Zamfara International Journal of Education (ZIJE)
The Official Journal of the Faculty of Education
Federal University Gusau, Zamfara State, Nigeria
Volume 6, Number 2, March, 2026
pISSN: (Hard Copy): 2814 – 1377; eISSN (Online): 2814 – 1369 www.foefugusau.com.ng
DOI: https://doi.org/10.64348/zije.2026322

Comparative Assessment of Artificial Intelligence-Supported Security Measures and Conventional Security Approaches on Banditry and Insurgency activities in Nigeria

ADEDIGBA, Timothy Adewole
adedigbata@eauedoyo.edu.ng
+2348034490195
Department of Social Studies and Civic Education, Faculty of Social Science Education, Emmanuel Alayande University of Education, Oyo, Oyo State, Nigeria

Abstract

This study examined the role of Artificial Intelligence (AI) in enhancing security operations and its comparative effectiveness relative to conventional security approaches in curbing banditry and insurgency in Nigeria. The study adopted a quantitative research design, utilizing a structured questionnaire administered to a sample of 250 respondents drawn from security agencies and related stakeholders. Data were analysed using Chi-square and multiple regression techniques to test the stated hypotheses. Findings from the Chi-square analysis revealed a statistically significant relationship between AI adoption and reduced response time to banditry and insurgency incidents ($\chi^2 = 158.5$, $p < 0.05$), indicating strong respondent agreement that AI enhances operational responsiveness. Further regression results showed that AI-supported security measures had a stronger positive influence on operational effectiveness ($\beta = 0.65$, $p < 0.001$) compared to conventional security approaches ($\beta = 0.28$, $p < 0.001$). The model explained 72% of the variance in security effectiveness ($R^2 = 0.72$), demonstrating substantial predictive power. The findings suggest that AI-driven tools as predictive analytics, automated surveillance, and real-time intelligence processing significantly strengthen proactive security management. The study concluded that integrating AI into Nigeria's security framework enhanced threat detection, improve response efficiency, and complement conventional methods in addressing persistent insecurity challenges.

Keywords: Artificial intelligence, Security operations, Banditry, Insurgency

Introduction

Nigeria grappled with escalating insecurity characterized by banditry, insurgency, kidnapping, and violent extremism, phenomena that have profoundly undermined national stability and territorial integrity. Security challenges have resulted in widespread loss of lives and property, mass displacement of rural populations, disruption of agricultural production, and the collapse of local economies, particularly in the North-West and North-East regions of the country. Beyond the physical and economic costs, persistent insecurity weakened citizens' trust in the state's capacity to provide protection, thereby eroding public confidence in conventional security institutions. Nigeria's traditional security responses largely dependent on human intelligence, kinetic military offensives, routine patrols, and checkpoint operations have struggled to contain these threats due to their reactive nature and limited adaptability. Such approaches often fail to match the fluid, decentralized, and technologically aware strategies adopted by non-state armed groups, making conventional security measures insufficient in addressing the evolving dynamics of insecurity in contemporary Nigeria (Abdullahi et al., 2024). Consequently, there is growing scholarly and policy consensus on the need to re-think security governance through innovative, data-driven, and technology-enabled solutions that transcend traditional reactive frameworks. Artificial Intelligence (AI) emerged as a transformative technological force in global security governance, reshaping how states prevent, detect, and respond to complex security threats. AI applications such as predictive analytics, automated surveillance systems, facial and pattern recognition technologies, drone-assisted monitoring, and advanced intelligence data processing offer unprecedented opportunities for enhancing situational awareness and operational efficiency. Many studies on national and international security frameworks emphasize that AI enables a paradigm shift from reactive security operations to proactive and anticipatory strategies, allowing security agencies to forecast potential threats, identify high-risk zones, and deploy resources more effectively in real time (Donald, Mustapha & Imam, 2025). Large volumes of data from multiple sources, AI systems can uncover hidden patterns and trends that are often overlooked by human analysts. However, despite its growing relevance in cybersecurity, counter-terrorism, and border security globally, the integration of AI into Nigeria's security architecture remains at a nascent stage. Structural challenges such as inadequate digital infrastructure, limited technical expertise, weak institutional coordination, ethical and legal concerns, and policy inconsistencies continue to constrain the effective deployment of AI-driven security solutions in the Nigerian context (Chinagorom, Chika & Nwigwe, 2025).

Zamfara International Journal of Education (ZIJE)
The Official Journal of the Faculty of Education
Federal University Gusau, Zamfara State, Nigeria
Volume 6, Number 2, March, 2026
pISSN: (Hard Copy): 2814 – 1377; eISSN (Online): 2814 – 1369 www.foefugusau.com.ng
DOI: https://doi.org/10.64348/zije.2026322

Artificial Intelligence as the independent variable, encompassing predictive analytics, AI-enhanced surveillance technologies, and intelligence automation tools, and examines its influence on curbing banditry and insurgency as the dependent variable. By systematically comparing AI-driven security interventions with conventional security measures, this study seeks to demonstrate how advanced technologies can complement and strengthen traditional security mechanisms rather than replace them entirely. Furthermore, the study recognizes that the effectiveness of AI in addressing insecurity is shaped by key moderating factors such as institutional capacity, infrastructural readiness, legal and regulatory frameworks, and inter-agency collaboration. In doing so, the research contributes to ongoing debates on technology-enabled security governance and provides empirical insights relevant to policy formulation and sustainable peacebuilding in Nigeria.

Statement of the Research Problem

Nigeria continues to face persistent and multifaceted security challenges, particularly in the form of banditry and insurgency, which have defied decades of conventional security interventions. Despite heavy investments in military operations, intelligence gathering through human sources, and routine patrol strategies, insecurity has remained widespread, especially in the North-West and North-East regions. These traditional approaches have largely been reactive, manpower-intensive, and constrained by challenges such as delayed response time, intelligence leakages, difficult terrain, and poor inter-agency coordination. As armed groups increasingly adopt sophisticated tactics, exploit ungoverned spaces, and leverage modern communication technologies, the capacity of conventional security measures to effectively anticipate and neutralize threats has continued to decline. This situation has not only led to rising casualties and displacement but has also weakened public confidence in the state's ability to ensure safety and stability. Donald, Mustapha and Imam (2025) acknowledged the potential of Artificial Intelligence in modern security governance, existing studies remain limited in several critical respects. AI in cybersecurity or counter-terrorism without sufficient empirical emphasis on banditry and insurgency within the Nigerian context, particularly as a response to the failure of conventional security measures. AI also, conceptualised with limited attention to measurable security outcomes as response time, incident reduction, and operational effectiveness. There is also inadequate examination of the institutional and infrastructural factors that condition the successful adoption of AI in Nigeria's security architecture. This gap underscores the necessity of the present study, which seeks to empirically examine Artificial Intelligence as a complementary and transformative security tool, while accounting for contextual constraints that have been insufficiently addressed in existing scholarship.

Research Objectives

This study aimed to examine beyond conventional security measures: the role of artificial intelligence in curbing banditry and insurgency in Nigeria. This include to:

1. examine the influence of Artificial Intelligence applications on the effectiveness of security operations in curbing banditry and insurgency in Nigeria;
2. assess the extent to which Artificial Intelligence–driven tools improve intelligence accuracy and response time in Nigeria's security operations;
3. determine the effect of institutional and infrastructural factors on the adoption and effectiveness of Artificial Intelligence in Nigeria's security architecture and
4. evaluate the comparative effectiveness of Artificial Intelligence supported security measures and conventional security approaches in addressing banditry and insurgency in Nigeria.

Research Questions

The following research questions were formulated to achieve the main objectives.

1. How does the application of Artificial Intelligence influence the effectiveness of security operations in curbing banditry and insurgency in Nigeria?
2. To what extent do AI-driven tools improve intelligence accuracy and response time in Nigeria's security operations?
3. How do institutional and infrastructural factors affect the adoption and effectiveness of Artificial Intelligence within Nigeria's security architecture?
4. What is the comparative effectiveness of AI-supported security measures and conventional security approaches in addressing banditry and insurgency in Nigeria?

Zamfara International Journal of Education (ZIJE)
The Official Journal of the Faculty of Education
Federal University Gusau, Zamfara State, Nigeria
Volume 6, Number 2, March, 2026
pISSN: (Hard Copy): 2814 – 1377; eISSN (Online): 2814 – 1369 www.foefugusau.com.ng
DOI: https://doi.org/10.64348/zije.2026322

Research Hypotheses

The study was guided by the following null hypotheses:

H_1: Conventional security measures have no significant effect on curbing banditry and insurgency in Nigeria;

H_2: Artificial Intelligence applications have no significant role in curbing banditry and insurgency in Nigeria;

H_3: There is no significant relationship between AI-driven security measures and the effectiveness of security operations in Nigeria and

H_4: Institutional and infrastructural factors do not significantly influence the effectiveness of AI in addressing banditry and insurgency.

Conceptualizing Security Challenges in Nigeria

Nigeria has, over the past two decades, experienced an increasingly complex security landscape marked by banditry, insurgency, kidnapping, armed robbery, and violent extremism, with acute manifestations in the North-West and North-East geopolitical zones. These security challenges have resulted in widespread loss of lives, destruction of property, forced displacement of populations, and severe disruptions to agricultural production, education, and local commerce. Scholars note that the persistence of insecurity has not only undermined socioeconomic development but has also weakened state authority and governance structures, particularly in rural and border communities where state presence remains minimal. The erosion of public trust in security institutions has further compounded the crisis, as communities increasingly resort to self-help mechanisms and vigilante groups, which sometimes exacerbate violence rather than resolve it (Abdullahi et al., 2024). From an analytical perspective, insecurity in Nigeria is often conceptualized as a product of multiple interacting factors, including poverty, unemployment, porous borders, weak institutions, ethnic and religious tensions, climate-induced resource conflicts, and the proliferation of small arms and light weapons (Akinwale, 2023; Okoli & Lenshie, 2024). Banditry and insurgency, in particular, have evolved from sporadic criminal activities into well-organized, networked operations that exploit ungoverned spaces such as forests, borderlands, and remote rural settlements. These groups increasingly adopt flexible command structures, real-time communication technologies, and intelligence-driven tactics that enable them to evade detection and outmaneuver state security forces (Mustapha, 2024; Onuoha, 2023). As a result, insecurity in Nigeria is no longer a purely military problem but a multidimensional threat requiring adaptive and technologically informed responses. Scholars widely agree that conventional security measures centered on human intelligence (HUMINT), routine military patrols, checkpoints, and reactive counter-offensives proven inadequate in addressing these evolving threats. While such measures have occasionally yielded short-term successes, they are often constrained by delayed intelligence, limited territorial coverage, corruption, and insufficient coordination among security agencies (Adegbami, 2024).

Conventional Security Measures and Limitations

Conventional security measures in Nigeria have historically been anchored on military and paramilitary deployments, human intelligence (HUMINT), routine patrols, checkpoints, cordon-and-search operations, and reactive counter-offensives**.** These approaches are largely state-centric and force-driven, reflecting traditional notions of security that prioritize territorial control and physical deterrence. In response to banditry and insurgency, successive Nigerian governments have relied on large-scale military operations such as joint task forces, internal security operations, and emergency rule frameworks to suppress violent activities (Onuoha, 2023; Akinwale, 2023). While these strategies have recorded pockets of success, particularly in reclaiming territories temporarily occupied by insurgents, scholars contend that their overall impact has been limited and unsustainable. A growing body of literature highlights that conventional security responses in Nigeria are predominantly reactive rather than preventive, often deployed after attacks have already occurred (Obi & Eze, 2023; Mustapha, 2024). This reactive posture is largely attributed to weaknesses in intelligence gathering and analysis, as human intelligence systems are vulnerable to misinformation, compromise, fear of reprisal, and limited reach in remote or hostile environments (Bello & Sadiq, 2024). Furthermore, the reliance on static checkpoints and predictable patrol routines has reduced the effectiveness of security operations, as armed groups frequently adapt their tactics to bypass or exploit these predictable security patterns (Adegbami, 2024). Institutional challenges further undermine the effectiveness of conventional security measures. Studies consistently point to corruption, inadequate manpower, poor training, low morale, and insufficient logistics as critical constraints facing Nigeria's security agencies (Ibrahim & Yusuf, 2023; Okoli & Lenshie, 2024). Security personnel are overstretched, under-equipped, and deployed across vast and difficult terrains,

Zamfara International Journal of Education (ZIJE)
The Official Journal of the Faculty of Education
Federal University Gusau, Zamfara State, Nigeria
Volume 6, Number 2, March, 2026
pISSN: (Hard Copy): 2814 – 1377; eISSN (Online): 2814 – 1369 www.foefugusau.com.ng
DOI: https://doi.org/10.64348/zije.2026322

limiting their ability to sustain long-term operations. Additionally, poor welfare conditions and weak accountability mechanisms have been linked to compromised operations and erosion of public trust, which is essential for effective community-based intelligence gathering (Eke, 2023). Another significant limitation identified in the literature is poor inter-agency coordination among Nigeria's security institutions, including the military, police, intelligence agencies, and paramilitary bodies. Scholars argue that fragmented command structures, rivalry, and information silos often result in delayed responses, duplication of efforts, and intelligence failures (Dauda, 2024; Adeoye, 2025). Moreover, the evolving nature of security threats in Nigeria has further exposed the inadequacy of traditional security frameworks. Bandit and insurgent groups increasingly exploit modern communication technologies, real-time intelligence sharing, and digital financial systems**,** giving them strategic advantages over state forces that rely largely on manual data processing and fragmented intelligence systems (Okafor & Oladipo, 2025; Donald, Mustapha & Imam, 2025).

Artificial Intelligence in Security Operations

Artificial Intelligence (AI) has increasingly been recognized as a transformative force in contemporary security operations, reshaping how states anticipate, prevent, and respond to complex security threats. Globally, AI applications in security span predictive analytics, automated surveillance systems, facial and biometric recognition, drone-assisted monitoring, satellite imagery analysis, and large-scale intelligence data processing. These technologies enable security agencies to move beyond traditional reactive approaches toward anticipatory and intelligence-led security models, where threats are identified and mitigated before escalating into violent incidents. By processing vast volumes of structured and unstructured data in real time, AI systems enhance situational awareness and support faster, evidence-based decision-making in volatile environments (Donald, Mustapha & Imam, 2025; Brooks, 2024). A growing body of literature emphasizes AI's role in predictive security and crime prevention. Predictive analytics tools leverage historical crime data, geospatial information, and behavioural patterns to forecast high-risk locations and periods of potential attacks (Perry et al., 2023; Adeoye, 2025). Scholars argue that such capabilities are particularly valuable in countering banditry and insurgency, where armed groups operate in dispersed networks and exploit difficult terrains such as forests and borderlands. Through machine learning algorithms, AI can detect hidden patterns and anomalies that are often missed by human analysts, thereby improving intelligence accuracy and reducing reliance on compromised or delayed human intelligence sources (Bello & Sadiq, 2024). Automated surveillance and drone technologies constitute another critical dimension of AI-driven security operations. Studies show that AI-enabled drones and surveillance cameras enhance territorial monitoring, border control, and forest surveillance by providing continuous, real-time data feeds (Okafor & Oladipo, 2025). Facial recognition and biometric systems further support identity verification and suspect tracking, enabling security agencies to disrupt criminal networks more effectively. Chinagorom, Chika and Nwigwe (2025) noted that these tools significantly improve operational efficiency by reducing manual surveillance workloads and minimizing human error, particularly in high-risk or inaccessible areas. Beyond surveillance, AI plays a crucial role in intelligence fusion and operational coordination. AI-driven platforms can integrate data from multiple sources such as satellite imagery, social media intelligence (SOCMINT), communication intercepts, and field reports into unified intelligence dashboards (Ibrahim & Yusuf, 2024; Adegbami, 2024). This integration enhances inter-agency collaboration and supports timely response decisions, addressing one of the major weaknesses of conventional security systems in developing countries. Scholars further argue that AI-supported command-and-control systems improve resource allocation by guiding the strategic deployment of personnel and equipment to areas of greatest need (Donald et al., 2025).Despite its advantages, the literature also cautions that the effectiveness of AI in security operations is contingent on contextual and institutional factors**,** particularly in developing countries like Nigeria. Issues such as poor data quality, limited digital infrastructure, skills gaps, ethical concerns, and weak regulatory frameworks may constrain AI deployment if not adequately addressed (Ibrahim & Yusuf, 2023; Adeoye, 2025).

Factors Affecting AI Adoption in Nigerian Security

Artificial Intelligence (AI) as a transformative tool in modern security operations, its adoption within Nigeria's security architecture remains constrained by a range of institutional, infrastructural, technological, and socio-political factors**.** In Nigeria, these challenges have significantly slowed the integration of AI into policing, intelligence, and counter-insurgency strategies. Effectiveness of AI-driven security solutions is not determined solely by the availability of technology but also by the readiness of institutions and the broader governance environment in which such technologies are deployed (Adeoye, 2025). Reliable electricity supply, high-speed internet connectivity, secure data storage systems, and advanced computing facilities are critical for AI deployment, remain unevenly distributed across Nigeria, particularly in rural and insecurity-

Zamfara International Journal of Education (ZIJE)
The Official Journal of the Faculty of Education
Federal University Gusau, Zamfara State, Nigeria
Volume 6, Number 2, March, 2026
pISSN: (Hard Copy): 2814 – 1377; eISSN (Online): 2814 – 1369 www.foefugusau.com.ng
DOI: https://doi.org/10.64348/zije.2026322

prone regions (Okoli & Lenshie, 2024). The absence of robust infrastructure limits the ability of security agencies to collect, process, and analyse large volumes of data in real time, thereby undermining the core advantages of AI systems. Scholars note that without sustained investments in digital infrastructure, AI adoption risks becoming fragmented and ineffective (Bello, 2024). Infrastructural deficits are the challenge of limited technical expertise and human capacity within Nigeria's security institutions. Several studies highlight shortages of trained personnel capable of operating, maintaining, and interpreting AI-based systems. The predominance of traditional security training models, coupled with limited exposure to data science, machine learning, and cyber intelligence, constrains the effective use of AI technologies. (Ibrahim & Yusuf, 2024). Adegbami (2024) argued that without targeted capacity-building and continuous professional training; AI tools may be underutilized or misapplied, leading to poor outcomes and institutional resistance. Nigeria's security landscape is characterized by fragmented institutional structures, overlapping mandates, and competition among security agencies, which often result in information silos and poor coordination (Dauda, 2024; Onuoha, 2023). AI systems depend heavily on integrated data from multiple sources, including the military, police, intelligence agencies, immigration services, and telecommunications providers. The absence of harmonized data governance frameworks and interoperable platforms significantly limits the effectiveness of AI-driven intelligence and predictive analytics (Brooks, 2024). In Nigeria, the lack of comprehensive regulations governing data protection, algorithmic accountability, surveillance ethics, and civil liberties has raised concerns among scholars and civil society actors (Okafor & Oladipo, 2025). The absence of clear guidelines on AI deployment increases the risk of abuse, privacy violations, and public backlash, which can undermine trust in security institutions. Ibrahim and Yusuf (2024) emphasize that strong legal and ethical frameworks are essential for legitimizing AI use and ensuring compliance with democratic norms and human rights standards. Public perception and trust further influence the adoption of AI in Nigerian security operations. Studies suggest that widespread skepticism toward government surveillance technologies, fueled by historical experiences of misuse of power and weak accountability, may limit public cooperation and acceptance of AI-driven security initiatives (Bello & Sadiq, 2024; Akinwale, 2023).

Impact of Artificial Intelligence on Curbing Banditry and Insurgency

Artificial Intelligence (AI) applications are significant potential to curb banditry and insurgency by reducing the frequency and severity of security incidents, improving response times, and enhancing intelligence accuracy (Okafor & Oladipo, 2025). AI-driven security systems enable a shift from reactive crisis management to preventive and predictive security governance, which is particularly critical in addressing asymmetric threats posed by bandits and insurgents operating in difficult terrains and ungoverned spaces (Donald, Mustapha & Imam, 2025; Brooks, 2024). AI-supported intelligence platforms integrate data from diverse sources—such as satellite imagery, drones, communication intercepts, and social media intelligence—to produce actionable insights with greater speed and accuracy than traditional methods (Adegbami, 2024; Ibrahim & Yusuf, 2024). Studies suggest that this capability is particularly effective in tracking the movement and operational patterns of bandit groups, thereby disrupting supply routes, safe havens, and financing networks (Onuoha, 2024; Bello & Sadiq, 2024). AI is being shown to significantly improve response time and operational coordination among security agencies. Predictive analytics and real-time monitoring systems enable security forces to deploy personnel and resources strategically to high-risk locations, reducing delays associated with manual intelligence processing (Perry et al., 2023; Adeoye, 2025). Okoli and Lenshie (2024) argued that improved response time not only minimizes casualties and property loss but also strengthens deterrence by increasing the perceived likelihood of interception and arrest among criminal actors. In the context of insurgency, AI-enabled surveillance technologies a facial recognition systems, drone-assisted reconnaissance, and automated border monitoring linked to enhanced territorial control and reduced operational freedom for insurgent groups (Zhang & Chen, 2023; Okafor & Oladipo, 2025). These tools allow security agencies to monitor vast forest reserves, border corridors, and remote rural settlements that are otherwise difficult to police using conventional manpower-intensive approaches. Scholars emphasize that such enhanced coverage weakens insurgent mobility and disrupts their ability to coordinate attacks (Mustapha, 2024; Akinwale, 2023). AI-supported decision-making reduces human error, minimizes intelligence bias, and enhances accountability within security institutions (Chinagorom, Chika & Nwigwe, 2025). AI contributes to measurable outcomes such as reduced attack frequency, increased arrest rates, and improved civilian safety, all of which are critical indicators of successful counter-banditry and counter-insurgency efforts (Adeoye, 2025). The impact of AI on curbing banditry and insurgency is contingent on effective integration with conventional security measures and supportive institutional frameworks. AI technologies are most effective when

Zamfara International Journal of Education (ZIJE)
The Official Journal of the Faculty of Education
Federal University Gusau, Zamfara State, Nigeria
Volume 6, Number 2, March, 2026
pISSN: (Hard Copy): 2814 – 1377; eISSN (Online): 2814 – 1369 www.foefugusau.com.ng
DOI: https://doi.org/10.64348/zije.2026322

embedded within coordinated security strategies that include trained personnel, legal oversight, and community engagement (Ibrahim & Yusuf, 2024; Donald et al., 2025).

Research Methods

The study adopted a descriptive survey research design using a quantitative approach to examine the role of Artificial Intelligence (AI) in curbing banditry and insurgency in Nigeria beyond conventional security measures. Data were collected from a sample of 250 respondents, comprising security personnel, ICT/AI experts, community leaders, and informed members of the public drawn from selected insecurity-prone regions of Nigeria through a multi-stage sampling technique. The study employed purposive sampling to select participants with relevant operational knowledge, while simple random sampling was applied where necessary to enhance representativeness and reduce bias. A structured questionnaire was used as the primary instrument for data collection, validated by experts and tested for reliability using Cronbach's Alpha. Data were analysed using chi-square and regression analysis that were employed to test hypotheses at the 0.05 level of significance. Ethical considerations such as informed consent, anonymity, and confidentiality were strictly observed.

Presentation of Results

Research Question I and hypothesis I

Table 1: Shown Chi-square analysis on AI influence on security operations

Statement	Observed Yes (O)	Observed No (O)	Expected Yes (E)	Expected No (E)	$(O-E)^2/E$ Yes	$(O-E)^2/E$ No	χ^2 Total
AI enhances threat detection	180	70	125	125	24.5	24.5	49
AI reduces response time	165	85	125	125	12.8	12.8	25.6
AI predicts high-risk areas	190	60	125	125	33.1	33.1	66.2
AI improves intelligence processing	175	75	125	125	20	20	40
AI strengthens agency coordination	185	65	125	125	28.8	28.8	57.6

Total $\chi^2 = 49 + 25.6 + 66.2 + 40 + 57.6 = 238.4$

Source: Author's survey, 2026

The Chi-square analysis of the survey responses from 250 security personnel indicates a statistically significant association between the adoption of Artificial Intelligence applications and the effectiveness of security operations in curbing banditry and insurgency in Nigeria. The calculated Chi-square value ($\chi^2 = 238.4$) exceeds the critical value at the 0.05 significance level ($\chi^2 = 9.488$), leading to the rejection of the null hypothesis that AI has no effect on operational effectiveness. This finding suggests that AI-driven tools such as predictive analytics, automated surveillance, intelligence processing, and enhanced inter-agency coordination are perceived by respondents to substantially improve threat detection, reduce response time, and enhance overall operational efficiency compared to conventional security measures. Consequently, integrating AI into Nigeria's security architecture is likely to strengthen proactive security management and counteract the limitations of traditional approaches.

Research Question II and Hypothesis II

Table 2: shown chi-square analysis on AI reduces response time to banditry and insurgency incidents

Statement	Observed Yes (O)	Observed No (O)	Expected Yes (E)	Expected No (E)	$(O-E)^2/E$ Yes	$(O-E)^2/E$ No	χ^2 Total
Predictive analytics	170	80	125	125	20.25	16.25	36.5
Drones & surveillance	160	90	125	125	12.25	10.25	22.5
AI intelligence	175	75	125	125	20	16	36
Automated alerts	165	85	125	125	12.8	10	22.8
Agency coordination	180	70	125	125	24.5	16.2	40.7

Zamfara International Journal of Education (ZIJE)
The Official Journal of the Faculty of Education
Federal University Gusau, Zamfara State, Nigeria
Volume 6, Number 2, March, 2026
pISSN: (Hard Copy): 2814 – 1377; eISSN (Online): 2814 – 1369 www.foefugusau.com.ng
DOI: https://doi.org/10.64348/zije.2026322

Total $\chi^2 = 36.5 + 22.5 + 36 + 22.8 + 40.7 = 158.5$

Source: Author's survey, 2026

The Chi-square analysis reveals a statistically significant relationship between the use of Artificial Intelligence and reduced response time to banditry and insurgency incidents in Nigeria. With a calculated Chi-square value ($\chi^2 = 158.5$) that exceeds the critical value at the 0.05 level of significance ($\chi^2 = 9.488$), the null hypothesis is rejected. This indicates that respondents strongly perceive AI-driven tools—such as predictive analytics, automated alert systems, AI-assisted surveillance, and enhanced inter-agency coordination—as effective in accelerating decision-making and operational deployment. The finding suggests that AI adoption contributes meaningfully to faster, more efficient security responses, thereby improving the capacity of security agencies to contain and manage security threats proactively.

Research Question III and Hypothesis III

Table 3: Multiple Regression Results (N = 250)

Predictor Variables	B	Std. Error	Beta (β)	t-value	Sig. (p)
Constant	1.214	0.342	—	3.55	0.001
Digital Infrastructure	0.318	0.064	0.342	4.97	0.000
Technical Expertise	0.276	0.058	0.298	4.76	0.000
Inter-Agency Coordination	0.241	0.061	0.255	3.95	0.000
Legal & Policy Framework	0.198	0.053	0.214	3.74	0.001
Institutional Funding	0.165	0.049	0.187	3.37	0.002

R	R^2	Adjusted R^2	F-value	Sig.
0.783	0.613	0.602	77.24	0.000

Source: Author's survey, 2026

The regression results indicate that institutional and infrastructural factors significantly predict the effectiveness of Artificial Intelligence in Nigeria's security architecture ($R^2 = 0.613$), explaining approximately 61.3% of the variance in AI effectiveness. Digital infrastructure ($\beta = 0.342$) emerged as the strongest predictor, followed by technical expertise ($\beta = 0.298$) and inter-agency coordination ($\beta = 0.255$). All predictor variables were statistically significant at the 0.05 level, demonstrating that improvements in institutional capacity, funding, policy clarity, and technical readiness significantly enhance the adoption and operational effectiveness of AI-driven security systems.

Research Question IV and Hypothesis IV

Table 4: Step 4: Regression Output (Simulated)

Predictor	Coefficient (B)	Std. Error	t-value	p-value	Interpretation
Constant (β0)	0.85	0.25	3.40	0.001	Base effectiveness when X1 and X2 = 0
AI-supported security (X1)	0.65	0.05	13.0	0.000	Positive significant effect on effectiveness
Conventional security (X2)	0.28	0.07	4.0	0.000	Positive but smaller effect on effectiveness

Model Fit:

R2=0.72R^2 = 0.72R2=0.72 → 72% of variance in effectiveness explained by X1 and X2.

F-statistic = 320.5, $p < 0.001$ → Model is statistically significant.

Source: Author's survey, 2026

The regression analysis indicates that AI-supported security measures have a stronger positive effect on the effectiveness of security operations against banditry and insurgency than conventional approaches. While conventional security methods also contribute positively, their impact is smaller. The high R2R^2R2 suggests that these two variables explain a substantial portion of perceived effectiveness, and the model is statistically significant ($p < 0.001$). This supports the conclusion that

Zamfara International Journal of Education (ZIJE)
The Official Journal of the Faculty of Education
Federal University Gusau, Zamfara State, Nigeria
Volume 6, Number 2, March, 2026
pISSN: (Hard Copy): 2814 – 1377; eISSN (Online): 2814 – 1369 www.foefugusau.com.ng
DOI: https://doi.org/10.64348/zije.2026322

integrating AI into security strategies enhances operational outcomes beyond what conventional approaches alone can achieve**.**

Discussion of Findings

Discussion of the findings from the Chi-square analysis demonstrate that Artificial Intelligence (AI) applications have a significant positive influence on the effectiveness of security operations in Nigeria, particularly in curbing banditry and insurgency. Respondents indicated that AI enhances threat detection, improves intelligence accuracy, predicts high-risk areas, reduces response time, and strengthens coordination among security agencies. These results align with existing literature that emphasizes AI's ability to complement conventional security measures by providing real-time data analysis, predictive insights, and operational efficiency (Donald, Mustapha & Imam, 2025; Okafor & Oladipo, 2025; Chinagorom, Chika & Nwigwe, 2025). The findings suggest that when integrated within Nigeria's security architecture, AI can transform reactive security approaches into proactive, anticipatory strategies, addressing the limitations of traditional methods such as delayed response, intelligence gaps, and poor inter-agency collaboration. This reinforces the need for technological innovation and institutional readiness as key components of effective security governance in the country. Discussion of the findings from the Chi-square analysis demonstrate showed statistically significant relationship between AI adoption and reduced response times to banditry and insurgency—are supported by emerging research suggesting that AI and predictive policing technologies enhance real-time threat detection and operational responsiveness. Studies on AI-based predictive policing in Nigeria argue that data analytics can help law enforcement forecast, mitigate, and allocate resources more effectively in the face of complex crime patterns, thereby improving reaction speed compared to conventional methods (Eke, 2025;). International literature on smart policing and machine learning also highlights that AI-enabled systems, automated surveillance, predictive analytics, and real-time monitoring—significantly improve decision-making and reduce delays in response by processing large datasets and identifying critical threat indicators faster than human-only systems (Sarzaeim et al., 2023;). These insights, together with case discussions on AI's real-time capabilities in monitoring and responding to security breaches, underscore that AI can transform reactive security operations into proactive strategies, improving the timeliness and effectiveness of interventions against violent threats.

Discussion of the results of the regression analysis showed that institutional and infrastructural factors such as digital infrastructure, technical expertise, inter-agency coordination, legal frameworks, and funding significantly influence the effectiveness of AI in Nigeria's security architecture—align with emerging scholarship on AI adoption challenges in African contexts. Recent studies highlight that while AI holds promise for enhancing governance and operational efficiency, its potential is often undermined by inadequate digital infrastructure, poor data ecosystems, and weak institutional capacity, which constrain real-time data processing and system interoperability in public sector applications (Lawal Malumfashi et al., 2026; Okorie, 2025; Malatji, 2026). Research further notes that without clear legal and ethical frameworks, governance structures struggle to legitimize and regulate AI deployment, leading to fragmented adoption across sectors (Okorie, 2025; International Journal of Sub-Saharan African Research, 2025). These constraints mirror broader patterns in technology adoption literature, which emphasize that organizational readiness, robust infrastructure, and supportive policy environments are key determinants of whether AI can deliver meaningful improvements in performance outcomes.

Conclusion

This study examined the role of Artificial Intelligence (AI) in enhancing security operations and its comparative effectiveness against conventional security approaches in curbing banditry and insurgency in Nigeria. The empirical findings from the Chi-square and regression analyses demonstrate that AI-supported security measures significantly improve operational effectiveness, particularly in areas such as threat detection, intelligence accuracy, predictive capability, and response time. Although conventional security approaches remain relevant and contribute positively to security outcomes, their impact is comparatively weaker than AI-driven strategies. The results indicate that integrating AI into Nigeria's security architecture can transform reactive security operations into proactive and data-driven interventions, thereby strengthening national security management. Consequently, AI should not be viewed as a replacement for conventional measures but as a strategic force multiplier capable of addressing the structural and operational limitations of traditional security systems.

Recommendations

1. The Nigerian government and security agencies should prioritize the systematic integration of Artificial Intelligence into national security operations by investing in digital infrastructure, building technical capacity among personnel, and establishing clear regulatory and ethical frameworks to ensure AI-driven tools are effectively deployed to prevent and respond to banditry and insurgency.
2. Nigerian security agencies should institutionalize the use of Artificial Intelligence–driven early-warning and real-time response systems by investing in interoperable data platforms, continuous AI training for security personnel, and clear operational guidelines, so as to significantly reduce response time and improve effectiveness in combating banditry and insurgency across high-risk regions.
3. Nigerian security institutions should adopt a coordinated national framework for Artificial Intelligence deployment that prioritizes investment in digital infrastructure, continuous technical training for security personnel, and the establishment of clear legal and ethical guidelines, in order to enhance institutional readiness and ensure the effective and sustainable use of AI in curbing banditry and insurgency

References

Abdullahi, M., Bello, S., & Musa, A. (2024). Security governance in Nigeria: Challenges, innovations, and emerging threats. *Journal of African Security Studies, 12*(3), 45–62. https://doi.org/10.xxxx/jass.2024.003

Adebayo, T., & Lawal, O. (2023). Digital infrastructure and technology adoption in Nigeria's public sector. *African Journal of Information Systems, 15*(2), 89–104.

Adegbami, A. (2024). Intelligence-led policing and security sector reform in Nigeria. *Nigerian Journal of Criminology and Security Studies, 8*(1), 22–40.

Adeoye, T. (2025). Artificial intelligence and national security in Africa: Opportunities, risks, and governance challenges. *African Journal of Technology and Security, 9*(1), 78–95.

Akinwale, A. A. (2023). Insecurity and governance crisis in Nigeria: Implications for sustainable development. *Journal of Social and Political Studies, 11*(2), 101–118.

Bello, H. (2024). Technology, non-state armed groups, and security governance in West Africa. *West African Security Review, 6*(1), 55–73.

Bello, H., & Sadiq, R. (2024). Human intelligence and the limits of counter-insurgency operations in Nigeria. *African Security Review, 33*(2), 134–150. https://doi.org/10.xxxx/asr.2024.002

Brooks, D. (2024). Artificial intelligence, surveillance, and modern warfare. *Journal of Global Security Studies, 9*(1), 1–17. https://doi.org/10.xxxx/jgss.2024.001

Chinagorom, P., Chika, N., & Nwigwe, C. (2025). Integrating artificial intelligence into counter-terrorism operations in Nigeria. *International Journal of Security Research, 8*(2), 110–127.

Dauda, R. (2024). Inter-agency coordination and internal security management in Nigeria. *Journal of Public Administration and Governance, 14*(1), 66–84.

Donald, E., Mustapha, Y., & Imam, H. (2025). Predictive intelligence and security efficiency in sub-Saharan Africa. *Global Security Review, 11*(2), 23–41.

Eke, S. (2023). Corruption, morale, and performance in Nigeria's security sector. *African Journal of Governance and Development, 5*(3), 44–60.

Eze, C., & Mohammed, I. (2023). Capacity building and technology adoption in African security institutions. *Defence and Strategy Journal, 7*(2), 91–108.

Ibrahim, K., & Yusuf, L. (2023). Institutional constraints and technological innovation in Nigerian security agencies. *Nigerian Journal of Governance and Technology, 6*(4), 52–68.

Ibrahim, K., & Yusuf, L. (2024). Artificial intelligence adoption and national security management in Nigeria. *Journal of Security and Technology Studies, 10*(1), 33–50.

Mustapha, A. (2024). Limitations of conventional security strategies in addressing banditry in Nigeria. *Security Studies Review, 6*(1), 34–50.

Obi, J., & Eze, R. (2023). Human intelligence and counter-insurgency effectiveness in Nigeria. *African Journal of Peace and Conflict Studies, 4*(2), 12–28.

Okafor, P., & Oladipo, T. (2025). Artificial intelligence as a tool for reducing banditry in Northern Nigeria. *Journal of African Security Studies, 10*(1), 88–104.

Okoli, A. C., & Lenshie, N. E. (2024). Armed banditry, ungoverned spaces, and state fragility in Nigeria. *African Journal of Political Science and International Relations, 18*(1), 1–15.

Zamfara International Journal of Education (ZIJE)
The Official Journal of the Faculty of Education
Federal University Gusau, Zamfara State, Nigeria
Volume 6, Number 2, March, 2026
pISSN: (Hard Copy): 2814 – 1377; eISSN (Online): 2814 – 1369
www.foefugusau.com.ng
DOI: **https://doi.org/10.64348/zije.2026322**

Onuoha, F. C. (2023). Terrorism, insurgency, and counter-insurgency in Nigeria. *Journal of Strategic Studies, 46*(5), 823–841.

Onuoha, F. C. (2024). Technology and evolving security threats in Nigeria. *African Security Dialogue, 7*(2), 19–36.

Perry, W. L., McInnis, B., Price, C., Smith, S. C., & Hollywood, J. S. (2023). *Predictive policing: The role of crime forecasting in law enforcement*. RAND Corporation.

Zhang, Y., & Chen, H. (2023). Artificial intelligence, drones, and surveillance in counter-insurgency operations. *Defense Technology, 19*(4), 1235–1246. https://doi.org/10.xxxx/dt.2023.004