INTERNATIONAL JOURNAL OF SOCIAL SCIENCE, MANAGEMENT, PEACE AND CONFLICT RESEARCH (IJSMPCR)
Journal homepage: https://ijsmpcr.com/

Integrating Artificial Intelligence into Nigeria's national security: Implications for good governance

By
IBILOYE Oluyemi Joshua
Institute of Governance and Development Studies, Nasarawa State University Keffi, Nigeria

International Journal of Social Science, Management, Peace and Conflict Research, 01(03), 132-145
Publication history: Received on 22 Jan 2026; Revised on 30 Jan 2026; Accepted on 28 Jan, 2026

Abstract

Nigeria's national security environment is confronted with persistent and complex threats, including insurgency, banditry, cyber-attacks, and weak intelligence coordination among security agencies. These challenges have exposed the limitations of conventional security approaches and underscored the urgent need for technological innovation. Artificial Intelligence (AI) has emerged globally as a transformative instrument capable of enhancing security operations, improving decision-making, and strengthening governance frameworks. This study critically examines the implications of integrating AI into Nigeria's national security architecture, with particular focus on its potential to advance good governance. Specifically, the study employed Digital Era Governance Theory to assess how AI can enhance inter-agency coordination by enabling real-time intelligence sharing and collaborative threat assessment among Nigeria's fragmented security agencies. It further investigates the extent to which AI-driven predictive analytics can improve the timeliness of threat detection, enabling security forces to transition from reactive responses to proactive, data-driven interventions. Using a qualitative research design reliant on secondary data from academic literature, policy documents, and security reports, the study identifies key opportunities presented by AI, including enhanced predictive intelligence, improved transparency and accountability, and faster threat response capabilities. However, the study also uncovers significant risks and challenges, such as algorithmic bias, cybersecurity vulnerabilities, infrastructural deficits, limited technical expertise, and over-reliance on foreign AI technologies. The findings reveal that while AI holds great promise for transforming Nigeria's security architecture, its successful integration depends on the existence of robust governance frameworks, ethical safeguards, and institutional preparedness. The study concludes that with strong political will, regulatory oversight, and strategic investment in AI literacy and infrastructure, Nigeria can harness AI to strengthen national security operations while simultaneously reinforcing democratic values, building citizen confidence, and promoting the principles of good governance. Policy recommendations emphasize the need for a national AI security policy, enhanced inter-agency collaboration through centralized intelligence platforms, ethical data governance, and public-private partnerships to ensure responsible and effective AI deployment.

Keywords: Artificial Intelligence, Ethical AI, Good Governance, National Security, Predictive Intelligence

Introduction

Nigeria has a complex and dynamic national security environment that is typified by unending insurgency, banditry, and new cyber threats. There is empirical data showing that banditry and armed military networks have grown in the north and central regions, leading to widespread loss of life, displacement, and economic disturbance (Accord, 2022). At the same time, insurgent organizations like Boko Haram and Islamic State West Africa Province (ISWAP) are still able to take advantage of weak institutional structures and loose borders and undermine the ability of the state to respond to the threat in time and efficiently (Musa et al., 2024). Simultaneously, the emergence of cyber threats, such as digital radicalization or data breaches and

* Corresponding author: IBILOYE Oluyemi Joshua
Department of Security and Strategic Studies, Nasarawa State University, Keffi, Nigeria.

critical infrastructure attacks, is becoming a recognized threat to national security and is challenging to govern and coordinate operations (Adishi et al., 2022).

The governance structures are important in determining the effectiveness of the national security operations. Empirical literature highlights the fact that clear, responsible, and coordinated governance facilitates intelligence sharing, allocation of resources, and cooperation between agencies and improves predictability and responsiveness of security systems (Adishi et al., 2022; Musa et al., 2024). Weak governance, corruption, and fragmented oversight mechanisms, on the other hand, cripple the ability of the security agencies to respond to the conventional and emerging threats.

Artificial intelligence (AI) is being actively used as a game changer in national security operations worldwide with its applications in predictive analytics, threat detection, autonomous systems, and cyber defense (Allen and Chan, 2017). The empirical data that has been gathered in developed countries proves that the implementation of AI increases the rate of decision-making, the precision of operations, and situational awareness, and, at the same time, increases ethical and governance concerns.

Due to Nigeria's security issues, this research aims at exploring how AI implementation can transform good governance in national security. The study will be done with the purpose of evaluating the capability of AI to enhance transparency, accountability, and strategic intelligence and identifying the possible risks and governance issues in order to adopt it responsibly. These dynamics are important to understand so that evidence-based policies that can be used to leverage technological innovations to improve the output of national security can be developed in a way that does not undermine the principles of democratic governance.

Research Questions

The following research questions were engaged by the study

i. How can the integration of Artificial Intelligence enhance inter-agency coordination in Nigeria's national security architecture?
ii. To what extent can predictive analytics improve timeliness of threat detection in Nigeria's national security architecture

Objectives of the Study

The objective of the study examines the integration of Artificial Intelligence into Nigeria’s national security as an implication for good governance. While specific objectives

i. Assess how integration of Artificial Intelligence into inter-agency coordination enhances Nigeria's national security architecture
ii. Investigate the extent that predictive analytics can improve timeliness of threat detection in Nigeria's national security architecture

Literature Review

Conceptual Framework

Artificial intelligence (AI) can be simply described as the process of emulating human intelligence on machines that can learn, reason, solve problems, and make decisions (Papagiannidis et al., 2025). In the framework of national security, AI will include threat detection and predictive analytics technology, cyber defense, and operational automation, thus improving the capabilities of the state to address complex security threats (Mishra, 2025). National security can be defined as safeguarding the citizens, infrastructure, and other institutions of a specific country against external and internal threats that happen within conventional, unconventional, and digital spheres (Nte & Eyororokumoh, 2025). Good governance, on the other hand, involves the presence of a system that is transparent, accountable, and participatory in decision-making and follows the rule of law, as well as the effective delivery of its services so that the security policies and operations are not only legitimate but also efficient (Dunleavy et al., 2006).

There are three theoretical frameworks that support the analysis of AI integration in the national security governance in this study. To begin with, the digital era governance puts an emphasis on the importance of information and communication technologies in making the work of the public sector more efficient, transparent, and active. It offers his prism through which one can observe how AI can maximize intelligence operations and foster accountability and responsive governance (Dunleavy et al., 2006). Second, adaptive leadership theory assumes that complex and fast-changing problems demand the leader, who is capable of marshaling resources, both organizational and societal, to solve systemic issues. Adaptive leadership can be used in finding strategic decisions in the unexplored environments, especially in incorporating new AI technologies in the security field (Heifetz et al., 2009). Third, strategic intelligence management is concerned with the methodological gathering, evaluation, and utilization of intelligence in decision-making and risk reduction. AI boosts all these by offering predictive intelligence, real-time data processing, and cross-security control, and it harmonizes the operational capacities with the purpose of governance (Mishra, 2025; Nte & Eyororokumoh, 2025).

In theoretical terms, this paper connects the deployment of AI to the outcomes of governance by a model where the adoption of AI enhances transparency, accountability, and efficiency in operations related to national security. Mediating mechanisms include predictive analytics, autonomous monitoring, and decision-

support systems, which can transform technological capabilities to have better governance performance (Papagiannidis et al., 2025). The model also takes into consideration the moderating effect of institutional capacity and regulatory control in seeing to it that AI plays a positive role in the process of democratic and responsible security governance.

Literature Review

The use of artificial intelligence (AI) in national security is gaining pace around the world, fueled by the necessity to address more and more complicated threats and to become more efficient in the operations. In the US, AI is widely applied to intelligence collection, autonomous systems, and decision support to quickly evaluate the threat and take proactive measures against conventional and cyber threats (Allen and Chan, 2017; Cummings, 2017). Likewise, the United Kingdom has been working on AI-based predictive analytics to bolster cybersecurity, streamline the workflow of intelligence operations, and facilitate such decisions at the policy level, which focuses on improving the combination of AI with human-driven analytical work to increase precision and efficiency (Brundage et al., 2018). The concept of AI has been at the heart of military modernization, border security, and social surveillance-focused programs in China, which has been a strategically oriented decision to focus on technological superiority in ensuring national security and state dominance (Horowitz, 2018).

The use of AI in intelligence and cybersecurity is complex. The integration of machine learning algorithms, predictive analytics, and big data helps the security agencies detect the emergence of threats, criminality or insurgency patterns, and predict possible security breaches (Allen and Chan, 2017). AI systems can aid in planning scenarios, evaluating risks, and distributing resources; therefore, enhancing the effectiveness and promptness of strategic decisions in a decision-making context (Cummings, 2017). Besides, AI also plays a role in interagency intelligence fusion, boosting information sharing and coordination of multifaceted operations (Horowitz, 2018).

Although such benefits are in place, there are still ethical and governance issues that are prevalent. The threats to the legitimacy and accountability of AI-driven security operations are algorithmic bias, opacities, and low explainability (Batool et al., 2023; Ziosi and Pruss, 2024). Biased data or non-transparent algorithms in decision-making might lead to loss of trust in the population, increase inequality, and disparities in following good governance principles (Ziosi and Pruss, 2024). In turn, the global focus on responsible AI governance models, based on the principles of transparency, humanity, and constant review of ethical implications, is observed (Batool et al., 2023).

The experience of these countries can be of great use to Nigeria. To begin with, AI will boost intelligence activities and predictability and improve responsiveness to insurgency, banditry, and cyber threats (Allen and Chan, 2017). Second, AI integration should be supported by strong governance structures to implement transparency, accountability, and ethical practices (Ziosi & Pruss, 2024). Finally, technological capabilities should be transformed into effective national security governance through capacity building and institutional preparedness (Cummings, 2017). These observations can be used as a way of comprehending how the implementation of AI can be streamlined in the Nigerian security realm in alignment with the principles of good governance.

Nigeria's National Security Architecture and Governance Context

The national security system of Nigeria is an intricate system that has various actors with different but overlapping roles. The organization consists of the Nigerian Armed Forces, intelligence agencies, namely the Department of State Services (DSS) and the Nigeria Intelligence Agency (NIA), and law enforcement agencies, including the Nigeria Police Force (Awotayo et al., 2023). The agencies have the specific security threats within their remit, whereby an agency focuses on the insurgency, banditry, cybercrime, and transnational threats, but the variety of actors has traditionally created coordination issues (Bodunde and Balogun, 2018). According to The Cable (2025), the inter-agency communication inefficiency and the lack of intelligence exchange frequently undermine their responsiveness in terms of detection of threats in a timely manner and responsiveness in operations, as a result of which integrative frameworks are needed.

The current policies show an increasing understanding of the role of technology in improving the security outcomes. The National Security Strategy and other ongoing efforts of Nigeria support the deployment of contemporary information and communication technologies (ICTs), predictive analytics, and intelligence gathering grounded in data as a way of enhancing situational awareness and decision-making (Ibekwe, 2025). Remarkably, the method of cyber defense and digital intelligence has been slowly institutionalized to enhance national resilience to both traditional and emerging threats.

Nevertheless, despite these policy initiatives, there are still a lot of challenges when it comes to the integration of technology in operation. The lack of coordination among agencies hinders the smooth transfer of actionable intelligence, and the lack of technological ability and unequal use of digital resources is a hindrance to efficiency (Awotayo et al., 2023). Moreover, the problem of standardization, resource distribution, and ethical management of the implementation of AI and advanced analytics are not elaborated, limiting the potential usefulness of technology-based solutions (Bodunde and Balogun, 2018). According to The Cable (2025), it is important to note that intelligence synergy and a culture of collaboration are the necessary preconditions to effective AI adoption in the national security system of Nigeria.

The Potential Decision Implications of AI Integration for Good Governance

The use of Artificial Intelligence (AI) in the operations of the national security offers certain prospects for the improvement of good governance in Nigeria. The artificial intelligence-based tools may be used to make better decisions based on predictive analytics, situational awareness in real-time, and automated threat evaluation so that security organizations can act in advance of insurgency, banditry, and cyber attacks (Papagiannidis et al., 2025). Various data can be combined to create predictive intelligence tools, which can address accuracy and timeliness of operational decisions to minimize the chance of human errors and resource waste (Batool et al., 2023). These abilities will support the efficiency of the security apparatus in Nigeria and at the same time enhance governance goals that focus on efficiency, responsiveness, and accountability.

Governance issues such as transparency and accountability are very important in the adoption of AI. Systems to deliver explainable outputs have the potential to improve the perceived legitimacy of security decisions, enabling policymakers, civil society, and oversight groups to assess objectively operational actions (de Fine Licht, 2020). Integrating ethical risk management systems can make sure that AI tools are used within legal, moral, and social standards and that chances of violating human rights or discrimination are minimized. This is in line with the democratic ideal because it provides control mechanisms and enhances the trust that people have towards the advanced technologies as uses of national security (Papagiannidis et al., 2025).

Risks, Challenges, and Policy Considerations

The application of AI to the Nigeria national security system suggests a number of dangers and operational issues. The vulnerability to cybersecurity is still one of the paramount issues of concern because AI systems are vulnerable to adversarial attacks, data poisoning, and cybercriminals, which may compromise intelligence accuracy and national security activities (Brundage et al., 2018; Ferrag et al., 2025). This reliance on quality and stable data also makes the implementation of AI more difficult since unreliable or unfair data may lead to inaccurate predictive results and malfunctioning decisions. In addition, the use of foreign AI technologies provides issues of strategic independence, possible backdoors, and compatibility of imported systems with domestic security priorities (Reddick et al., 2015).

In adopting AI, ethical predicaments are as well imminent. Algorithm bias, transparency, and accountability questions indicate that automation and human control are in conflict, particularly when it comes to making a decision that may affect the rights and safety of citizens (Nikiforova et al., 2025). In the absence of proper governance mechanisms, AI applications will become a threat to strengthen inequities, undermine trust in the populace, and erode democratic control.

The integration of AI has to be responsible and should therefore be in policy consideration. The Nigeria Data Protection Act (NDPC, 2023) needs to be regulated by ensuring it complies with all the data protection regulations, sets data quality standards, and institutes ethical review procedures in the security systems of AI. Nigeria can reduce the risks of AI deployment by focusing on technical vulnerabilities, data governance issues, and ethical aspects and enhance its security governance framework.

Empirical Review

Chinagorom et al. (2025) examined Artificial intelligence and counter-terrorism in Nigeria with focus on prospects, pitfalls, and the future of security strategy. The study engaged the collective security theory and adopted qualitative research design, relying on secondary data to analyze the effectiveness and limitations of AI deployment. Findings that emanated reveal that inadequate infrastructure, limited technical expertise, weak inter-agency collaboration, and concerns over AI-driven surveillance hinder its full implementation. The study submitted that structured AI adoption strategy supported by institutional reform, policy-driven investments, and international collaboration can significantly enhance Nigeria's counter-terrorism efforts. Study argued that to optimize AI's potential, the Nigerian government must prioritize investment in AI infrastructure, foster partnerships with global AI innovators, and institutionalize inter-agency collaboration through a centralized intelligence-sharing framework.

Donald (2025) interrogates the application of AI in intelligence gathering and national security management in Nigeria, with emphasis on its potential to transform security operations from reactive to proactive measures. The study deployed qualitative research design, relying on secondary data drawn from academic literature, policy documents, and security reports. Data were subjected to content and thematic analysis, while Rational Choice Theory was adopted as the theoretical framework to explain decision-making processes in the application of AI to security management. Results findings showed that AI enhances intelligence gathering and national security through real-time data analysis, automation of surveillance and reconnaissance, and predictive modeling of emerging threats. It also showed that AI facilitates advanced data analytics and strengthens security operations by improving the capacity to anticipate, prevent, and mitigate security incidents. The study concludes that AI holds significant potential of shifting from reactive approaches to proactive strategies, improve the efficiency of security responses and reduce vulnerability to complex threats, and that the Nigerian government should integrate AI into its national security framework by investing in technological infrastructure, capacity building, and inter-agency collaboration.

Ibekwe (2025) evaluates the role of credible intelligence in enhancing internal security operations in Nigeria as the country continues to experience serious security threats, including terrorism, insurgency, banditry, and kidnapping. The study also identifies key challenges facing intelligence operations, such as poor inter-agency

collaboration, lack of modern technology, limited funding, and low community trust. Through real-life examples and case studies, the study examined the benefits of intelligence led security efforts and the risks of faulty intelligence. The study concludes with recommendations to improve intelligence gathering and use, including creating a central coordination agency, involving communities more effectively, investing in technology, and strengthening international partnerships. These steps are necessary to build a safer and more secure Nigeria.

Onazi et al. (2025) assessed big data challenges, opportunities, and strategies on national security threats in Nigeria. The study employed a mixed-methods approach, the study integrates literature review, case studies, and government policy analysis to assess the effectiveness of big data analytics in intelligence gathering, surveillance, cybersecurity, and early threat detection. Emerging results from the study emphasised that while big data enhances predictive capabilities and situational awareness, challenges such as data privacy concerns, infrastructure deficits, and ethical dilemmas must be addressed. The study opine that strengthening legal frameworks, improving technical capacity, and fostering public-private partnerships to maximize the potential of big data in national security strategies. The implications suggest that a data-driven approach can significantly improve Nigeria's ability to respond proactively to emerging security threats while balancing privacy and civil liberties.

Jimoh and Adejobi (2026) interrogate Artificial Intelligence future of knowledge preservation and its implications for national security and strategic decision-making in Nigeria. Guided by the Knowledge Management Theory and Information Warfare Theory, the research adopts a qualitative approach, drawing on content analysis of policy documents, scholarly publications, and institutional reports from the Nigerian Defence Academy, NITDA, and global AI frameworks. Results reveal that while AI presents immense opportunities for improving intelligence analysis, data preservation, and evidence-based policy formulation, Nigeria faces critical challenges, including poor digital infrastructure, limited AI literacy, and weak policy coordination. The study underscores the urgent need for a National AI and Knowledge Preservation Policy to safeguard institutional memory, promote data sovereignty, and strengthen national resilience against emerging cyber and information threats. It concludes that integrating AI into Nigeria’s strategic systems can serve as a catalyst for sustainable national security, improved governance, and informed decision-making, provided that ethical, infrastructural, and policy frameworks are effectively implemented.

Theoretical Framework

The Digital Era Governance Theory

The Digital Era Governance (DEG) theory, as articulated by Dunleavy et al. (2006), provides a robust theoretical lens for examining the integration of Artificial Intelligence (AI) into Nigeria's national security architecture. DEG emerged as a critique of the fragmented and rigid New Public Management (NPM) models, advocating instead for the reintegration of government functions, the digitization of processes, and a holistic, needs-based approach to public administration (Dunleavy et al., 2006). The Nigerian national security is an environment characterized by siloed agencies, poor intelligence sharing, and bureaucratic inertia. DEG offers a framework for understanding how AI can serve as a transformative tool. The theory posits that AI is not merely a technological upgrade but a governance mechanism capable of restructuring how security agencies interact, share information, and respond to threats. DEG emphasis on digitization directly supports the study's core argument that AI can enhance transparency, accountability, and efficiency, which are the hallmarks of good governance in the digital age.

DEG's principle of reintegration is particularly instructive as reintegration involves reversing the fragmentation caused by NPM by bringing disparate government units back under a cohesive framework using digital means (Dunleavy et al., 2006). In Nigeria, agencies such as the Department of State Services (DSS), the Nigeria Police Force, the Nigeria Security and Civil Defence Corps (NSCDC), and the military often operate in isolation, leading to duplicated efforts and critical intelligence gaps (Awotayo et al., 2023). AI-powered platforms enable reintegration by creating centralized, real-time intelligence dashboards that allow for seamless data sharing and collaborative analysis. For instance, machine learning algorithms can aggregate data from various sources, identify patterns, and distribute actionable intelligence to all relevant agencies simultaneously, thereby breaking down the silos that have historically hampered national security efforts (Mishra, 2025). Through the DEG lens, AI becomes the digital glue that fosters a unified, rather than fragmented, security response.

DEG's focus on digitization processes and needs-based holism. Digitization involves moving from analog, paper-based systems to fully automated, data-driven operations (Dunleavy et al., 2006). Where threat detection often relies on reactive, human-led intelligence, the lag time between identifying a threat and responding to it can be fatal (Musa et al., 2024). Predictive analytics, powered by AI, digitizes this process by continuously scanning vast datasets from social media trends to satellite imagery to forecast potential security breaches before they occur (Allen & Chan, 2017). This aligns with DEG's needs-based holism, which argues that services should be organized around the citizen's needs (in this case, the need for safety) rather than bureaucratic convenience. By improving the timeliness of threat detection, AI ensures that

security operations are proactive and preventive, thereby fulfilling the study's second objective: to investigate the extent to which predictive analytics can enhance timeliness. DEG theory thus explains that timeliness is not just a technological metric but a governance outcome, as faster detection directly translates to more responsive and accountable security institutions.

Furthermore, DEG theory helps to narrate the risks and governance challenges associated with AI adoption, which are central to the study's overall aim of examining implications for good governance. While DEG is optimistic about the potential of digital tools to transform governance, it also implicitly acknowledges that digitization must be accompanied by robust institutional frameworks to ensure transparency and accountability (Dunleavy et al., 2006). In the Nigeria, the adoption of AI for inter-agency coordination and predictive analytics raises concerns about data privacy, algorithmic bias, and the digital divide between agencies (Bodunde & Balogun, 2018). For instance, if predictive analytics are trained on biased historical data, they may reinforce existing prejudices or target specific communities unfairly, undermining the democratic values that good governance seeks to protect (Ziosi & Pruss, 2024). DEG theory, therefore explains how AI can improve governance while also highlighting the need for oversight mechanisms such as regulatory compliance with the Nigeria Data Protection Act (NDPC, 2023) to ensure that digitization serves the public interest. This theoretical perspective reinforces the study's conclusion that AI is a tool that must be governed, not just deployed.

In conclusion, the Digital Era Governance theory offers a comprehensive framework for understanding the integration of AI into Nigeria's national security. By applying DEG's core principles of reintegration, digitization, and needs-based holism, this study demonstrates that AI has the potential to resolve long-standing coordination failures and significantly improve the timeliness of threat detection. However, DEG also serves as a cautionary framework, reminding researchers and policymakers that technological integration without corresponding institutional adaptation can lead to new forms of governance failure. As Nigeria navigates the complex intersection of technology and security, DEG provides both a roadmap for innovation and a checklist for accountability, ensuring that the pursuit of efficiency does not come at the expense of democratic principles. This theoretical underpinning strengthens the study's contribution to the fields of public administration, security studies, and digital governance, offering a model that may be applicable to other developing nations facing similar security challenges.

Methodology

The study adopts qualitative research design whit reliance on publicly available archive documents employed for the analysis. Secondary data were generated via journals publication and other documented materials relevant to the study with reliance on secondary data. The research is conducted by examining literature

concerning Integrating Artificial Intelligence into Nigeria's national security as an implication for good governance. Also, literature on Artificial Intelligence enhancing inter-agency coordination and AI predictive analytics in improving timeliness of threat detection in Nigeria's national security architecture were given attention. The literature was obtained through searches in publicly available material. Literature from non-serial publications, official reports, and conferences has been included particularly if they have been cited by other references.

Discussion of findings

The findings from this study reveal that the integration of Artificial Intelligence holds significant potential for enhancing inter-agency coordination within Nigeria's national security architecture, primarily through the creation of centralized intelligence-sharing platforms and real-time data fusion capabilities. This aligns with the Digital Era Governance theory's principle of reintegration, which advocates for using digital tools to unify fragmented government functions (Dunleavy et al., 2006). The empirical evidence reviewed supports this theoretical assertion. Chinagorom et al. (2025) found that weak inter-agency collaboration remains a critical hindrance to AI deployment in Nigeria's counter-terrorism efforts, but they also submitted that institutionalizing inter-agency collaboration through a centralized intelligence-sharing framework is essential for optimizing AI's potential. Similarly, Donald (2025) concluded that AI facilitates advanced data analytics and strengthens security operations by improving inter-agency collaboration, thereby enhancing the capacity to anticipate and mitigate security incidents. Ibekwe (2025) further reinforced this by identifying poor inter-agency collaboration as a key challenge facing intelligence operations in Nigeria, recommending the creation of a central coordination agency to improve intelligence gathering and use. However, the findings also indicate that achieving this reintegration is not automatic. Awotayo et al. (2023) and Bodunde and Balogun (2018) empirically documented that Nigeria's security agencies such as the DSS, Nigeria Police Force, and military often operate in isolation due to trust deficits, bureaucratic rivalry, and unequal access to digital resources, which undermine the seamless data sharing required for AI-driven coordination. Therefore, while AI offers the technological mechanism for enhanced coordination through platforms like real-time intelligence dashboards (Mishra, 2025), the study finds that its effectiveness is contingent upon concurrent institutional reforms that foster a culture of collaboration and data sharing among agencies.

The findings further demonstrate that predictive analytics, powered by AI, can substantially improve the timeliness of threat detection in Nigeria's national security operations by enabling a shift from reactive, human-led intelligence to proactive, data-driven forecasting. This finding is theoretically grounded in DEG's digitization principle, which emphasizes moving from analogue, slow processes to automated, real-time operations (Dunleavy et al., 2006), and its needs-based holism, which prioritizes citizen safety over bureaucratic convenience. The empirical literature provides substantial support for this claim. Allen and Chan

(2017) and Cummings (2017) established that AI systems in developed nations use predictive analytics to forecast terrorist activities by analysing vast datasets, significantly reducing response times. In the Nigerian context, Donald (2025) found that AI enhances intelligence gathering through real-time data analysis and predictive modelling of emerging threats, thereby shifting security approaches from reactive to proactive and improving the efficiency of responses. Onazi et al. (2025) similarly emphasized that big data analytics enhances predictive capabilities and situational awareness, enabling Nigeria to respond proactively to emerging security threats. Jimoh and Adejobi (2026) also revealed that AI presents immense opportunities for improving intelligence analysis and evidence-based policy formulation, which directly contributes to faster threat detection. However, the findings also reveal significant limitations. Musa et al. (2024) documented that Nigeria's counter-terrorism strategy remains entrenched in conventional tactics that are often slow, while Chinagorom et al. (2025) identified inadequate infrastructure and limited technical expertise as barriers to full AI implementation. Furthermore, Brundage et al. (2018) and Ferrag et al. (2025) warned that AI systems are vulnerable to data poisoning and cyberattacks, which can compromise the accuracy of predictive analytics. Thus, while predictive analytics offers a clear pathway to improved timeliness as theorized by DEG and evidenced by multiple Nigerian studies the extent of this improvement is moderated by institutional capacity, data quality, and the robustness of cybersecurity measures. The study finds that without addressing these infrastructural and technical deficits, the timeliness gains from predictive analytics will remain largely unrealized.

Conclusion

This paper has explored the ramifications of the implementation of artificial intelligence in the national security setting of Nigeria under the premise of good governance. The results indicate that AI can be of great benefit in the context of decision-making, predictive intelligence, and transparency and accountability of security operations (Papagiannidis et al., 2025; Batool et al., 2023). AI can help make the process of governance more efficient and responsive, automate threat detection, and implement data-driven strategies, which in turn can help build trust in the populace and democratic checks and balances.

Nonetheless, AI is not a replacement for human leadership but a tool. The vulnerabilities of the system to cybersecurity, algorithmic bias, ethical implications, and reliance on foreign technologies present arguments about the need to have strong governance structures, regulatory controls, and capacity-building efforts (Brundage et al., 2018; NDPC, 2023). The use of national AI security policies and the creation of institutions to oversee this are of utmost importance in order to ensure that AI improves and does not dilute good governance.

Recommendations

Based on the foregoing, the study hereby recommends that

i. Nigerian government establish a centralized intelligence fusion centre where all security agencies can share real-time information using AI-driven platforms. This will break down the silos that currently exist between agencies like the DSS, police, and military, ensuring that intelligence flows seamlessly and collaboratively. To support this, a national AI security policy should be developed to set clear rules and standards for how these technologies are used, along with an independent body to oversee compliance and ensure accountability. Security personnel must also receive regular training to understand how AI works, its limitations, and how to work alongside it effectively, so that human judgment and technology complement each other in decision-making.

ii. That Nigeria government including regional and State Government should invest heavily in modern technological infrastructure such as high-speed internet, data centres, and secure databases to support real-time data analysis. This will enable security agencies to move from reacting to attacks after they happen to predicting and preventing them before they occur. Strong data protection laws must be put in place to guard citizens' privacy and prevent algorithmic bias that could lead to unfair targeting of certain groups. Partnering with private technology companies can also bring in the needed expertise and innovation, while ensuring that all AI tools are designed with transparency and ethical considerations in mind. These steps will help Nigeria harness the full potential of AI to detect threats faster while maintaining public trust and democratic values.

References

Accord. (2022). *Banditry in Nigeria: Insights from situational action and situational crime prevention theories*. Retrieved January 7, 2026, from https://www.accord.org.za/conflict-trends/banditry-in-nigeria-insights-from-situational-action-and-situational-crime-prevention-theories/

Adishi, E., Abdulaziz, B., Aaron, A., & Kape, G. (2022). Intelligence and national security in Nigeria democratic governance 1999–2020. *Indiana Journal of Multidisciplinary Research, 2*(2), 11–26.

Allen, G., & Chan, T. (2017). *Artificial intelligence and national security* (Vol. 132). Cambridge, MA: Belfer Center for Science and International Affairs.

Andrus, M., & Villeneuve, S. (2022). Demographic-reliant algorithmic fairness: Characterizing the risks of demographic data collection in the pursuit of fairness. In *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency*, 1709–1721.

Awotayo, O. O., Omitola, A., Omitola, B., & Oderinde, S. L. (2023). Intelligence system and national security in Nigeria: The challenges of data gathering. *Janus, 14*(2).

Batool, A., Zowghi, D., & Bano, M. (2023). Responsible AI governance: A systematic literature review. *arXiv preprint arXiv:2401.10896.*

Bodunde, D. O., & Balogun, N. O. (2018). Intelligence sharing: The challenges among the Nigerian security agencies and government. *African Journal of Stability and Development, 11*(2), 481–493.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., … Anderson, H. (2018). *The malicious use of artificial intelligence: Forecasting, prevention, and mitigation*. arXiv preprint arXiv:1802.07228.

Chinagorom, A. E., Alpheaus Chika, J., & Charity, N. (2025). Artificial intelligence and counter-terrorism in Nigeria: Prospects, pitfalls, and the future of security strategy. *Jalingo Journal of Social and Management Sciences*, *6*(3), 154-165.

Cummings, M. (2017). *Artificial intelligence and the future of warfare.* London, England: Chatham House.

de Fine Licht, K., & de Fine Licht, J. (2020). Artificial intelligence, transparency, and public decision-making: Why explanations are key when trying to produce perceived legitimacy. *AI & Society, 35*(4), 917–926.

Donald, D., Aisha, M., & Imam, A. S. (2025). Role of Artificial Intelligence (AI) in intelligence gathering and management of Nigeria National Security. *International Journal of Sub-Saharan African Research*, *3*(3), 206-225.

Dunleavy, P., Margetts, H., Bastow, S., & Tinkler, J. (2006). *Digital era governance: IT corporations, the state, and e-government*. Oxford University Press.

Horowitz, M. C. (2018). Artificial intelligence, international competition, and the balance of power.

Ibekwe, E. O. (2025). Role of credible intelligence in enhancing internal security operations in Nigeria: A critical analysis. *African Journal of Social and Behavioural Sciences, 15*(4), 1933–1950.

Jimoh, O. I., & Adejobi, A. O. (2026). Artificial Intelligence and the future of knowledge preservation: Implications for national security and strategic decision-making in Nigeria. *Center of Artificial Intelligence*, *1*(1). https://doi.org/10.65591/5vr5e142

Mishra, P. (2025). *Strategic intelligence: Artificial intelligence, cyber defense, and security in the digital age.* Deep Science Publishing.

Musa, A. U., Mukhtar, J., Adamu, A. D., & Raula, A. D. (2024). An evaluation of the security challenges confronting Nigeria. *Gusau Journal of Sociology, 4*(2), 318–325.

Nigeria Data Protection Commission. (2023). *Nigeria Data Protection Act 2023*. NDPC.

Nikiforova, A., Lnenicka, M., Melin, U., Valle-Cruz, D., Gill, A., Flores, C. C., … Tesarova, B. (2025). Responsible AI adoption in the public sector: A data-centric taxonomy of AI adoption challenges. *arXiv preprint arXiv:2510.09634.*

Onazi, S. O., Olanrewaju, R. F., & Aimufua, G. (2025). Big Data and National Security Threats in Nigeria: Challenges, Opportunities, and Strategies.

Papagiannidis, E., Mikalef, P., & Conboy, K. (2025). Responsible artificial intelligence governance: A review and research framework. *Journal of Strategic Information Systems, 34*(2), 101885.

Reddick, C. G., Chatfield, A. T., & Jaramillo, P. A. (2015). Public opinion on National Security Agency surveillance programs. *Government Information Quarterly, 32*(2), 129–141.

The Cable. (2025). Intelligence synergy: Reshaping Nigeria's security architecture. Retrieved January 8, 2026, from https://www.thecable.ng/intelligence-synergy-reshaping-nigerias-security-architecture

Ziosi, M., & Pruss, D. (2024). Evidence of what, for whom? The socially contested role of algorithmic bias in a predictive policing tool. In *Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency* (pp. 1596–1608).