African Journal of Social and Behavioural Sciences (AJSBS)
Volume 16, Number 1 (2026) ISSN: 2141-209X

ARTIFICIAL INTELLIGENCE AND SECURITY IN NIGERIA: A SOCIO-TECHNICAL ANALYSIS OF OPPORTUNITIES AND CONSTRAINTS

Juliet Anulika Ndoh[1]* & Chudi Emmanuel Iwuh[2] & Stanley Chibuzo Ugochukwu[3]

[1]Department of Public Administration, Imo State University, Owerri, Nigeria

[2]Department of Political Science, Imo State University, Owerri, Nigeria

[3]Department of General Studies, Federal College of Land Resources Technology, Owerri, Nigeria

*anuligr8@gmail.com

ABSTRACT: This study critically examines the role of artificial intelligence (AI) in Nigeria's security architecture through a socio-technical lens, analysing the nexus between technological opportunities, institutional constraints, and governance challenges. Rather than providing a broad overview, this research demonstrates that effective AI adoption requires integrating technological systems with strong institutions, ethical frameworks, and human capacity development, rather than relying on technology deployment alone. Using secondary data sources, including peer-reviewed journals (2021–2026), policy documents, government publications, and international reports, the study employs qualitative content analysis to examine Nigeria's current AI-security landscape. Findings reveal that while AI tools such as facial recognition, predictive policing, and cyber defence systems offer significant potential, Nigeria's adoption remains constrained by poor digital infrastructure, inadequate policy frameworks, and weak institutional capacity. The study concludes that successful AI integration requires a holistic approach that combines technological investment with governance reforms, capacity building, and ethical safeguards. The research contributes to existing scholarship by moving beyond techno-optimism to examine how failures of socio-technical systems explain Nigeria's lagging AI adoption in security despite the urgent need.

Keywords: Artificial Intelligence (AI), Security, Socio-Technical Systems, Governance, Nigeria

INTRODUCTION

Artificial Intelligence (AI) has emerged as one of the most transformative technologies of the 21st century, reshaping virtually all aspects of human society, including healthcare, education, commerce, and, importantly, security. However, in developing countries, the application of AI in security remains limited due to inadequate infrastructure, poor governance, and ethical dilemmas (Mhlanga, 2022). Nigeria’s contemporary security landscape is characterised by overlapping crises that go beyond terrorism to include militancy, banditry, kidnapping, herder–farmer clashes, separatist agitations, and police brutality (Iherue, 2021). Similarly, Campbell (2020) opined that Nigeria, being Africa’s most populous country, faces persistent and multifaceted security challenges such as terrorism (Boko Haram and ISWAP), militancy in the Niger Delta, banditry in the North-West, cybercrime, kidnapping for ransom, and communal conflicts. Recent developments, such as the EndSARS protests and escalating banditry, have deepened public anxiety and highlighted the limitations of traditional security approaches. Nigeria's slow adoption of AI in security is not fundamentally a technological problem but a socio-technical one. Sophisticated tools cannot deliver security outcomes without complementary institutional reforms, human capacity, and ethical governance structures. While some observers argue that Nigeria has "teetered on the precipice of failure" and is at risk of becoming a "fully failed state" (Iherue, 2021), this research argues that effectively addressing insecurity requires not merely acquiring AI technologies but integrating them within functional institutions, skilled personnel, and transparent governance frameworks.

These threats undermine peace, disrupt economic activities, and erode public trust in the state’s capacity to provide security. In this context, AI offers opportunities to enhance Nigeria’s intelligence-gathering, surveillance, and counterterrorism capabilities. For example, predictive policing algorithms and biometric surveillance could strengthen law enforcement's ability to prevent attacks and identify criminal networks before they strike (UNESCO, 2021).

Despite these prospects, Nigeria’s adoption of AI in the security sector has been slow and fragmented. The challenges include inadequate technological infrastructure, insufficient funding, limited expertise among security personnel, and weak policy frameworks to guide AI integration (Adeleke, 2021). Moreover, ethical concerns regarding privacy, data protection, and potential abuse of AI surveillance technologies remain unresolved, raising questions about the balance between security and civil liberties. Against this background, this study seeks to explore the intersection of AI and security in Nigeria.

Statement of the Problem

Security remains one of the most pressing challenges confronting Nigeria in the 21st century. The country grapples with terrorism, insurgency, banditry, kidnapping, cybercrime, and communal violence, all of which have undermined national stability, human security, and economic growth (Campbell, 2020). Despite huge investments in traditional security measures such as military operations, intelligence services, and policing, the state has struggled to contain these threats effectively. Egbert & Heimstädt (2024) document that algorithmic crime prevention in developed contexts achieves a 60-70% reduction in police workload through automated data processing, but warn that effectiveness depends entirely on data quality and institutional readiness, neither of which Nigeria currently possesses.

However, the adoption of AI in Nigeria’s security architecture faces multiple challenges, including weak technological infrastructure, poor funding, inadequate technical expertise, and insufficient policy frameworks (Adeleke, 2021).

While developed countries are making significant strides in deploying AI to counter terrorism and enhance national security, developing nations like Nigeria remain marginal players in the global AI-security landscape (Mhlanga, 2022). This technological gap not only limits Nigeria’s ability to secure its citizens but also exposes the country to external cyber vulnerabilities and risks of technological dependency.

The central problem, therefore, is the disconnect between Nigeria's urgent security needs and its slow adoption of AI technologies. Without deliberate efforts to bridge this gap, Nigeria risks continued insecurity, economic stagnation, and weakened state legitimacy. This study critically examines the role of AI in addressing Nigeria's security challenges, interrogating both the opportunities and constraints of its application within the Nigerian context.

Objectives of the Study

1. To examine the role of AI in enhancing security in Nigeria.
2. To analyze the challenges hindering the effective adoption of AI for security in Nigeria.
3. To propose policy recommendations for improving AI integration into Nigeria's security framework.

Research Questions

1. What are the roles AI can play in enhancing security in Nigeria?
2. What challenges hinder the adoption of AI in Nigeria's security system?
3. What strategies can improve AI integration into Nigeria's security architecture?

Theoretical Framework

This study is anchored on Agenda Setting and Socio-Technical Systems theories, which explain the nexus between technology, security, and governance in developing nations. The major theory would be socio-technical systems, as it explains the conditions under which AI can effectively address security challenges in Nigeria.

Agenda Setting Theory

The term agenda setting was coined by Maxwell McCombs and Donald L. Shaw in 1972 and first published in Public Opinion Quarterly (McQuail & Deuze, 2020). The theory describes the media as instruments used to influence public opinion by emphasising an issue and, through such emphasis, prompting the public to consider it important. The media do this by frequently reporting certain issues and/or by giving them prominence. This implies that the more frequently and prominently a news item is promoted in the media, the more important it becomes to the audience. In other words, the news media lead the public on issues. Hence, as the media emphasize on the need to fight against insurgency and expose the heinous crimes insurgents commit, the people take them to be serious issues. Also, the more seriously the government and those affected by the insurgents' activities take it.

Moreover, since the activities of Boko Haram and herdsmen in Nigeria affect the people negatively, the media should expose the harm done to innocent Nigerians by these groups. The theory was also considered suitable for this study because the media has an influence on the public, but can create mass awareness on the important issues concerning insurgency and how AI can be used to stop the insurgents from winning the war.

Basic Assumptions of Agenda-Setting Theory

In its most basic sense, agenda setting is the creation of public awareness and concern of salient issues by the news media (Agenda Setting Theory, 2012). The two most basic assumptions of agenda setting are: (1) the press and the media do not reflect reality; they filter and shape it; (2) media concentration on a few issues and subjects leads the public to perceive those issues as more important than other issues (Agenda Setting Theory, 2012). The time frame for this is one of the most critical aspects of the agenda-setting role in mass communications.

Agenda setting occurs through a cognitive process known as “accessibility,” whereby the more frequently and prominently the news media covers an issue, the more accessible it becomes in the audience’s memory (Iyengar & Kinder, 1987). Basically, when surveyed about what they feel are the most important problems the country faces, respondents reply with issues that the media focuses on the most. For example, when FOX News issued a poll regarding President Obama’s birth certificate, 37 percent of Republican respondents said they believe that Obama was not a natural born citizen compared to just 12 percent of Democrats (Blanton, 2011). The agenda-setting theory suggests that this is the result of repeated coverage by FOX News of the birth certificate issue, an issue that was not covered as much by other networks.

Socio-Technical Systems Theory (STS)

Socio-Technical Systems Theory (STS), first developed by Eric Trist and Fred Emery in the 1950s at the Tavistock Institute in London, provides an analytical framework for understanding how social systems (people, culture, and institutions) and technical systems (machines, tools, and technology) must work together harmoniously for organizational and societal effectiveness. Morgan (1997) later expanded on this by emphasizing that organizations are not merely technical structures but living systems in which technology interacts with human actors, governance mechanisms, and wider environmental contexts. In essence, STS posits that technology alone cannot bring about transformation unless it is integrated with supportive human, cultural, and institutional systems.

Applied to the study of Artificial inteligence (AI) and Security in Nigeria, STS provides important insights. While AI technologies such as predictive policing, biometric systems, drones, and cyber defense tools have the potential to significantly strengthen Nigeria’s security framework, their effectiveness depends heavily on the broader socio-political and institutional environment in which they are deployed. For instance, a predictive policing system may generate accurate data on crime-prone areas, but if the Nigerian police force lacks professionalism, adequate training, or the resources to act on such intelligence, the system becomes ineffective. This reflects the central argument of STS that technical systems must be complemented by capable human and social systems.

Recent scholarship on AI implementation in developing countries emphasizes the socio-technical gap increasingly prevalent in nations attempting rapid technology adoption (Mienye et al., 2024). Mienye et al. (2024) identify that inadequate digital infrastructure, limited technical expertise, data availability challenges, and governance gaps create a "socio-technical gap" in African countries where technology exists but enabling systems do not. Bridging the AI divide requires comprehensive approaches addressing infrastructure, capability, and equity simultaneously, not technological deployment alone (World Bank, 2025). Nigeria's institutional weaknesses, including corruption, poor policy implementation, and weak rule of law (Aghedo & Eke, 2013), create risks that AI-based surveillance tools could be misused for political repression or human rights abuses without robust institutional checks and ethical frameworks.

Furthermore, the theory also highlights the importance of capacity building and human capital. AI requires skilled experts in data science, cybersecurity, machine learning, and robotics. In Nigeria, however, there is a shortage of such technical expertise due to brain drain and inadequate investment in education and research (Ndukwe, 2020). This shortage creates a "socio-technical gap," where advanced tools exist but the human systems needed to operate and maintain them are weak. Bridging this gap requires significant investments in education, training, and collaboration with global AI institutions to build local capacity.

Finally, STS emphasizes the role of cultural and social acceptance of technology. In Nigeria, many communities remain sceptical of advanced surveillance and digital monitoring due to fears of privacy invasion, government overreach, and mistrust of institutions. For AI-based security systems to succeed, there must be societal buy-in, transparency in data usage, and public education to ensure citizens understand how AI serves their security needs without undermining their freedoms.

The Socio-Technical Systems Theory underscores that the adoption of AI in Nigeria's security sector cannot be viewed solely through a technological lens. Success depends on how well AI tools are integrated into the broader socio-political context, supported by strong institutions, skilled human capital, ethical oversight, and societal acceptance. Without this integration, Nigeria risks falling into a trap where sophisticated AI tools are acquired but remain underutilized or misused, thereby undermining both security and governance outcomes.

Justification and Application of Theories

The two theories provide a comprehensive framework for this research. Agenda Setting Theory explains how insecurity becomes a national priority and how media framing drives public and political demand for AI, Socio-Technical Systems Theory explains the conditions under which AI can actually be effective in addressing security challenges in Nigeria. The theories complement each other by addressing both the perceptual (public awareness and prioritization) and practical (integration of technology with social systems) dimensions of AI adoption in the Nigerian security sector.

The two theories explain why AI-based security tools may not yield results if institutions are corrupt or unprofessional. Highlights the "socio-technical gap" in Nigeria, where technology exists, but trained human expertise, accountability, and cultural acceptance are weak. The theories justify the need for a holistic approach, where AI adoption is accompanied by capacity building, institutional reform, and public sensitization and also helps assess how Nigeria can avoid misuse of AI tools (e.g., surveillance for political repression) by embedding them within ethical and transparent governance frameworks.

LITERATURE REVIEW

Artificial Intelligence: Definitions, Applications, and Emerging Debates

Artificial inteligence (AI) refers to computational techniques especially machine learning and data-driven models that enable systems to perform tasks requiring human-like inference, pattern recognition, and decision support; contemporary relevance is driven by advances in machine learning, big data analytics, and deep learning, which have expanded AI's practical use across sectors (IBM, 2023). While "AI as efficiency" remains a dominant narrative emphasizing automation, faster decision-making, and extraction of operational insight from large datasets (Davenport & Ronanki, 2018), this view increasingly competes with "AI as uneven capability," which stresses that the benefits of AI concentrate in settings with data, infrastructure, and governance capacity leaving many developing contexts as users of imported systems rather than co-producers of innovation (World Economic Forum, 2025).

In security, proponents frame AI as a force-multiplier for surveillance, border management, counterterrorism, and cyber defense through predictive analytics, biometric recognition, and automated monitoring (Brundage et al., 2018; Gonzalez & Smith, 2020). However, a persistent counter-position argues that security gains are contingent rather than automatic: AI systems can reproduce bias, intensify surveillance, and enable rights violations when deployed without strong safeguards, oversight, and accountability mechanisms (Bryson & Winfield, 2017). Recent governance-oriented scholarship reinforces this shift by emphasizing that global policy debates are moving away from purely technical discussions toward multidimensional governance covering ethical norms, data rights, auditability, and cross-border regulatory coordination because security-focused AI often implicates sensitive personal data and coercive state power (IEEE, 2025).

Cybersecurity In Developing Nations: Africa and Nigeria

For developing countries, the cybersecurity literature illustrates a persistent "capability–governance gap" (Chaudhuri, 2020). On one hand, the accelerating digitization of finance and public services expands the attack surface and increases the urgency of AI-enabled defenses, since AI can support anomaly detection, fraud monitoring, and faster incident triage at scale (Ayoade, 2021). On the other hand, scholars argue that models and maturity frameworks designed for high-capacity environments do not transfer cleanly into resource-constrained settings, where infrastructural constraints, skills shortages, and institutional fragmentation limit both deployment and sustained maintenance (Gonzalez & Vasquez, 2024). This tension is sharpened by evidence that AI is also being leveraged by adversaries like automating phishing, enhancing social engineering, and evolving malware tactics meaning that weak governance and capacity can leave developing systems exposed on both the defensive and offensive sides of AI adoption (Mohammed & Thomas, 2024; Deloitte Nigeria, 2025).

Predictive Policing in Developing Contexts

Debates around predictive policing similarly reflect a split between operational promise and socio-institutional risk (Perry et al., 2013). Technical studies and operational accounts emphasize that predictive tools can improve resource allocation and reduce workloads through automated processing of incident records and hotspot forecasting (Egbert & Heimstädt, 2024). Yet comparative research also warns that these benefits depend on data quality, institutional readiness, and stakeholder collaboration, because poor data can produce misleading predictions while opaque models can undermine legitimacy and accountability (Rajesh & Patel, 2024). In developing contexts, these concerns are amplified by uneven record-keeping, limited transparency, and historically low trust in policing institutions, making fairness, explainability, and oversight central, not optional, design requirements for predictive security systems (Akinlabi & Okafor, 2024; Eze, Ogbuabor, & Ugwoke, 2021).

AI Governance in Africa

Within Africa, the emerging AI governance literature emphasizes that adoption is shaped by regulatory maturity, data protection, accountability, and the geopolitical implications of imported AI (Musoni, 2024). Policy analyses highlight persistent gaps, including uneven data protection coverage, limited institutional capacity for regulators, and weak accountability frameworks for external AI vendors and cross-border data flows (Musoni, 2024). At the same time, scholarship underscores new regional priorities: harmonizing standards, strengthening AI safety and reliability, promoting sovereign capability (to reduce dependency), and building innovation-enabling environments that still protect rights and public interests (Mushemeza & Zille, 2025). Related AI safety analyses further argue that concrete institutional activity on AI safety remains limited in many African states, implying that risk management lags behind adoption pressures (Sarfo et al., 2025).

Artificial Intelligence and Security in Nigeria

Against this backdrop, Nigeria's AI–security literature is increasingly framed as a socio-technical question rather than a purely technical one (Adebayo & Aluko, 2022). Nigeria's security challenges, such as terrorism, banditry, kidnapping, cybercrime, and communal conflicts, create a strong demand for tools that can expand surveillance reach, speed up intelligence analysis, and strengthen cyber defences (Omotayo, 2021; Ayoade, 2021). Yet the literature consistently indicates that AI outcomes in security depend on enabling conditions: reliable infrastructure, skilled personnel, digitized and interoperable data systems, and legal/ethical governance that constrains misuse while enabling legitimate security objectives (Adeleke, 2021; Ndukwe, 2020). Therefore, the most analytically useful position is not whether AI "works," but under what institutional and governance conditions AI can produce security benefits in Nigeria without deepening rights risks, surveillance abuse, or technology dependency (Mhlanga, 2022).

Gap in Literature

Existing scholarship on AI and security has largely focused on developed nations with advanced infrastructure, strong policy frameworks, and significant investments. Research on developing nations, particularly Africa, remains limited and often generalised without a country-specific focus (Adeleke, 2021). A comprehensive policy framework analysis by UNCTAD (2025) demonstrates this disparity starkly: at the end of 2023, approximately two-thirds (66%) of developed countries had established national AI strategies, but only 6 of 89 Least Developed Countries had done so (UNCTAD, 2025). Nigeria, despite facing acute security crises that justify urgent AI adoption, only recently released a comprehensive National AI Strategy in May 2025 (NCAIR & NITDA, 2025), highlighting how policy lag undermines practical deployment.

In the Nigerian context specifically, most studies examine traditional security challenges such as terrorism, militancy, and cybercrime (Omotayo, 2021; Ayoade, 2021), with limited emphasis on how emerging technologies reshape security responses. Where AI is mentioned, discussions remain largely theoretical rather than empirical, highlighting potentials without assessing real-world applications, implementation barriers, or the socio-technical conditions necessary for effective adoption (Ndukwe, 2020; Adeleke, 2021). This gap underscores the need for a critical, country-specific appraisal of AI and security in Nigeria, situating the discussion within global technological landscapes while addressing Nigeria-specific institutional realities, governance frameworks, and capacity constraints.

METHODOLOGY

This study adopts a qualitative methodological approach anchored on secondary data to explore the nexus between artificial intelligence (AI) and security in developing nations with a specific focus on Nigeria. The choice of method is driven by the need to understand existing scholarship, examine national policy directions, and analyse institutional frameworks, all of which provide insight into the country's readiness and challenges in integrating AI into security operations. By drawing from books, peer-reviewed journals, policy documents, government publications, security strategy papers, and international reports, the study is able to contextualize Nigeria's current AI landscape within broader global and African security trajectories. Special emphasis is also placed on analysing the National Defence Policy (NDP) of Nigeria, which outlines national defence priorities, modernization strategies, and the increasing need for technological adaptation against emerging security threats.

Research Design

The research adopted an explanatory and descriptive design. This design is appropriate because the study seeks to clarify how AI technologies influence security processes, responses, and policy development in Nigeria. Through explanation, the study investigates why AI has become central to national security debates, particularly in addressing issues such as terrorism, cybercrime, border insecurity, and intelligence gathering. The descriptive component of the research allows for documentation and interpretation of existing patterns, implementation processes, and institutional developments shaping AI usage in Nigeria's security sector. As such, the design enables a systematic review of how defence and security agencies conceptualize technological integration, especially in alignment with provisions in the National Defence Policy of Nigeria.

Data Collection Method

Data were obtained exclusively from secondary sources using a structured documentary review. Source selection prioritised peer-reviewed journal articles, academic books, government policy documents, international organisation reports, and technology media published between 2021 and 2026 to ensure currency given rapid AI and security policy developments. Geographic and thematic focus favoured sources addressing Nigeria, Africa, or developing nations; sources addressing AI governance, security implications, implementation challenges, and institutional capacity. Special emphasis was placed on analyzing Nigeria's National AI Strategy (May 2025), National Defence Policy, National Cybersecurity Policy and Strategy (2021), and the proposed Digital Economy and E-Governance Bill (2025).

Data Analysis Method

Collected data were analysed using qualitative content analysis through three iterative phases. In the first phase, documents were coded thematically, identifying recurring patterns across AI-driven surveillance, cybersecurity threats, governance frameworks, capacity constraints, implementation barriers, and ethical concerns. In the second phase, Nigeria's AI–security environment was compared with experiences in other developing nations (Kenya, South Africa, Rwanda, India) to identify Nigeria-specific gaps and transferable lessons. In the third phase, insights were synthesised to construct a holistic understanding of opportunities and constraints shaping AI–security dynamics. Conclusions were grounded in evidence from policy documents and peer-reviewed research rather than inference, ensuring analytical rigour and transparency.

FINDINGS AND ANALYSIS

The Role of AI in Enhancing Security in Nigeria

1. AI in Crime Prevention and Predictive Policing

One of the most significant contributions of AI to security in Nigeria is its application in crime prevention and predictive policing. Predictive policing employs algorithms and machine learning models to analyse historical crime data and identify patterns that can forecast potential criminal activities. According to Perry et al. (2013), predictive policing enables law enforcement agencies to anticipate crimes before they occur by identifying "hotspots" and deploying resources accordingly. In contexts like Nigeria, where the police force is often overstretched and underfunded, such technologies could enhance efficiency. Akinlabi & Okafor (2024) conducted qualitative study of predictive policing implementation in Lagos State, examining effectiveness in crime prevention and resource allocation. Findings demonstrate: (1) AI-assisted CCTV networks reduced average police response times from 47 minutes to 13 minutes in monitored high-crime zones; (2) Predictive algorithms improved patrol resource allocation, reducing overtime expenses by 28%; (3) However, effectiveness depended critically on reliable crime data; fragmented record-keeping in Lagos currently undermines optimization potential.

Also, Lagos, Abuja, and Port Harcourt experience recurrent challenges such as armed robbery, kidnapping, and cult-related violence. By analysing patterns of past crimes, AI systems could guide the Nigerian Police Force to concentrate their patrols in areas with high probabilities of attacks, thereby reducing response time and preventing crimes (Eze et al., 2021). This approach can also help to forecast kidnapping hotspots in states like Kaduna and Zamfara, where abductions have become rampant, thus enabling security operatives to intervene before incidents escalate. However, the effectiveness of predictive policing in Nigeria depends heavily on the availability of reliable and comprehensive crime data, which is often fragmented due to poor record-keeping and weak institutional frameworks.

2. AI-Powered Surveillance and Intelligence Gathering

Another critical role of AI is in strengthening surveillance and intelligence gathering. Surveillance systems enhanced with AI can process vast streams of video data, identify unusual activities, and recognize faces in real time (Zeng et al., 2017). In developing nations where manual surveillance is limited by lack of personnel, AI-powered tools such as drones, facial recognition, and biometric systems provide additional layers of intelligence support.

In Nigeria, AI-powered drones can be deployed in remote forests in the North-East and North-West regions, which serve as hideouts for Boko Haram insurgents and armed bandits. Similarly, facial recognition technologies can be installed at airports, border checkpoints, and urban centres to identify suspects or wanted criminals, thereby enhancing counterterrorism efforts. Nonetheless, the use of such technologies also raises ethical concerns about privacy and the potential for misuse by state actors in repressing political dissent (Ajibade, 2022).

3. Strengthening Cybersecurity

Cybersecurity has emerged as one of the fastest-growing security concerns in developing nations due to increased digitization. Mohammed et al. (2024) conducted systematic review of AI applications in cybersecurity, identifying key techniques: (1) intrusion detection systems using neural networks (achieving 93-98% accuracy), (2) malware classification via deep learning, (3) federated learning for privacy-preserving threat detection, (4) DDoS mitigation. For Nigeria, these applications could strengthen banking sector, electoral systems, and critical infrastructure.

Nigeria, identified as a cyber-enabled financial fraud epicentre in Africa, can benefit significantly from AI-powered systems. Nigerian banks and fintech institutions already employ AI-based fraud detection tools identifying irregular transactions and blocking fraudulent activities in real time (Okon & Effiong, 2020). However, cybersecurity remains constrained by poor infrastructure, shortage of skilled professionals, and weak legal frameworks limiting AI integration effectiveness.

4. Counterterrorism and Extremism Monitoring

Terrorism and violent extremism remain some of the most pressing security challenges in Nigeria, with groups such as Boko Haram and the Islamic State West Africa Province (ISWAP) destabilizing the North-East for over a decade. AI offers valuable tools for counterterrorism, particularly through Natural Language Processing (NLP), which can analyse online communications, detect extremist propaganda, and monitor radicalization patterns. According to Binns (2018), NLP technologies can identify hate speech, extremist narratives, and recruitment content across digital platforms.

AI-based monitoring systems can detect such content, trace recruiters, and alert authorities to prevent radicalization among vulnerable youths. Furthermore, AI can be applied to map terrorist communication networks and financial flows, thereby providing intelligence agencies with actionable insights to disrupt planned attacks. Nevertheless, the deployment of AI in this domain must be balanced with respect for freedom of expression and human rights, as excessive monitoring could lead to censorship and abuse by state authorities.

5. Enhancing Border and Maritime Security

Developing nations often struggle with porous borders and weak maritime controls, making them vulnerable to smuggling, human trafficking, and transnational organized crime. AI technologies, including automated surveillance systems, unmanned aerial vehicles, and motion detection sensors, can play a central role in strengthening border and maritime security (Chaudhuri, 2020).

For Nigeria, securing its borders is critical given the inflow of small arms and light weapons that fuel internal conflicts. AI-powered scanners at border posts can detect contraband hidden in vehicles, while drones can monitor illegal crossings across vast stretches of ungoverned terrain. In addition, Nigeria faces persistent maritime insecurity in the Gulf of Guinea, including piracy, illegal fishing, and oil theft. AI-enabled maritime monitoring systems could help the Nigerian Navy track pirate vessels and suspicious oil tankers in real time, thereby safeguarding the nation’s economic lifeline from the oil sector. The challenge, however, lies in the high cost of such technologies and Nigeria’s reliance on foreign suppliers, which raises concerns of technological dependency.

6. Supporting Emergency Response and Conflict Management

Finally, AI plays an important role in conflict prevention and disaster response, especially in fragile states prone to communal violence and humanitarian crises. AI systems can process environmental, economic, and demographic data to predict conflicts and provide early warning signals (UNESCO, 2021).

Recurrent farmer–herder conflicts have caused widespread loss of lives and displacement. Additionally, AI-powered disaster response tools, such as satellite mapping and automated rescue drones, could assist in locating survivors during natural disasters or terror attacks. However, Nigeria’s weak integration of technology into its disaster management institutions limits the practical application of such tools.

Artificial intelligence holds immense potential in enhancing security in developing nations, particularly Nigeria, by enabling predictive policing, surveillance, cybersecurity, counterterrorism, border protection, and conflict management. These applications could significantly improve Nigeria’s capacity to address insecurity challenges that have hampered its socio-economic development for decades. However, the successful adoption of AI in security requires deliberate investment in digital infrastructure, skilled human capital, ethical regulations, and strong governance frameworks. Without addressing these structural barriers, AI could become a double-edged sword, reinforcing authoritarianism and dependence on foreign technologies rather than fostering sustainable peace and security.

Challenges Hindering the Adoption of AI in Nigeria's Security System

Although Artificial Intelligence (AI) holds great promise for transforming security management in Nigeria, several obstacles hinder its effective adoption. These challenges are rooted in technological, financial, institutional, and socio-political factors. Unless they are addressed, Nigeria may remain dependent on outdated security frameworks while other nations harness AI for advanced security operations.

1. Inadequate Technological Infrastructure: The deployment of AI requires a robust technological ecosystem, including reliable electricity supply, broadband internet, modern data centres, and smart devices. However, Nigeria faces persistent infrastructural deficits. According to Ndukwe (2021), Nigeria's power sector crisis continues to undermine the smooth functioning of digital systems, while internet penetration remains uneven, especially in rural and conflict-affected areas. Without stable infrastructure, AI-powered surveillance systems, drones, or predictive policing tools cannot operate effectively.
2. Limited Funding and Resource Allocation: AI technologies are capital-intensive, requiring significant investments in hardware, software, and research. Nigeria's security sector already consumes a large share of the national budget, but most of it is allocated to personnel and traditional military equipment rather than emerging technologies (Okon & Effiong, 2020). The limited prioritization of research and development leaves security agencies dependent on foreign imports, which are often costly and unsustainable. Furthermore, Nigeria's economic challenges, compounded by fluctuating oil revenues, restrict the funds available for AI adoption.
3. Shortage of Skilled Professionals and Brain Drain: The application of AI in security relies on experts in machine learning, data science, and cybersecurity. However, Nigeria faces a shortage of such professionals due to weak educational and research capacity in advanced technology fields. According to Adebayo and Aluko (2022), many Nigerian AI experts migrate abroad in search of better opportunities, contributing to brain drain. As a result, security agencies often lack the human capital required to develop, deploy, and maintain AI systems locally.
4. Data Scarcity and Poor Digitization: AI systems thrive on large volumes of high-quality data for effective learning and decision-making. In Nigeria, access to reliable crime data is constrained by poor record-keeping, fragmented databases, and limited digitization across government agencies (Eze, Ogbuabor, & Ugwoke, 2021). This makes it difficult to build predictive policing tools or counterterrorism algorithms. Moreover, sensitive national data is often stored manually, making it vulnerable to loss, manipulation, or corruption. Without a culture of data-driven governance, AI adoption in security becomes impractical.
5. Cybersecurity Risks and Technological Dependence: Ironically, while AI can strengthen cybersecurity, its adoption also exposes Nigeria to new vulnerabilities. Dependence on foreign technologies, especially from powerful states or multinational corporations, raises concerns of "digital colonialism," where sensitive national security data may be exploited (Chaudhuri, 2020). Imported AI surveillance tools could contain hidden backdoors, creating risks of espionage. Nigeria's weak cyber defense infrastructure makes the country particularly vulnerable to such risks.
6. Political and Ethical Concerns: The use of AI in security also raises ethical and political challenges. Authoritarian tendencies within Nigeria's political system create the risk of misuse

of AI tools for mass surveillance, political repression, or violation of human rights. Ajibade (2022) notes that surveillance technologies in Africa are sometimes deployed to monitor political opposition and civil society rather than for public safety. Without strong legal and institutional safeguards, AI adoption in Nigeria may entrench state control rather than improve citizen security.

The challenges hindering the adoption of AI in Nigeria's security system are multifaceted, ranging from inadequate infrastructure and limited funding to cybersecurity risk and political misuse. While AI offers powerful solutions for combating terrorism, cybercrime, and communal violence, Nigeria's ability to benefit from it depends on addressing these systemic barriers. A strategic roadmap involving investment in infrastructure, human capital development, ethical governance, and regional collaboration will be essential for AI to fulfil its potential in strengthening Nigeria's security architecture.

Strategies to Enhance AI Integration into Nigeria's Security Architecture

To overcome the barriers hindering the adoption of Artificial Intelligence (AI) in Nigeria's security system, deliberate and well-coordinated strategies are required. These strategies must address infrastructural gaps, human capacity, regulatory frameworks, and governance challenges while ensuring ethical application. The following approaches are central to enhancing AI integration into Nigeria's security architecture.

1. Strengthening Technological Infrastructure

AI applications require stable electricity, fast internet, cloud computing facilities, and data centres. Nigeria must prioritize investments in digital infrastructure to support AI-driven security solutions. According to Ndukwe (2021), without reliable infrastructure, AI-enabled surveillance systems, drones, and predictive policing tools cannot function effectively. The Nigerian government, in collaboration with private investors and international development partners, should accelerate broadband penetration and establish regional innovation hubs to facilitate AI adoption in security.

2. Increased Funding and Resource Allocation

Adequate financing is essential for building AI systems tailored to Nigeria's security needs. Okon and Effiong (2020) argue that budgetary allocation to research and development in security technology remains low compared to defense spending on conventional arms. Redirecting part of Nigeria's security budget toward AI research, acquisition of smart technologies, and public-private partnerships will boost innovation. Foreign partnerships should also be leveraged to fund pilot projects in AI-based border control, cyber defense, and counterterrorism.

3. Developing Human Capital and Retaining Talent

AI integration cannot succeed without a pool of skilled professionals. Nigeria must invest in training programs in machine learning, data science, robotics, and cybersecurity through universities, military academies, and specialized institutions. Adebayo and Aluko (2022) emphasize that brain drain remains a major obstacle; therefore, policies should incentivize Nigerian experts abroad to contribute through mentorship, remote collaborations, or return programs. Scholarships, innovation grants, and hackathons could further attract young innovators to AI security research.

4. Enhancing Data Collection and Digitization

Effective AI deployment depends on access to accurate and comprehensive datasets. Nigeria should digitize crime records, border data, and intelligence reports into centralized databases. As noted by Eze, Ogbuabor, and Ugwoke (2021), fragmented record-keeping undermines predictive security tools. Establishing integrated databases across police, immigration, and intelligence agencies, while ensuring strict privacy protection, will provide the datasets required for machine learning models to identify crime trends and anticipate threats.

5. Building Cybersecurity and Reducing Technological Dependence

Since AI systems are vulnerable to hacking and espionage, Nigeria must simultaneously strengthen cybersecurity. Chaudhuri (2020) highlights that developing nations risk digital colonialism if they over-depend on foreign technologies. Nigeria should adopt a dual strategy: building indigenous AI solutions while diversifying international partnerships to reduce dependency. Establishing strong cyber defense units within security agencies will safeguard AI systems against malicious attacks. For AI to become a transformative force in Nigeria's security architecture, efforts must move beyond rhetoric toward concrete action. By investing in infrastructure, funding innovation, developing human capital, strengthening legal frameworks, and fostering public trust, Nigeria can harness AI to address its security challenges. A coordinated approach that integrates technology with human expertise and ethical governance will ensure that AI serves as a tool for peace, stability, and sustainable national development.

DISCUSSION OF FINDINGS

The findings of the study revealed three interrelated dimensions: the role of AI in enhancing security, the challenges hindering its adoption, and the strategies required for effective integration.

i. The findings indicate that AI holds transformative potential in addressing Nigeria's persistent security challenges. AI can improve crime prediction and prevention through data-driven models capable of analysing patterns in criminal behaviour. Tools such as surveillance drones, biometric systems, and predictive policing technologies enable more proactive security responses. AI also strengthens border management by deploying intelligent monitoring systems that detect illegal migration, smuggling, and insurgent movements across porous borders.

ii. Despite its potential, AI adoption in Nigeria faces systemic obstacles. The most significant challenge is the lack of digital infrastructure, including unreliable electricity, poor broadband penetration, and inadequate data storage facilities. Insufficient funding and overdependence on foreign technologies also limit innovation. Human capital shortages and brain drain further weaken Nigeria's capacity to build and sustain AI-driven solutions.

These findings suggest that Nigeria's security architecture is not yet structurally prepared for large-scale AI integration.

iii. To overcome these barriers, several strategies are necessary. First, strengthening infrastructure such as reliable power supply, internet connectivity, and data centers is critical for AI deployment. Increased funding, both from government and private sector partnerships, is required to support AI-driven innovation in security. Building human capacity through specialized training and retention incentives can counteract brain drain. Finally, public sensitization and regional cooperation with bodies such as ECOWAS and the African Union are essential to foster trust and share best practices.

Overall, the findings highlight a paradox: while AI presents an unprecedented opportunity to transform Nigeria's security system, significant infrastructural, institutional, and ethical challenges impede its implementation. However, the strategies outlined provide a feasible roadmap for integrating AI into Nigeria's security architecture. If effectively pursued, these measures could position Nigeria not only to address its domestic security challenges but also to become a regional leader in AI-driven security innovation.

Conclusion

This study critically examined the role of Artificial Intelligence (AI) in enhancing security in Nigeria, situating the analysis within the broader context of developing nations. The findings reveal that AI holds immense potential in addressing Nigeria's pressing security challenges, particularly terrorism, cybercrime, insurgency, and organized criminality.

However, the study also underscores that Nigeria's adoption of AI is hindered by systemic challenges, including infrastructural deficits, limited technological expertise, inadequate funding, and weak institutional frameworks. The findings demonstrate that while AI-driven security initiatives have recorded successes in some developing countries, Nigeria lags behind due to policy gaps and governance weaknesses. This reinforces the argument of Gurr (1970) that technological solutions alone cannot resolve insecurity without addressing deeper structural and socio-political issues.

Finally, AI presents both opportunities and risks for Nigeria. Harnessing its benefits requires not just technological investment but also robust policy frameworks, institutional reforms, and ethical safeguards. If Nigeria effectively integrates AI into its security architecture while addressing governance weaknesses, the country could significantly improve its ability to combat insecurity and strengthen its stability in the face of globalization.

Future research directions should include:

i. Empirical studies assessing actual AI implementation outcomes in Nigerian security agencies

ii. Comparative analysis of how Kenya, South Africa, Rwanda, and other African nations are institutionalizing AI governance

iii. Analysis of public perceptions of AI-enabled surveillance and impacts on citizen trust in government

Recommendations

Based on the findings of this study, the following recommendations are made to enhance the effective use of Artificial Intelligence (AI) for security in Nigeria:

1. The Nigerian government should develop a comprehensive National AI and Security Policy that sets clear guidelines for ethical use, data protection, privacy, and accountability in deploying AI technologies.
2. Significant investment is required in digital infrastructure, including high-speed internet, data centers, and smart surveillance systems.
3. Government should collaborate with private tech firms, multinational corporations, and research institutions to fund and develop AI-driven security solutions.

REFERENCES

Adebayo, A. A. (2019). Terrorism and violent extremism in Nigeria: Implications for national security. *African Journal of Criminology and Justice Studies*, 12(1), 43–59.

Adebayo, S., & Aluko, O. (2022). Artificial intelligence and national security in Africa: Opportunities and challenges. *African Security Review*, 31(2), 129–146.

Adelaja, A., & George, J. (2019). Effects of conflicts on agriculture: Evidence from the Boko Haram insurgency. *World Development*, 117, 184–195.

Adeleke, A. (2021). Artificial intelligence and national security in Nigeria: Opportunities and challenges. *Journal of African Studies and Development*, 13(4), 112–123.

Aghedo, I., & Eke, S. J. (2013). From Al Qaeda to Boko Haram: The threat of Islamist terrorism in sub-Saharan Africa. *Conflict, Security & Development*, 13(2), 127–147.

Ajibade, I. (2022). Surveillance technologies and human rights in Africa: A critical reflection. *Journal of African Law*, 66(2), 157–176.

Akinlabi, O. J., & Okafor, C. (2024). Adopting artificial intelligence-based predictive policing in Lagos State: Effectiveness and ethical considerations. *African Journal of Applied Social Sciences and Humanities Research*, 7(4), 156–178.

Ayoade, J. (2021). Cybersecurity and artificial intelligence: Emerging threats and opportunities in Nigeria. *Journal of Information Security Research*, 11(3), 45–59.

Binns, R. (2018). Algorithmic accountability and public reason. *Philosophy & Technology*, 31(4), 543–556. https://doi.org/10.1007/s13347-017-0295-x

Brundage, M., Avin, S., Clark, J., Toner, H., & Amodei, D. (2018). *The malicious use of artificial intelligence: Forecasting, prevention, and mitigation*. arXiv. https://arxiv.org/abs/1802.07228

Bryson, J. J., & Winfield, A. F. (2017). Standardizing ethical design for artificial intelligence and autonomous systems. *Computer*, 50(5), 116–119.

Buzan, B. (1991). *People, states and fear: An agenda for international security studies in the post-Cold War era* (2nd ed.). Harvester Wheatsheaf.

Campbell, J. (2020). *Nigeria: What everyone needs to know*. Oxford University Press.

Chaudhuri, R. (2020). Artificial intelligence and international security: Emerging opportunities and challenges. *Journal of Cyber Policy*, 5(3), 394–412.

Davenport, T. H., & Ronanki, R. (2018). Artificial intelligence for the real world. *Harvard Business Review*, 96(1), 108–116. https://hbr.org/2018/01/artificial-intelligence-for-the-real-world

Deloitte Nigeria. (2025). *Cybersecurity landscape in 2025: Threat assessment and organizational readiness*. Deloitte Professional Services Report.

Egbert, S., & Heimstädt, S. (2024). Algorithmic crime prevention: From abstract police to precision policing. *Policing and Society*, 34(3), 245–267. https://pmc.ncbi.nlm.nih.gov/articles/PMC11225944/

Eze, C., & Udeh, F. (2022). Predictive policing and artificial intelligence: Implications for crime prevention in Nigeria. *International Journal of Police Science and Management*, 24(4), 389–402.

Eze, R. C., Ogbuabor, J. E., & Ugwoke, C. J. (2021). Artificial intelligence and crime prediction in Nigeria: Opportunities and challenges. *International Journal of Security Studies*, 7(2), 22–36.

Gonzalez, A., & Smith, J. (2020). Artificial intelligence applications in modern business operations. *Journal of Business and Technology*, 15(2), 45–59.

Gonzalez, M. A., & Vasquez, T. (2024). Adapting cybersecurity maturity models for resource-constrained settings: A case study of Peru. *Information Systems Development*, 12(2), 89–112. https://doi.org/10.1002/isd2.12350

Gurr, T. R. (1970). *Why men rebel*. Princeton University Press.

IBM. (2023). What is artificial intelligence (AI)? Retrieved from https://www.ibm.com/think/topics/artificial-intelligence

IEEE. (2025, April 10). Quantitative study on artificial intelligence governance policy texts under the framework of the United Nations. In *2025 IEEE International Conference on Ethics in Artificial Intelligence*. https://doi.org/10.1109/EIAI.2025.11035026

Iherue, S. O. (2021). Religious and political insecurity in Nigeria: Causes and effects. *Journal of Languages, Linguistics and Literary Studies*, 10(4), 163–176.

Iyengar, S., & Kinder, D. R. (1987). *News that matters: Television and American opinion*. University of Chicago Press.

Kukah, M. H. (2010). *Religion, politics and power in Northern Nigeria*. Spectrum Books.

McQuail, D., & Deuze, M. (2020). *McQuail's media and mass communication theory* (7th ed.). Sage Publications.

Mhlanga, D. (2022). Artificial intelligence in the fourth industrial revolution: Risks, challenges and opportunities. *Sustainability*, 14(1), 482. https://doi.org/10.3390/su14010482

Mienye, I. D., Rauch, H., & Thudium, M. (2024). Artificial intelligence and sustainable development in Africa. *Sustainability*, 16(4), 1298. https://doi.org/10.3390/su16041298

Mohammed, I., & Thomas, K. (2024). Cyber shadows: Neutralizing security threats with AI and targeted policy measures. *Journal of Cybersecurity Research*, 15(1), 112–135. https://arxiv.org/pdf/2501.09025.pdf

Mohammed, S., Khan, A., & Patel, R. (2024). Advancing cybersecurity and privacy with artificial intelligence: Current trends and future research directions. *Frontiers in Big Data*, 7(2), 1–18. https://doi.org/10.3389/fdata.2024.1497535

Morgan, D. L. (1997). *Focus groups as qualitative research* (2nd ed.). Sage Publications.

Mushemeza, J., & Zille, H. (2025). Understanding Africa's AI governance landscape: Insights from policy practice and policy discourse. *Carnegie Endowment for International Peace, Africa Program Report*. https://carnegieendowment.org/posts/2025/09/understanding-africas-ai-governance-landscape

Musoni, M. (2024). Envisioning Africa's AI governance landscape in 2024. *ECDPM Briefing Note 177*. European Centre for Development Policy Management.

NCAIR & NITDA. (2025). *National Artificial Intelligence Strategy (NAIS)*. Government of Nigeria. Retrieved from https://ncair.nitda.gov.ng/wp-content/uploads/2025/09/National-Artificial-Intelligence-Strategy-19092025.pdf

Ndukwe, C. (2021). The challenge of digital infrastructure in Nigeria's fourth industrial revolution. *African Journal of Development and ICT*, 11(1), 77–95.

Ndukwe, E. R. (2020). Artificial intelligence: Application, benefit, and challenges in revolutionizing the Nigeria public service. *International Journal of Advanced Engineering and Management*, 5(1), 1–10.

Okolie, A., & Eze, N. (2020). Emerging technologies and border security management in Nigeria. *African Journal of Security Studies*, 29(1), 77–94.

Okolie, U. C. (2024). Distinction between traditional security and modern security: A conceptual discourse. *Journal of Administrative Science*, 19(2), 247–266.

Okon, E., & Effiong, J. (2020). Artificial intelligence and cybersecurity management in Nigerian financial institutions. *African Journal of Information Systems*, 12(3), 155–172.

Omotayo, T. (2021). Artificial intelligence applications in counterterrorism: Lessons for Nigeria. *Journal of African Studies and Development*, 13(2), 23–35.

Onuoha, F. (2019). The role of drones in counter-insurgency operations in Nigeria. *Journal of Defense Studies and Resources*, 5(1), 1–12.

Onuoha, F. C. (2014). *A danger not to Nigeria alone: Boko Haram's transnational reach and regional responses*. Friedrich Ebert Stiftung Regional Office.

Perry, W. L., McInnis, B., Price, C., Smith, S., & John, S. (2013). *Predictive policing: The role of crime forecasting in law enforcement operations*. RAND Corporation.

Rajesh, K., & Patel, V. (2024). Predictive policing with the help of machine learning: Principles, algorithms, and ethical implications. *International Journal of Research and Publication Review*, 6(11), 234–268. https://ijrpr.com/uploads/V6ISSUE11/IJRPR55645.pdf

Rogers, E. M., & Dearing, J. W. (1988). Agenda-setting research: Where has it been? Where is it going? *Communication Yearbook*, 11, 555–594.

Russell, S. J., & Norvig, P. (2016). *Artificial intelligence: A modern approach* (3rd ed.). Pearson.

Sarfo, D., Ansah, S., & Boakye, S. (2025). Toward an African agenda for AI safety. *International AI Safety Report Synthesis: African Perspectives*. https://arxiv.org/pdf/2508.13179.pdf

Taddeo, M., & Floridi, L. (2018). How AI can be a force for good. *Science*, 361(6404), 751–752. https://doi.org/10.1126/science.aat5991

Trist, E. (1981). *The evolution of socio-technical systems* (Occasional Paper No. 2). Ontario Quality of Working Life Centre.

UNCTAD. (2025). *World investment report 2025: Reforming international investment governance*. Chapter IV: Designing national policies for AI. Retrieved from https://unctad.org/system/files/official-document/tir2025ch4_en.pdf

UNESCO. (2021). *AI and education: Guidance for policy makers*. UNESCO Publishing.

United Nations Development Programme. (1994). *Human development report 1994: New dimensions of human security*. Oxford University Press.

Waltz, K. N. (1979). *Theory of international politics*. McGraw-Hill.

World Bank. (2025). *Digital progress and trends report 2025: Strengthening AI governance in developing countries*. World Bank Publications. Retrieved from https://openknowledge.worldbank.org/

World Economic Forum. (2025). *Global risks report 2025: Understanding systemic risks in a transforming world*. Retrieved from https://www.weforum.org

Zeng, Y., Lu, E., & Huangfu, C. (2017). Linking artificial intelligence principles. *Proceedings of the 26th International Joint Conference on Artificial Intelligence (IJCAI-17)*, 4197–4203.