International Journal of Sub-Saharan African Research (IJSSAR)
Vol. 3, Issue 3, pp. 206-225, September 2025, ISSN: 3043-4467 (Online), 3043-4459 (Print)
DOI:10.5281/zenodo.17252277

Role of Artificial Intelligence (AI) in Intelligence Gathering and Management of Nigeria National Security

[1]David Donald, [2]Mustapha Aisha & [3]Abubakar Sanusi Imam

[1]Rayhaan University, Birnin Kebbi, Nigeria
[2]Ahmadu Bello University, Zaria, Kaduna State, Nigeria
[3]Al-Qalam University, Katsina, Katsina State, Nigeria

[1]https://orcid.org/0009-0004-9446-6035
[2]https://orcid.org/0009-0000-3067-2711
[3]https://orcid.org/0009-0009-4410-0023

***Corresponding author:** donalddavidworld@gmail.com

ABSTRACT

Background: Artificial intelligence (AI) has emerged as a defining concept in contemporary security discourse, analysis, policy, and strategic thinking. It plays a central role in military and security operations, gaining strategic relevance as a critical tool for national defense and as an instrument for mitigating threats in a hostile security climate characterised by terrorism, cybercrime, maritime crimes, insurgency, and banditry. In Nigeria, where security threats have become increasingly sophisticated, technology-driven, and repetitive, conventional responses are proving inadequate in addressing the scale, scope, and frequency of incidents.
Objective: This study investigates 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.
Method: The study employed a 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 revealed 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.
Conclusion: The study concludes that AI holds significant potential to revolutionize intelligence gathering and national security management in Nigeria. By shifting from reactive approaches to proactive strategies, AI can improve the efficiency of security responses and reduce vulnerability to complex threats.

International Journal of Sub-Saharan African Research (IJSSAR)
Vol. 3, Issue 3, pp. 206-225, September 2025, ISSN: 3043-4467 (Online), 3043-4459 (Print)
DOI:10.5281/zenodo.17252277

Unique Contribution: This research contributes to the growing literature on AI in African security contexts, highlighting its capacity to reshape intelligence operations and address persistent gaps in Nigeria's security architecture.

Key Recommendation: The Nigerian government should integrate AI into its national security framework by investing in technological infrastructure, capacity building, and inter-agency collaboration. Policy should prioritise the ethical use of AI, while addressing root causes of insecurity such as poverty and poor governance to ensure that technological adoption produces sustainable outcomes.

Keywords: Artificial Intelligence, National Security, Security, Nigeria Intelligence Community

INTRODUCTION

The Nigerian security environment has over time, seen a steady spike in threats and existential threats to national security and defensive capabilities. Insurrection, terrorism, banditry, maritime crime, farmer-herder conflict, cybercrime, and cultism have consistently weakened the security of the nation by grossly undermining safety, economic prosperity, food security, and development. The fight against these threats to Nigerian security and strategic geopolitical positions has assumed a destructive dimension, with the Nigerian security architecture seemingly unable to enforce its superiority to detect, deter, and neutralize these criminal enterprises. The complexities of these threats, the poor intelligence gathering, especially in the management of a large swath of poorly governed land mass in Northern Nigeria, the porous border control, and the sheer absence of technology in the management of its border with its neighbors have further worsened the precarious security landscape.

A report from SBM Intelligence (strategic intelligence firm) underscored that between July 2022 and June 2023, 3,620 people were abducted in 582 kidnap-related incidents in Nigeria, and at least N5 billion ($6,410,256 as of 30 June 2023) were reported as ransom demands, while verified ransom payouts amounted to N302 million ($387,179), or six percent of what was demanded. The escalating farmer-herder conflict in Nigeria, which has led to over 10,000 deaths since 2011, reflects a critical intelligence failure in effectively predicting, preventing, and mediating violence due to inadequate early warning systems and conflict resolution mechanisms (International Crisis Group, 2024). The Gulf of Guinea has become a global hotspot for piracy and maritime crime, with over 130 attacks reported in 2020 alone (International Maritime Bureau, 2021). Despite efforts by the Nigerian Navy and regional bodies, there is evidence of insufficient coordination and poor maritime surveillance capabilities, leaving vast coastal areas vulnerable.

Nigeria loses an estimated 400,000 barrels of crude oil daily to theft (according to the Nigeria Extractive Industries Transparency Initiative, NEITI). This ongoing problem reveals weaknesses in both the physical security of oil infrastructure and intelligence regarding illegal smuggling

International Journal of Sub-Saharan African Research (IJSSAR)
Vol. 3, Issue 3, pp. 206-225, September 2025, ISSN: 3043-4467 (Online), 3043-4459 (Print)
DOI:10.5281/zenodo.17252277

networks. Efforts to combat this, such as Operation Delta Safe, have had limited success due to corruption, underfunding, and lack of intelligence integration.

The complexity and scale of these threats have put immense pressure on the nation's security apparatus, which often struggles with intelligence gathering, processing, and response. Traditional methods of intelligence gathering, such as human intelligence (HUMINT), signals intelligence (SIGINT), electronic intelligence (ELINT), and technical intelligence (TECHINT), have proven inadequate in handling the volume and sophistication of data needed to counter these security threats effectively.

According to Okoli and Iortyer (2014), one of the major issues undermining Nigeria's prospect of thwarting these plethoras of threats, traditional and emerging, is the slow processing of intelligence data, which delays response times and weakens the security agencies' ability to predict or prevent attacks. This is where artificial intelligence (AI) becomes essential.

AI technologies, particularly in the areas of data analytics, machine learning, and automated surveillance, can provide the speed and precision necessary to process vast amounts of data in real time. The future of intelligence gathering is inextricably linked to AI, ML (machine learning), and automation. In an era of exponentially growing volumes of data, the Nigerian intelligence community, like other intelligence communities, has to holistically leverage an advanced level of AI maturity or risk obsolescence and irrelevance—potentially on a short timeline. This is because AI-driven systems have hugely revolutionized security thinking and operational capabilities by enhancing automotive machine tasks, reinforcing predictive analytics, and having decision-making (Ugochukwu 2022, Willie 2024, Unalp 2024). In this regard, AI can address some of the core challenges currently facing Nigeria's national security landscape. Recent empirical evidence from Nigeria highlights the limitations of current intelligence-gathering methods. Security agencies are dwarfed by the technological capacity to effectively monitor and counter numerous threats, revealing the critical need for advanced AI systems capable of detecting and neutralizing digital security threats in real time. Additionally, the increasing cybercrime wave in Nigeria, often attributed to organized crime networks, further emphasizes the need for AI-driven intelligence (Ikechukwu et. al 2024).

While much research has examined Nigeria’s insecurity, little attention has been given to the role of artificial intelligence in strengthening intelligence gathering. This study therefore aims to assess weaknesses in current systems, explore how AI can improve intelligence processes, address challenges and ethical concerns, and propose ways to integrate AI into Nigeria’s security framework.

International Journal of Sub-Saharan African Research (IJSSAR)
Vol. 3, Issue 3, pp. 206-225, September 2025, ISSN: 3043-4467 (Online), 3043-4459 (Print)
DOI:10.5281/zenodo.17252277

CONCEPTUAL REVIEW

Artificial Intelligence (AI)

According to the National Information Technology Development Agency (2021), AI is a technology that enables machines to perform tasks that would normally require human intelligence, including learning from data, making decisions, and recognizing patterns. This definition focuses on AI's role in automating tasks and decision-making processes.

The diverse and complex research in the field of AI makes it quite difficult to project a universal definition. One of the earliest definitions came in 1956, the year AI was discovered as an acceptable field of science when John McCarthy defined the term as the development and use of machines to execute tasks that usually require human intelligence (Hoadley & Lucas, 2018). Artificial Intelligence, broadly speaking, may be defined as a branch of computer science that investigates and develops computational approaches and techniques that allow machines to perform tasks that would normally require some level of human intelligence. In other words, it makes machines intelligent (Russell & Norvig, 2021). Similarly, El-Had (2023) conceived AI as the branch of computer science dealing with the reproduction or mimicking of human-level intelligence, self-awareness, knowledge, and thought in computer programs. Looking at all these conceptual clarifications and descriptions of AI, one repeated attribute is that AI aims to develop human-level intelligence in machines. The European Commission (2018) defined AI as systems that display intentional behavior through the analysis of their environment and take specific actions, with some degree of autonomy to achieve specified goals.

The US Congressional Research Services (2020) has operationally conceived AI as an artificial system that performs tasks under different degrees and unpredictable exigencies without significant human presence, or that can learn from experience and improve performance when exposed to information. Artificial systems developed in computer software, physical hardware, or other contexts that solve tasks requiring human-like perception, cognition, planning, learning, communication, or physical action. An artificial system designed to think or act like a human, including cognitive architectures and neural networks.

An artificial system designed to act rationally, including an intelligent software agent or embodied robot that actualizes goals using perception, planning, reasoning, learning, communicating, decision-making, and acting. Essentially, what appears quite central in all these definitions is that: artificial intelligence is a system that thinks like humans, thinks rationally and acts rationally.

International Journal of Sub-Saharan African Research (IJSSAR)
Vol. 3, Issue 3, pp. 206-225, September 2025, ISSN: 3043-4467 (Online), 3043-4459 (Print)
DOI:10.5281/zenodo.17252277

Security

Security as a concept, suggests freedom from all forms of dangers, threats of danger, and anxiety. Security, ultimately, demonstrates a sense of safety from harm, fear, forces of subjugation, oppression, lack, despair and illiteracy. It denotes the protection and preservation of core values and threats to those values. It involves deliberate and committed efforts aimed at eliminating all forms of threats to survival and means of survival. It is in this light that Williams (2008) sees security as the alleviation of threats to cherished values.

Buzan (1991) also conceives security from two broad lenses. In one of the lenses, he sees security to mean the pursuit of freedom from threat and the ability of states and societies to maintain their independent identity and their functional integrity against forces of change that they see as hostile. . He further emphasizes that the bottom line of security is survival, but it also reasonably includes a significant range of worries about the conditions of existence. In the words of Imobighe (2003), security has to do with freedom from danger or threats to a nation's ability to protect and develop itself, promote its cherished values and legitimate interests, and enhance the well-being of its people. Thus, according to Omoleye & Filani (2019), internal security could be seen as the freedom from oreal timeence of those tendencies, that could undermine internal cohesion, the corporate existence of a country, and its ability to maintain its vital institutions for the promotion of its core values and socio-political and economic objectives, as well as meet the legitimate aspirations of the people.

Mbachu and Yesufu (2011), stressed that strategically, security has objective and subjective meanings. Objectively, it measures the absence of threat to life, liberty, property, and core values; and subjectively measures the absence of fear anxiety, tension, or apprehension of being in danger of losing life, liberty, and property and care values.

Schaefer (1989) cited in Mbachu (2011), defined security as the total of actions and measures, including legislative and operational procedures adopted to ensure peace, stability, and general well-being of a nation and its citizens.

It is fundamentally important to state that human security occupies a central position in recent security discourse. In the post-Cold War era, where threats and open confrontation between states have steadily decreased, attention has been shifted to internal threats emanating from groups with sinister intentions, struggling to amass economic advantage to their members. Consequently, security has now been viewed from the lens of the human being. Human security is conceived as the ability to protect the vital core value of all human lives in such a way that it enhances human freedoms and human fulfillment. Edekobi (2018) noted that human security means protecting fundamental freedoms that are the essence of life. It means protecting people from serious and persistent threats and situations. Also, means using processes that build on people's strengths and aspirations. It means creating political, social, environmental, economic, military, and cultural systems that together give people the building blocks of survival,

International Journal of Sub-Saharan African Research (IJSSAR)
Vol. 3, Issue 3, pp. 206-225, September 2025, ISSN: 3043-4467 (Online), 3043-4459 (Print)
DOI:10.5281/zenodo.17252277

livelihood, and dignity. From the aforementioned, it is important therefore to assert that there are layers to human security which include:

Political security concerns access to the organizational stability of states, systems of government, and the ideologies that give them legitimacy. Economic security concerns access to the resources finance and markets necessary to sustain acceptable levels of welfare and state power. Society security concerns the ability of societies to reproduce their traditional patterns of language culture, association, and religious and national identity and customs within acceptable conditions for evolution. Environmental security concerns the maintenance of the local and planetary biosphere as the essential support system on which all other human enterprise depends. These five sectors do not operate in isolation from each other. Each defines a focal point within the security problematique, and a way of ordering priorities, but all are woven together in a strong web of linkage (Buzan 1991).

National Security

The concept of national security has often been taken to merely connote the preservation of sovereignty, territorial integrity, and internal stability with a focus on the coercive power of the state. The concept of national security has often been taken to merely connote the preservation of sovereignty, territorial integrity, and internal stability with a focus on the coercive power of the state.

Defining the Concept of National Security, Lippmann (1943), posited that a nation has security when it does not have to sacrifice is it legitimate interest to avoid war and is able, if challenged, to maintain it by war.

Katzenstein (1996), posited that national security is the state of being free from external physical threats. Katzenstein argued that all moral and intellectual dangers should be considered, but it is physical violence that is widely regarded as the ultimate leverage against the state, and thus, as a real and tangible threat to its survival. However, if nations were not concerned with the defense of their values other than their survival as sovereign states, they would not have to be concerned about their security as much as they do now. Robert McNamara, the former US Secretary of State offers a more plausible conception of the concept of security, vis a vis national security. To him, security is not military hardware, though it may include it; security is not military force though it may encompass it, security is development, and without development, there is no security.

Intelligence

Intelligence in security, is a clear-cut strategy deliberately designed and developed by security apparatus to access and exhume privileged information from the opposite camp via infiltration, espionage, planting cameras, hacking, etc. with the overriding purpose to outsmart and forestall

International Journal of Sub-Saharan African Research (IJSSAR)
Vol. 3, Issue 3, pp. 206-225, September 2025, ISSN: 3043-4467 (Online), 3043-4459 (Print)
DOI:10.5281/zenodo.17252277

security glitches which would affect negatively the safety, health, welfare and socio-economic development of a nation (Enyia, et al 2022).

In another perspective, Lowenthal (1999) conceived intelligence as the process by which specific types of information important to national security are requested, collected, analyzed, and provided to policy makers; the products of that process; the safeguarding of these processes and this information by counterintelligence activities; and the carrying out of operations as requested by lawful authorities.The important components involved in the intelligence gathering are well imbued in the concept, which is collected, analysed and utilized in the processing of information. Here, the effective analysis of raw information, bearing in mind its validity and reliabilit, that leads to the conclusion,which is intelligence. Ultimately, without rigorous analysis of raw facts generated, there cannot be intelligence.

To Ngboawaji (2013), the term intelligence here also refer to the organization that is primarily involved in the chain of activities in the processing of Information, beyond the organization level, intelligence is described in the concept as a profession that carries out certain activities such intelligence activities. The tri-dimensional feature of this concept of intelligence provided a broad perspective in dealing with every aspect of intelligence as it relates to military.

According to Ayodele and Musa (2023), intelligence refers to the systematic process of gathering, analyzing, and interpreting information about internal and external threats to national security, aimed at supporting strategic decision-making that will thwart any act of aggression that threatens stability of the state.

THEORETICAL FRAMEWORK

Theoretically, the research employ the Rational Choice Theory, to better demonstrate the remarkable growth of artificial intelligence and its impact on national security strategy. Rational choice, according to Wittek (2013) is an umbrella term for a variety of models, explaining social phenomena as outcomes of individual action that can in some way, be construed as rational. Rational behavior is suitable for the realization of stated goals, given the constraints imposed by the situation. The theory of rational choice posits that given several options, a rational actor will choose the option that tends to maximize his utility (Becker, 1976; Hedström and Stern, 2008; Lohmann, 2008; Grüne-Yanoff, 2012). Witteck (2013) contended that the key elements of all rational choice explanations are individual preferences, beliefs, and constraints. The preference here denotes the positive or negative evaluations individuals attach to the possible outcomes of their actions. Preferences can have many roots, ranging from political goals, public policy, military action, defense strategy, or weapon deployment. Elster (1989) highlighted the prominence of rational choice theory when he said that when faced with several courses of action, people usually do what they believe is likely to have the best overall outcome. This theory assumes several factors and these include the fact that the decision maker has all the information that he can use to generate several options. In addition, he can be able to construct

International Journal of Sub-Saharan African Research (IJSSAR)
Vol. 3, Issue 3, pp. 206-225, September 2025, ISSN: 3043-4467 (Online), 3043-4459 (Print)
DOI:10.5281/zenodo.17252277

all options as well as calculate the resulting utility for each option. What this entails essentially, is that decision-makers decide on outcomes with the lowest possible cost.

Key Assumptions

Three assumptions are made within the framework of the rational choice theory: (1) individuals have selfish preferences, (2) individuals maximize their utility; and (3) they act independently based on full information.

Usefulness

Rational choice theory is fundamentally proving instrumental in explaining the competition in artificial intelligence and the expected utility in security management and intelligence gathering. Militaries around the world are investing enormous sums in the development, adoption and deployment of AI capabilities. Against the backdrop of great power rivalry and a changing multipolar order, AI has emerged as a particular focus of competition. Prominently, artificial intelligence offers credible utility in counter terrorist operations. AI allows seemingly swift actions by checkmating movement and financial transactions. AI tools allow decision-makers to evaluate the costs of inaction (e.g., increased casualties) against the benefits of preemptive actions (e.g., thwarting attacks). AI systems can identify potential terror cells by analyzing geospatial data. RCT can then help agencies allocate limited resources, such as deploying troops in areas where the probability of an attack is highest that is, through incorporating more robotics and autonomous systems into their forces, electromagnetic spectrum dominance, tactics, command-control, which will accelerate data analysis and quick responses that will eclipse human ability.

AI-enhanced intelligence gathering tools for such as drones and facial recognition software, provide actionable intelligence. RCT ensures these tools are deployed where the perceived benefits (reducing incidents) outweigh the operational costs, especially as Nigeria grapples with resource scarcity which hinders the operational success of the Nigerian intelligence community. Nigeria's porous borders allow the influx of illegal arms and contraband.

AI-enabled border surveillance systems, such as automated drones and motion detectors, can monitor illicit activities. Rational Choice Theory ensures the deployment of these technologies by prioritizing areas with the highest smuggling risks in border towns with Chad, Cameroon, Niger, Benin Republic and the Gulf of Guinea.

AI can enhance the effective management of national security by facilitating intelligence gathering. AI significantly enhances intelligence gathering methods like Human Intelligence (HUMINT), Signals Intelligence (SIGINT), and Technical Intelligence (TECHINT) by automating processes, improving analysis, and enabling real-time decision-making. This is capable of enhancing the efficiency of the Nigerian intelligence community, which will facilitate threat perception and response to perceive threats within the Nigerian geostrategic landscape. It

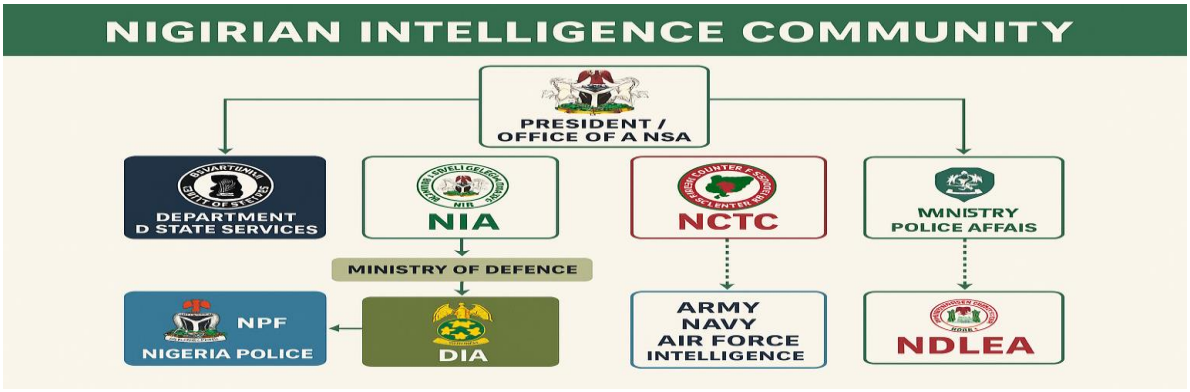
International Journal of Sub-Saharan African Research (IJSSAR)
Vol. 3, Issue 3, pp. 206-225, September 2025, ISSN: 3043-4467 (Online), 3043-4459 (Print)
DOI:10.5281/zenodo.17252277

is as Allen & Gregory (2020) observed, that AI can be incorporated into a range of semi-autonomous and autonomous vehicles, including ground vehicles, naval vessels, fighter aircraft, and drones. AI technologies in this space are used to perceive and map the environment, fuse sensor data, identify obstacles, plan navigation, and communicate with other vehicles (Center for Security and Emerging Technology, 2020).

Nigeria with her unprecedented security Imbroglio can ultimately derive utility and positive outcome in her fight against the challenges of terrorism, banditry, farmer-herder conflict, maritime crimes, secession, and other emerging threats.

Nigerian Intelligence Community

Nigerian intelligence gathering involves a multifaceted approach that combines traditional espionage techniques with modern technology to ensure national security and address a range of internal and external threats. The country's intelligence framework includes several key agencies: the Department of State Services (DSS), the National Intelligence Agency (NIA), the Defence Intelligence Agency (DIA), and the Force Intelligence Bureau (FIB). Each of these agencies plays a crucial role in Nigeria's security architecture, employing various methods and technologies to achieve their objectives. Despite their importance, these agencies face significant challenges such as inadequate funding, inter-agency rivalry, and political interference (Johnson, 2020).



I. Department of State Services (DSS)

Established in 1986 as the successor to the National Security Organization (NSO), the DSS is tasked with internal security and counterintelligence operations within Nigeria (Musa, 2021). Its main responsibilities are within the country and include counter-intelligence, medical intelligence, economic intelligence, internal security, counter-terrorism, and surveillance as well as investigating some other types of serious crimes against the state. It is also charged with the protection of senior government officials, particularly the President, Vice President, state governors and visiting heads of states and governments with their respective families.The DSS

International Journal of Sub-Saharan African Research (IJSSAR)
Vol. 3, Issue 3, pp. 206-225, September 2025, ISSN: 3043-4467 (Online), 3043-4459 (Print)
DOI:10.5281/zenodo.17252277

employs a range of methods, including human intelligence (HUMINT), which involves using a network of informants and undercover agents to gather actionable information (Ayodele & Musa, 2024). The agency also utilizes advanced technical surveillance systems to monitor and counter potential threats. Historically, the DSS has played a critical role in Nigeria's internal security landscape, notably in combating threats to national security. For instance, it has been involved in efforts to disrupt ISWAP and Boko Haram's operational capabilities and prevent terrorist attacks, banditry, and organized crimes. Despite these successes, the DSS has faced criticisms for human rights abuses and political bias, often being accused of serving political interests rather than purely national security (Eme & Anyadike, 2019).

II. National Intelligence Agency (NIA)

The NIA, founded in 1986, is responsible for collecting and analyzing foreign intelligence. Its activities include gathering information on external threats, international espionage, and diplomatic intelligence (Adejoh and Shimawua, 2018). The NIA operates through Nigerian diplomatic missions, high commissioners, and embassies abroad, leveraging international partnerships to collect relevant intelligence. The NIA's role has been pivotal in monitoring foreign threats and espionage activities. It has been involved in countering espionage activities from rival nations and safeguarding Nigeria's diplomatic interests.

III. Defence Intelligence Agency (DIA):

The DIA, established in 1999, focuses on military intelligence and provides crucial support to the Nigerian Armed Forces. Its responsibilities include gathering and analyzing information related to defense and security threats, both internal and external (Oghi and Unumen, 2014). The DIA plays a vital role in countering insurgent groups such as Boko Haram, bandit, piracy, pipeline vandals and other militant organizations, providing actionable intelligence to support military operations. Despite its importance, the DIA faces several challenges, including inter-agency cooperation issues, outdated equipment, and inadequate training. These challenges often impact the agency's effectiveness in addressing contemporary security threats (Moses, et al, 2020). Efforts to modernize the DIA's capabilities have been hampered by budgetary constraints and bureaucratic hurdles.

IV. Force Intelligence Bureau (FIB):

The FIB is part of the Nigerian Police Force and is tasked with providing intelligence on crime and national security. It focuses on gathering, evaluating, and disseminating criminal intelligence, particularly related to organized crime (Abdallah 2024). The FIB employs traditional policing methods, informants, and digital forensics to combat criminal activities.The FIB's role in addressing organized crime and ensuring public safety is crucial, but the agency often struggles with challenges such as inadequate funding, limited technology, and corruption.These issues hinder its ability to effectively combat crime and gather intelligence.

International Journal of Sub-Saharan African Research (IJSSAR)
Vol. 3, Issue 3, pp. 206-225, September 2025, ISSN: 3043-4467 (Online), 3043-4459 (Print)
DOI:10.5281/zenodo.17252277

Intelligence Gathering Methods

Human Intelligence (HUMINT)

HUMINT involves gathering information from human sources, including undercover agents and informants. This method is essential for countering insurgency and organized crime in Nigeria. The effectiveness of HUMINT depends on the quality of agents and the reliability of information obtained (Adebimpe et al, 2024).

Signals Intelligence (SIGINT)

SIGINT involves intercepting and decrypting communications and electronic signals to obtain valuable information. It has been instrumental in monitoring terrorist communications and activities. However, SIGINT operations in Nigeria face challenges related to outdated technology and cybersecurity issues (Ayodele and Musa, 2024).

Cyber Intelligence

This method utilizes cyber capabilities to monitor online activities, combat cyber threats, and collect digital information. As cybercrime and online radicalization increase, Nigerian intelligence agencies have increasingly relied on cyber intelligence. However, the lack of advanced technical expertise and resources remains a significant challenge.

Technical Intelligence (TECHINT)

TECHINT uses advanced technologies such as drones, satellite imagery, and surveillance equipment to gather data. This method has enhanced Nigeria's ability to monitor insurgent activities and secure borders. Despite its advantages, TECHINT is often limited by access to cutting-edge technologies and inadequate training.

Artificial Intelligence and the Management of National Security

The role of Artificial Intelligence (AI) in the management of national security has become increasingly significant due to its ability to enhance intelligence gathering, decision-making, and operational efficiency in addressing complex security threats. In recent years, AI has revolutionized national security operations by improving surveillance, predictive analytics, and autonomous systems, proving instrumental in safeguarding nations against evolving challenges (Allen & Gregory, 2020). The following are some of the ways AI are used in the management of national security:

International Journal of Sub-Saharan African Research (IJSSAR)
Vol. 3, Issue 3, pp. 206-225, September 2025, ISSN: 3043-4467 (Online), 3043-4459 (Print)
DOI:10.5281/zenodo.17252277

Intelligence Gathering and Analysis

One of AI's most critical contributions to national security is its ability to process and analyze vast amounts of data from various sources. Through machine learning algorithms and natural language processing, AI can sift through social media data, satellite images, and other surveillance platforms to detect patterns and emerging threats. AI systems analyze large datasets in real-time, enabling security agencies to make informed decisions swiftly. For instance, in counter-terrorism operations, AI tools have been used to predict terrorist activities by analyzing data from multiple sources, improving the accuracy of threat assessments (Center for Security and Emerging Technology, 2020).

Autonomous Systems

Autonomous systems powered by AI — from unmanned aerial vehicles (UAVs) to autonomous naval vessels — are already integral to national security. These systems are capable of performing missions from reconnaissance to combat operations without direct human intervention. UAVs enabled with AI, for instance, are no longer just auxiliary support of ISR (intelligence, surveillance, reconnaissance) missions but a key player, making it possible to conduct 24/7 monitoring of borders, critical infrastructure, and conflict zones. In the affect this trend, the Center for Security and Emerging Technology (2020) highlights total army and security agencies the intelligence of analytical pattern in sensor data through these systems in real time.

Cybersecurity

The second key area is in the area of cybersecurity as AI can significantly complement intelligence in the security architecture of Nigeria. As Nigeria's dependence on digital infrastructures for its political, economic and security processes increases, AI could be deployed to protect such systems from cyber-attacks. AI-powered systems can monitor large volumes of network traffic in real-time, identifying unusual patterns and potential vulnerabilities. By leveraging machine learning algorithms, these systems can detect emerging threats, including malware, phishing, and ransomware, before they cause significant damage. This early detection capability is vital in a country where cyber-attacks on financial institutions, critical infrastructures, and government agencies are on the rise (Brundage et al., 2018).

Moreover, AI enables faster response times by automating the detection and response to cyber threats. Through AI, Nigerian security agencies can deploy real-time solutions to neutralize cyber threats, thereby minimizing the potential impact of an attack.

International Journal of Sub-Saharan African Research (IJSSAR)
Vol. 3, Issue 3, pp. 206-225, September 2025, ISSN: 3043-4467 (Online), 3043-4459 (Print)
DOI:10.5281/zenodo.17252277

Predictive Capabilities and Decision-Making

AI's predictive analytics capabilities have transformed strategic decision-making in national security. By analyzing historical data and current trends, AI models can provide forecasts on potential threats and help design countermeasures. In counter-terrorism, for example, predictive algorithms are used to forecast the likelihood of attacks, allowing security agencies to preemptively allocate resources and enhance preparedness (Boulanin & Verbruggen, 2017).

AI has been identified as a tool that could greatly enhance intelligence gathering to combat terrorism, banditry, and other security threats. Given the vast size and complexity of Nigeria's security landscape, AI could help analyze surveillance data from different sources, identify patterns of insurgency, and predict possible attack points (Okwor, 2022). The Nigerian Joint Intelligence Board has recognized AI's potential in addressing gaps in traditional intelligence methods, providing real-time actionable intelligence for security agencies.

Target Acquisition

AI significantly improves target acquisition by enabling faster and more accurate identification of potential threats. AI-driven systems can analyze data from multiple sensors, such as radar, infrared cameras, and UAVs, to detect, track, and classify targets in real-time. For instance, in military operations, AI helps identify enemy vehicles, drones, and personnel, providing instant intelligence for quicker decision-making (Allen & Gregory, 2020). Through machine learning algorithms, AI enhances the precision of target identification by filtering out false positives and focusing on relevant threats.

Maritime Security

AI is transforming maritime security by helping to monitor vast oceanic areas and detect illegal activities such as piracy, smuggling, and crude oil theft in the Gulf of Guinea. Autonomous systems and AI-powered surveillance systems enable real-time monitoring of maritime zones, tracking of vessels and ships which will adequately improve situational awareness for naval forces. These systems use AI to process satellite images, sensor data, and maritime traffic information, identifying suspicious patterns of activity. AI-enabled systems can predict routes used by smugglers and pirates by analyzing historical data and current conditions, allowing authorities to intercept threats before they occur (Boulanin & Verbruggen, 2017). These technologies have been effectively deployed in regions such as Southeast Asia and the Gulf of Guinea, where maritime crime is prevalent. In Nigeria, AI could be vital for securing its extensive coastline against piracy and oil theft, both of which are major concerns in its maritime domain.

International Journal of Sub-Saharan African Research (IJSSAR)
Vol. 3, Issue 3, pp. 206-225, September 2025, ISSN: 3043-4467 (Online), 3043-4459 (Print)
DOI:10.5281/zenodo.17252277

Border Management

AI is revolutionizing border management by enhancing surveillance, automating threat detection, and improving the efficiency of immigration control. AI technologies, including facial recognition, biometric systems, and drones, provide comprehensive monitoring of national borders, reducing the risk of illegal crossings and smuggling. AI-powered drones are particularly useful in patrolling remote and hard-to-reach areas, offering real-time data on border activities and allowing authorities to respond to incidents more swiftly. In Europe and North America, AI-based facial recognition and biometric systems have been integrated into border checkpoints to expedite identity verification and prevent illegal immigration (Brundage et al., 2018). These systems can cross-reference databases in seconds, flagging potential security risks and ensuring that border control remains efficient without compromising security. Additionally, AI's predictive analytics capabilities can identify patterns in border crossings, helping to anticipate migrant flows and smuggling activities.In Nigeria, AI could improve border security along its porous northern and eastern borders, where smuggling, illegal migration, and insurgency pose significant security challenges. By integrating AI with existing surveillance and security systems, Nigeria's border security agencies could achieve better situational awareness and respond proactively to potential threats (Onuoha, 2021).

AI and Nigeria Intelligence Gathering: Scanning the Horizon

Artificial Intelligence (AI) has the potential to significantly enhance intelligence gathering capabilities in Nigeria, addressing the multifaceted security challenges facing the country. By leveraging AI technologies, Nigerian intelligence agencies can improve their efficiency, accuracy, and responsiveness in tackling issues such as banditry, terrorism, herdsmen conflicts, Biafra secessionist activities, and pipeline vandalism.

International Journal of Sub-Saharan African Research (IJSSAR)
Vol. 3, Issue 3, pp. 206-225, September 2025, ISSN: 3043-4467 (Online), 3043-4459 (Print)
DOI:10.5281/zenodo.17252277

Essence of AI in Intelligence Gathering

Predictive Analytics for Threat Assessment

AI-powered predictive analytics involves analyzing large volumes of data to identify patterns and predict future events. In the context of intelligence gathering, AI can analyze historical data, social media activity, and other sources to forecast potential security threats. AI can process data on past bandit attacks, movements, and social media chatter to predict where future attacks might occur, enabling proactive deployment of resources and preventive measures (Bello & Adeyemi, 2023). Similarly, AI can analyze data from various sources, including communication intercepts and social media, AI can identify early warning signs of terrorist activities, allowing for timely intervention.

Enhanced Surveillance and Monitoring

AI technologies such as computer vision and facial recognition improve the capability to monitor and analyze visual data. These technologies can be integrated into surveillance systems to enhance the detection of suspicious activities and individuals. For example, AI-powered drones can monitor pipeline infrastructure in real-time, detecting unauthorized access or suspicious activities and sending automated alerts to prompt immediate responses from security personnel (Ojo, 2022). AI-equipped surveillance systems, if deployed in troubled areas of farmer-herder clash can also monitor grazing areas and detect illegal activities or clashes between herders and farmers, providing early alerts and responses to security forces.

International Journal of Sub-Saharan African Research (IJSSAR)
Vol. 3, Issue 3, pp. 206-225, September 2025, ISSN: 3043-4467 (Online), 3043-4459 (Print)
DOI:10.5281/zenodo.17252277

Data Integration and Correlation

AI plays a pivotal role in integrating and analyzing data from various intelligence sources such as human intelligence (HUMINT), signals intelligence (SIGINT), technical intelligence (TECNIT), and open-source intelligence (OSINT). AI can substantially amalgamate information from platforms like social media, intercept communications, and ground-level intelligence. AI can substantially enhance the understanding of groups like IPOB, Boko Haram, Etc. Chukwu & Hassan (2022) asserted that this comprehensive approach not only aids in threat assessment but also contributes to strategic planning. Again, AI's ability to synthesize data from diverse sources enables a more profound insight into the activities of criminal elements. Moreover, in combating organized crime, AI's capacity to merge data from financial transactions and criminal records proves instrumental in identifying and dismantling criminal networks. Through automated threat detection and response mechanisms, AI strengthens security measures by swiftly identifying potential threats and responding effectively.

Automated Threat Detection and Response

AI systems can automate the detection of threats and initiate responses based on predefined criteria, reducing the time required to identify and act on security threats. For example, AI can monitor network traffic for signs of cyber threats, such as attempted breaches or malware infections, and trigger automated responses to mitigate these threats quickly. Additionally, AI can analyze communication data to detect potentially dangerous activities, such as coordinated attacks or criminal planning, and generate real-time alerts for immediate action (Bello & Adeyemi, 2023). In developed nations where technology is profoundly deployed, AI-driven systems are used for real-time threat detection and automated response in cybersecurity and military applications. Nigeria could benefit from similar technologies to enhance its security infrastructure and operational capabilities in tackling criminal enterprises.

Cyber Intelligence and Digital Forensics

AI technologies can enhance cyber intelligence and digital forensics by analyzing digital data to uncover cyber threats, trace their origins, and understand their impact. AI can assist in identifying cyber threats targeting pipeline infrastructure, analyzing digital footprints to trace the source of attacks, and preventing future incidents (Asad and Steltzer, 2025). Similarly, AI can detect patterns of financial fraud and cybercrime, such as money laundering linked to organized crime. This can potentially enhance Nigerian intelligence community ability to detect threat, tract it and neutralize it.

International Journal of Sub-Saharan African Research (IJSSAR)
Vol. 3, Issue 3, pp. 206-225, September 2025, ISSN: 3043-4467 (Online), 3043-4459 (Print)
DOI:10.5281/zenodo.17252277

CONCLUSION

In conclusion, Artificial Intelligence (AI) has the potential to significantly enhance Nigeria's intelligence gathering by providing tools for predictive analytics, advanced surveillance, data integration, automated threat detection, and cyber intelligence. AI can help security agencies identify emerging threats, analyze vast data efficiently, and improve situational awareness, allowing for proactive responses to terrorism, banditry, and other criminal enterprises troubling the Nigerian State. AI-driven systems can also protect critical infrastructure and improve counter-terrorism efforts by tracking networks and disrupting communication. To fully harness AI's potential, Nigeria must invest in infrastructure, training, and ethical standards.

Ethical Clearance

This study complied with ethical standards, ensuring informed consent, confidentiality, and voluntary participation. All data were securely stored and used exclusively for academic purposes.

Acknowledgements

We thank all participants, stakeholders, and policymakers for their contributions. Special appreciation to JessieGie Research Associates and the peer reviewers for their insightful feedback.

Conflict of Interest

The authors affirm that the research was carried out without any commercial or financial ties that might be perceived as a potential conflict of interest.

Funding

No external funding was received for this study.

Authors' Contributions

David Donald led the study and analysis. Mustapha Aisha contributed to literature review and thematic organization, while Abubakar Sanusi Imam handled documentation and editing. All authors reviewed and approved the final manuscript and are responsible for its content.

Availability of Data and Materials

The datasets on which conclusions are made for this study are available on reasonable request

Cite this article this way:

David, D., Mustapha, A., & Abubakar, S.I. (2025). Role of Artificial Intelligence (AI) in Intelligence Gathering and Management of Nigeria National Security. International Journal of Sub-Saharan African Research (IJSSAR), 3(3)

International Journal of Sub-Saharan African Research (IJSSAR)
Vol. 3, Issue 3, pp. 206-225, September 2025, ISSN: 3043-4467 (Online), 3043-4459 (Print)
DOI:10.5281/zenodo.17252277

REFERENCES

Adejoh, S., & Shimawua, D. (2018). The National Intelligence Agency (NIA) and Nigeria's diplomatic relations in contemporary times. KIU Journal of Humanities, 3(2), 81–86.

Allen, G., & Gregory, R. (2020). AI and the future of intelligence: National security in the era of machine learning. Center for Security and Emerging Technology. https://cset.georgetown.edu

Baldwin, D. A. (1997). The concept of security. Review of International Studies, 23(1), 5–26. https://doi.org/10.1017/S0260210597000053

Becker, G. S. (1976). The economic approach to human behavior. University of Chicago Press.

Beland, D. (2007). Insecurity and politics: A framework. Canadian Journal of Sociology, 32(3), 317–340. https://doi.org/10.29173/cjs1650

Boulanin, V., & Verbruggen, M. (2017). Mapping the development of autonomy in weapon systems. Stockholm International Peace Research Institute. https://sipri.org

Buzan, B. (1991). People, states, and fear: An agenda for international security studies in the post-Cold War era. Lynne Rienner Publishers.

Center for Security and Emerging Technology. (2020). AI and national security: Opportunities and risks. https://cset.georgetown.edu

Elster, J. (1989). Social norms and economic theory. Journal of Economic Perspectives, 3(4), 99–117. https://doi.org/10.1257/jep.3.4.99

Enyia, J., Achu, A., Duke, O., Njong, C., Takim, O., & Okpa, J. (2022). Intelligence gathering imperative: A tool for successful security outfits' operation. International Journal of Criminology and Sociology, 11, 136–143. https://doi.org/10.6000/1929-4409.2022.11.15

European Commission. (2018). Definition and principles of artificial intelligence. https://europa.eu

Grüne-Yanoff, T. (2012). Paradoxes of rational choice theory. In S. Roeser, R. Hillerbrand, P. Sandin, & M. Peterson (Eds.), Handbook of risk theory (pp. 499– 516). Springer. https://doi.org/10.1007/978-94-007-1433-5_19

Hedström, P., & Stern, C. (2008). Rational choice and sociology. In S. N. Durlauf & L. E. Blume (Eds.), The New Palgrave Dictionary of Economics (2nd ed.). Palgrave Macmillan. https://doi.org/10.1057/9780230226203.1381

Hoadley, D. S., & Lucas, N. J. (2018). Artificial intelligence and national security (CRS Report No. R45178). Congressional Research Service. https://digital.library.unt.edu/ark:/67531/metadc1157028

Imobighe, T. A. (Ed.). (2003). Civil society and ethnic conflict management in Nigeria. Spectrum Books.

International Crisis Group. (2024). Farmer–herder conflicts in Nigeria: An escalating crisis. https://crisisgroup.org

International Maritime Bureau. (2021). Piracy and armed robbery report. https://icc-ccs.org

Katzenstein, P. J. (Ed.). (1996). The culture of national security: Norms and identity in world politics. Columbia University Press.

Lippmann, W. (1943). U.S. foreign policy: Shield of the republic. Little, Brown, and Co.

Lohmann, S. (2008). Rational choice and political science. In S. N. Durlauf & L. E. Blume (Eds.), The New Palgrave Dictionary of Economics (2nd ed.). Palgrave Macmillan. https://doi.org/10.1057/9780230226203.1406

Lowenthal, M. M. (1999). Intelligence: From secrets to policy. CQ Press.

Mbachu, O., & Sokoto, A. A. (Eds.). (2011). Nigeria defence and security: Policies and strategy. Medusa Publishers.

Mbachu, O., & Yesufu, M. I. (2011). Contemporary strategy: Theoretical perspectives and policy options. Medusa Publishers.

Moses, R. O., & Abiodun, T. F. (2020). Challenges of interagency collaboration in emergency response in Nigeria. Global Scientific Journal, 8(3), 1–12.

Musa, F. (2021). Department of State Services and counterintelligence in Nigeria. Journal of Intelligence and Security Studies, 15(1), 44–63.

National Information Technology Development Agency. (2021). Artificial intelligence: Policy guidelines for Nigeria. https://nitda.gov.ng

Nte, N. D. (2013). An analysis of intelligence support to security operations in Nigeria: A review of some Joint Task Force operations. Peace and Security Review, 5(9), 1– 23.

International Journal of Sub-Saharan African Research (IJSSAR)
Vol. 3, Issue 3, pp. 206-225, September 2025, ISSN: 3043-4467 (Online), 3043-4459 (Print)
DOI:10.5281/zenodo.17252277

Oghi, F. E. (2014). Military intelligence and the challenge of national security in contemporary Nigeria. International Journal of Research in Humanities and Social Studies, 1(2), 7–13.

Onyeka, U. N. (2024). Enhancing sustainability accounting through artificial intelligence (AI): A case of Nigerian manufacturing companies. International Journal of Advances in Engineering and Management, 6(2), 242–246. https://doi.org/10.35629/5252-0602242246

Unalp, A. (2024). AI-driven predictive analytics: Shaping the future of strategic decision making. ResearchGate. https://doi.org/10.13140/RG.2.2.22309.41447

Williams, P. D. (2008). Security studies: An introduction. Routledge.

Wittek, R. (2013). Rational choice theory. In R. Wittek, T. A. B. Snijders, & V. Nee (Eds.), The handbook of rational choice social research (pp. 3–22). Stanford University Press.