cybersecurity governance and crime prevention.

3. Literature Review and Theoretical Foundation

3.1 Information Management and Security Governance

Information management has become a critical component of modern security governance because effective security responses depend largely on the timely collection, processing, dissemination, and utilization of intelligence. Contemporary security institutions increasingly rely on integrated information systems to detect threats, coordinate responses, and support strategic decision-making (Boin & Lodge, 2021; UNODC, 2023). Consequently, information management extends beyond data storage to encompass intelligence gathering, communication, surveillance, risk analysis, and inter-agency collaboration.

In Nigeria, information management has assumed greater importance due to the changing character of insecurity. Emerging security threats such as terrorism, banditry, kidnapping, cybercrime, farmer-herder conflicts, and organized criminal networks operate across multiple jurisdictions and often exploit weaknesses in intelligence coordination (International Crisis Group [ICG], 2023). Despite numerous security reforms, intelligence failures, fragmented databases, institutional rivalry, and inadequate information sharing continue to undermine effective security operations (National Bureau of Statistics [NBS], 2024). Studies have consistently shown that countries with integrated security information systems respond more effectively to emerging threats because intelligence is shared promptly among relevant agencies (World Bank, 2023; United Nations Development Programme [UNDP], 2024). Effective information management therefore constitutes an indispensable requirement for proactive security governance and sustainable national development.

3.2 Emerging Security Challenges in Nigeria

Nigeria's security environment has become increasingly complex over the last decade. While conventional crimes remain prevalent, the country now faces multidimensional security threats involving terrorism, insurgency, kidnapping for ransom, cybercrime, violent extremism, communal conflicts, separatist agitations, and transnational organized crime (UNODC, 2023). These challenges have significantly affected governance, investment, agricultural productivity, educational activities, and social cohesion. According to the Armed Conflict Location and Event Data Project (ACLED, 2024), violent incidents continue to spread across several geopolitical zones, overwhelming conventional security responses. Similarly, the International Crisis Group (2023) observed that many of these security threats are sustained by poor intelligence coordination, delayed information flow, and weak institutional collaboration. Cybercrime presents an additional concern as rapid digitalization has created opportunities for financial fraud, identity theft,

ransomware attacks, and online criminal networks. These developments require sophisticated information management systems capable of supporting predictive intelligence, digital surveillance, and evidence-based security planning (Interpol, 2023). The persistence of these threats demonstrates that effective security management increasingly depends on the availability of reliable information, modern technology, and institutional coordination rather than conventional policing alone.

3.3 Information Management as a Tool for Addressing Insecurity

Contemporary literature increasingly recognizes information management as a strategic instrument for preventing and responding to security threats. Modern information systems facilitate intelligence gathering, crime mapping, early warning mechanisms, predictive analysis, and coordinated decision-making, thereby improving operational efficiency among security agencies (Gilson, 2022; World Bank, 2023). Digital technologies, including geographic information systems (GIS), artificial intelligence, biometric databases, integrated communication networks, and big data analytics, have transformed intelligence management across many countries. These technologies enable security agencies to detect emerging threats, monitor criminal activities, and deploy resources more effectively (Interpol, 2023; UNDP, 2024).

However, the effectiveness of information management depends on institutional capacity, technological infrastructure, skilled personnel, and inter-agency cooperation. In Nigeria, inadequate funding, obsolete information systems, corruption, bureaucratic bottlenecks, and fragmented intelligence structures continue to limit the effectiveness of information-driven security governance (ICG, 2023; NBS, 2024). Addressing these challenges requires sustained investment in digital infrastructure, institutional reforms, and capacity building to strengthen intelligence-led security management.

3.4 Theoretical Foundation

This study is anchored on **Systems Theory** and **Securitization Theory**, which collectively provide a comprehensive framework for understanding the relationship between information management and insecurity in Nigeria.

Systems Theory

Systems Theory, developed by Ludwig von Bertalanffy (1968), conceptualizes society as an interconnected system in which the effectiveness of each component depends on its interaction with other parts. Applied to security governance, the theory suggests that intelligence agencies, law enforcement institutions, policymakers, communication systems, and information networks function as interdependent subsystems whose coordination determines overall security performance. The theory explains that weaknesses in any component of the information management system such as delayed intelligence sharing, poor communication, or institutional fragmentation can reduce the effectiveness of national security responses. Consequently, strengthening information management requires improving coordination, integration, and collaboration among all security stakeholders.

Securitization Theory

Securitization Theory, advanced by Barry Buzan, Ole Wæver, and Jaap de Wilde (1998), argues that issues become security concerns when political leaders and institutions successfully

present them as existential threats requiring extraordinary policy responses. The theory emphasizes that security is socially constructed through discourse, institutional action, and public acceptance. Within the Nigerian context, terrorism, kidnapping, banditry, cybercrime, and violent extremism have increasingly been securitized because they threaten national stability and socioeconomic development. Effective securitization, however, depends heavily on accurate intelligence, credible information systems, and timely communication. Without reliable information management, governments may fail to identify threats early, formulate appropriate policies, or coordinate effective responses. Together, Systems Theory and Securitization Theory provide complementary explanations for the study. While Systems Theory highlights the importance of institutional coordination and integrated information systems, Securitization Theory explains how effective information management shapes threat identification, security policymaking, and national responses to emerging security challenges.

4. Methodology

This study adopted a qualitative documentary research design to examine the implications of globalization and cybersecurity for AI-driven policing in Nigeria. The design was appropriate because it enabled a systematic review and critical synthesis of existing scholarly and institutional evidence without generating primary data. Data were obtained exclusively from secondary sources, including peer-reviewed journal articles, books, conference proceedings, government publications, policy documents, and reports from reputable. To ensure currency and relevance, priority was given to publications produced between 2020 and 2025, while seminal studies were consulted to provide conceptual and theoretical grounding. The selection of documentary materials followed purposive sampling based on relevance to the study objectives, credibility of the source, and methodological quality. Data were analyzed using thematic content analysis, through which information was systematically coded, categorized, and synthesized into major themes relating to globalization, cybersecurity threats, AI-driven policing, institutional challenges, and governance issues. This analytical approach facilitated the identification of recurring patterns and generated evidence-based insights into the opportunities and challenges associated with AI-enabled policing in Nigeria.

5. Results and Discussion

The findings presented in this paper are based on the synthesis of contemporary literature, policy documents, and institutional reports on information management and insecurity in Nigeria. The discussion is organized according to the objectives of the study.

The review established that effective information management has become indispensable for addressing Nigeria's evolving security challenges. Contemporary security threats including terrorism, banditry, kidnapping, cybercrime, communal violence, and violent extremism are increasingly sophisticated and transnational, requiring intelligence-driven rather than reactive security responses. Studies indicate that countries with integrated information systems demonstrate greater capacity for threat detection, intelligence coordination, and strategic decision-making than those relying on fragmented information structures (World Bank, 2023; UNDP, 2024). In Nigeria, however, information management remains constrained by weak intelligence coordination, inadequate technological infrastructure, fragmented databases, and institutional rivalry among security agencies. These deficiencies often result in delayed responses, intelligence

failures, duplication of operational efforts, and ineffective security interventions (International Crisis Group, 2023; NBS, 2024). The review therefore suggests that improving national security requires strengthening integrated information management systems capable of supporting timely intelligence gathering, analysis, dissemination, and coordinated action. These findings support **Systems Theory**, which emphasizes that the effectiveness of security governance depends on the functional interaction of interconnected institutions. Weaknesses in information flow or institutional collaboration reduce the overall effectiveness of the security system, regardless of the capacity of individual agencies.

The review further demonstrates that effective information management enhances security governance by facilitating intelligence-led policing, inter-agency collaboration, strategic planning, and evidence-based decision-making. Modern information systems support real-time surveillance, crime mapping, predictive analytics, biometric identification, and early warning mechanisms that improve operational efficiency and proactive responses to security threats (Interpol, 2023; UNODC, 2023). Several studies indicate that countries investing in digital intelligence infrastructure achieve better coordination among security institutions and more effective responses to organized crime and terrorism (Gilson, 2022; World Bank, 2023). In contrast, Nigeria continues to experience institutional fragmentation, incompatible information systems, poor communication networks, and limited interoperability among security agencies. These challenges constrain intelligence sharing and weaken coordinated responses to emerging threats. The findings further reinforce **Securitization Theory**, which argues that effective security governance depends not only on recognizing threats but also on the availability of credible information that enables governments to formulate appropriate policy responses. Reliable intelligence therefore remains central to successful securitization processes.

The review reveals that persistent insecurity has profound implications for Nigeria's socioeconomic development. Widespread insecurity discourages domestic and foreign investment, disrupts agricultural production, increases unemployment, weakens educational systems, and undermines public confidence in government institutions (UNDP, 2024; World Bank, 2023). Businesses increasingly incur higher operational costs due to security expenditures, while communities affected by violent conflicts experience displacement, poverty, and declining access to essential social services. Educational institutions have also been adversely affected through repeated school closures, attacks on educational facilities, and disruptions to academic activities, thereby weakening human capital development. Similarly, insecurity has reduced government revenue through declining economic activities while increasing public expenditure on security operations, humanitarian interventions, and post-conflict reconstruction (NBS, 2024). The findings indicate that insecurity extends beyond public safety to constitute a significant development challenge capable of undermining sustainable national growth. Effective information management should therefore be regarded as an important component of national development planning rather than solely a security concern.

Despite advances in information and communication technologies, several factors continue to limit the effectiveness of information management in Nigeria's security architecture. The review identifies inadequate funding, obsolete technological infrastructure, poor digital integration, weak institutional coordination, corruption, insufficient technical expertise, and inadequate legislative support as major constraints affecting intelligence management (ICG, 2023; Interpol, 2023). Another critical challenge is the absence of fully integrated national information systems capable of facilitating seamless intelligence sharing among security agencies. Bureaucratic procedures and

organizational rivalry frequently discourage collaboration, thereby limiting timely dissemination of intelligence required for effective security operations. The review also identifies increasing cyber threats as an emerging challenge requiring continuous investment in digital security infrastructure, cybersecurity frameworks, and advanced information technologies. Without adequate modernization, security institutions may remain unable to respond effectively to rapidly evolving security threats. Overall, the findings demonstrate that technological investment alone is insufficient. Institutional reforms, professional capacity development, stronger legal frameworks, and improved inter-agency collaboration are equally necessary for strengthening information management and enhancing national security governance.

6. Conclusion and Recommendations

This paper examined the relationship between information management and insecurity in Nigeria and assessed its implications for national development. The review demonstrates that effective information management has become indispensable for contemporary security governance, particularly in addressing multidimensional threats such as terrorism, banditry, kidnapping, cybercrime, violent extremism, and communal conflicts. The findings indicate that integrated information systems strengthen intelligence gathering, facilitate inter-agency collaboration, enhance strategic decision-making, and improve proactive responses to emerging security challenges. Conversely, fragmented intelligence structures, weak institutional coordination, inadequate technological infrastructure, insufficient funding, and poor information-sharing mechanisms continue to undermine national security efforts.

The study further established that persistent insecurity has serious consequences for national development through its adverse effects on economic growth, investment, agricultural productivity, education, social cohesion, and public confidence in state institutions. These findings reinforce the propositions of **Systems Theory**, which emphasizes institutional interdependence in security governance, and **Securitization Theory**, which highlights the centrality of credible information in identifying and responding to security threats. Accordingly, information management should be regarded not merely as an administrative function but as a strategic national security asset essential for sustainable development.

To strengthen information-driven security governance in Nigeria, the study recommends the following:

1. Government should modernize national security information infrastructure by investing in integrated digital intelligence systems, real-time surveillance technologies, secure communication platforms, and interoperable databases to enhance intelligence gathering and information sharing among security agencies.
2. Institutional collaboration should be strengthened through the establishment of coordinated information-sharing frameworks that promote timely intelligence exchange and joint security operations among relevant agencies.
3. Capacity-building programmes should be intensified to improve the digital competencies of security personnel in intelligence analysis, cybersecurity, information management, and emerging security technologies.

4. Government should increase investment in cybersecurity infrastructure and strengthen legal and regulatory frameworks to protect critical national information systems from cyber threats and unauthorized access.
5. Information management should be integrated into national security and development policies by promoting evidence-based planning, continuous intelligence assessment, and strategic monitoring of emerging security threats.
6. Public-private partnerships should be encouraged to facilitate technological innovation, research collaboration, and resource mobilization for improving national information management systems.
7. Future studies should adopt empirical approaches to examine the effectiveness of digital information management systems and intelligence-led security strategies in addressing contemporary security challenges within Nigeria and comparable developing countries.

REFERENCES

McLuhan, M. (1964). *Understanding media: The extensions of man*. McGraw-Hill.

Amnesty International. (2021). *Nigeria: Time to end impunity and torture by police*. Amnesty International Publications.

Giddens, A. (2021). *Runaway world: How globalization is reshaping our lives*. Routledge.

Held, D., & McGrew, A. (2021). *Globalization theory: Approaches and controversies*. Polity Press.

Adebayo, T., & Ojo, S. (2022). *Globalization and cyber fraud networks in Nigeria*. African Journal of Criminology and Security Studies, 8(2), 44–59.

Castells, M. (2022). *The rise of the network society* (3rd ed.). Wiley-Blackwell.

Johnson, P., & Taylor, S. (2022). *Ethical governance and AI policing systems in democratic societies*. Journal of Artificial Intelligence and Society, 14(2), 88–105.

Okeshola, F., & Adeta, A. (2022). *Cyber security threats and digital criminality in Nigeria*. International Journal of Cyber Criminology, 16(2), 133–149.

Russell, S., & Norvig, P. (2022). *Artificial intelligence: A modern approach* (4th ed.). Pearson Education.

Smith, L., & Miller, T. (2022). *AI surveillance systems, human rights, and democratic governance*. International Journal of Human Rights and Technology, 7(4), 92–110.

United Nations. (2022). *Digital globalization and technological transformation report*. United Nations Publications.

Akinwale, O., & Adekunle, F. (2023). *Artificial intelligence and crime prevention in Africa*. International Journal of Security and Intelligence Studies, 12(1), 66–84.

Brown, M., & Davis, R. (2023). *Predictive policing and algorithmic bias in urban security management*. Journal of Digital Policing and Ethics, 5(3), 71–89.

Economic and Financial Crimes Commission (EFCC). (2023). *Annual report on cybercrime and financial fraud in Nigeria*. EFCC Publications.

Europol. (2023). *Artificial intelligence and the future of policing in Europe*. Europol Publications.

Interpol. (2023). *Global cybercrime assessment report*. Interpol Publications.

International Telecommunication Union (ITU). (2023). *Global cyber security index report*. ITU Publications.

United Nations Office on Drugs and Crime (UNODC). (2023). *Cybercrime and international security governance report*. UNODC Publications.

Yusuf, M., & Ibrahim, K. (2023). *Cyber security awareness and digital fraud in Nigeria*. Nigerian Journal of Information and Communication Technology, 11(2), 54–72.

Eze, P., & Nwankwo, J. (2024). *Digital policing innovations and cyber security governance in Nigeria*. Nigerian Journal of Security Administration, 10(1), 101–121.

Nigerian Communications Commission (NCC). (2024). *Annual statistical report on internet usage and digital communication in Nigeria*. NCC Publications.
Nigerian Inter-Bank Settlement System (NIBSS). (2024). *Digital financial fraud report in Nigeria*. NIBSS Publications.
Ogunode, N., & Jegede, A. (2024). *Institutional challenges affecting AI-driven policing in Nigeria*. Journal of African Security and Governance, 9(1), 57–76.