ROLES AND EFFECTIVENESS OF INTELLIGENCE GATHERING IN THE MAINTENANCE OF SECURITY IN NIGERIA

Gladys Amaechi OHAZULIKE
Department of Sociology/Anthropology
Faculty of Social Sciences
Nnamdi Azikiwe University, Awka, Anambra State
Email: ga.ohazulike@unizik.edu.ng
&
Queeneth Ndidiamaka OKAFOR
Department of Sociology/Anthropology
Faculty of Social Sciences
Nnamdi Azikiwe University, Awka, Anambra State
Email: qn.okafor@unizik.edu.ng

Abstract

Intelligence gathering plays a central role in national security management, particularly in states facing complex and asymmetric threats. Nigeria has confronted multiple security challenges, including insurgency, terrorism, banditry, kidnapping, oil theft, and separatist agitations. This paper critically examines the role and effectiveness of intelligence gathering in maintaining security in Nigeria. It explores institutional frameworks, intelligence strategies, operational challenges, and systemic weaknesses. The study employed secondary sources drawing from the existing literature, such as journal articles, government reports, and security analyses, to evaluate how intelligence contributes to counterterrorism, crime prevention, and internal stability. The paper finds that while intelligence gathering has significantly contributed to disrupting terrorist networks and criminal enterprises, structural issues such as inter-agency rivalry, inadequate technological capacity, corruption, and weak community trust undermine its full effectiveness. The paper concludes that strengthening inter-agency coordination, investing in technological intelligence systems, and enhancing community-based intelligence are critical for sustainable security management in Nigeria.

Keywords: effectiveness, intelligence gathering, Nigeria, roles, security

Introduction

Security remains a fundamental responsibility of the state, forming the bedrock upon which sovereignty, governance, and socio-economic development rest. Traditionally, national security has been conceptualized as the protection of territorial integrity and political independence. However, contemporary security discourse has expanded this notion to encompass protection against internal threats such as terrorism, insurgency, organized crime, and communal violence (Buzan, 1991; United Nations Development Programme, 2022). This broadened understanding reflects the evolving nature of threats confronting modern states, particularly in developing and conflict-prone regions, where human security concerns, such as economic stability, community safety, and political inclusion, are increasingly recognized as integral to national security (United Nations, 2023; World Bank, 2024).

In Nigeria, the persistence and transformation of internal security threats have elevated intelligence gathering to a central position within the national security architecture. As Africa's most populous country and one of its largest economies, Nigeria occupies a strategic geopolitical position in West Africa, such that instability within its borders often produces significant regional repercussions. Over the past two decades, Nigeria's security environment has undergone a profound transformation, most notably with the emergence and escalation of the Boko Haram insurgency in the northeastern region. Initially a localized extremist movement, Boko Haram evolved into a violent insurgent organization with transnational reach, engaging in bombings, kidnappings, and attacks on both civilian and military targets (Onuoha, 2014). This development exposed critical institutional weaknesses in Nigeria's intelligence and security systems, particularly in early threat detection, information coordination, and strategic response.

Intelligence gathering, defined as the systematic collection, analysis, interpretation, and dissemination of information relevant to national security decision-making, plays a crucial anticipatory role in mitigating threats before they fully materialize (Davies & Phythian, 2016; Lowenthal, 2017). Its effectiveness depends not merely on the volume of information collected but on the timeliness, accuracy, reliability, and actionable value of such information (Lowenthal, 2017). In practice, intelligence gathering encompasses multiple modalities, including human intelligence (HUMINT), signals intelligence (SIGINT), geospatial intelligence (GEOINT), and open-source intelligence (OSINT), all of which collectively support strategic planning, tactical operations, and policy formulation (Davies &Phythian, 2016; Johnson, 2017).

In Nigeria, responsibility for intelligence gathering is distributed among key institutions within the national security framework. The Department of State Services (DSS) is primarily tasked with domestic intelligence, counterintelligence, and internal security monitoring, including the detection and prevention of threats such as terrorism, espionage, and subversion (Department of State Services, 2024). The National Intelligence Agency (NIA) is responsible for foreign intelligence collection and external threat assessment, while the Defence Intelligence Agency (DIA) provides military intelligence, supporting defence planning, strategic reconnaissance, and counterinsurgency operations (Olowonihi & Musa, 2024; National Security Agencies Act, 1986). Together with the Nigeria Police Force and other specialized security units, these agencies form the backbone of Nigeria's intelligence community, collaborating to address evolving security challenges (Iwuoha et al., 2024). Intelligence gathering within this framework underpins proactive security governance by enabling the identification of emerging threats, disruption of criminal networks, monitoring of extremist activities, and protection of critical infrastructure (Akin, 2021; Usman, 2022). Through inter-agency coordination and intelligence sharing, these institutions contribute to strategic decision-making, law enforcement effectiveness, and national stability, although their performance is often shaped by broader institutional and resource constraints.

Notwithstanding its centrality, the effectiveness of intelligence gathering in Nigeria remains contested. While intelligence-led operations have contributed to counterterrorism efforts against Boko Haram and other criminal networks, persistent insecurity raises concerns about systemic deficiencies. Scholars argue that intelligence failures during the early stages of the Boko Haram insurgency were linked to poor inter-agency coordination, limited technological capacity, and weak community engagement mechanisms (Onuoha, 2014). Furthermore, inter-agency rivalry, bureaucratic fragmentation, and political interference have often undermined intelligence-sharing processes and operational coherence, thereby constraining the overall effectiveness of security responses.

The effectiveness of intelligence systems extends beyond institutional presence or data accumulation; it is contingent upon professionalism, inter-agency collaboration, technological sophistication, accountability mechanisms, and public trust. As Lowenthal (2017) emphasizes, intelligence institutions function optimally when embedded within transparent oversight frameworks that balance operational autonomy with accountability. In Nigeria, challenges such as corruption, politicization of security agencies, and resource constraints often impede the translation of intelligence into sustainable security outcomes.

Compounding these challenges is the increasingly complex and multidimensional nature of Nigeria's threat environment. Security concerns range from insurgency in the Northeast and banditry in the Northwest to secessionist agitations in the Southeast, communal conflicts in the Middle Belt, and piracy in the Gulf of Guinea (International Crisis Group, 2020; Armed Conflict Location & Event Data Project, 2023). These threats frequently intersect, involving transnational criminal networks, illicit arms flows, and the use of digital communication technologies, thereby necessitating advanced intelligence capabilities across cyber, financial, and border security domains (United Nations Office on Drugs and Crime, 2021; Global Initiative Against Transnational Organized Crime, 2022).

Equally critical to intelligence effectiveness is the issue of community trust. Human intelligence, in particular, relies heavily on cooperation from local populations. Where security agencies are perceived as repressive, corrupt, or politically biased, public willingness to share information diminishes, weakening early warning systems and grassroots threat detection (African Journal of Social Sciences and Humanities Research, 2024). Empirical studies on Nigeria show that effective information sharing between citizens and security agencies depends fundamentally on trust, which is often undermined in contexts marked by allegations of human rights abuses and lack of transparency. Consequently, intelligence effectiveness is closely linked to broader issues of human rights, civil-military relations, and democratic accountability. In many Nigerian communities, strained civil-military relations and perceptions of security forces as adversarial actors further weaken cooperation and intelligence flow (Center for Strategic and International Studies, 2025). These dynamics highlight the necessity of citizen-centric and community-based security approaches, where trust-building, accountability, and respect for human rights are integral to strengthening intelligence systems and enhancing national security outcomes

At the regional and international levels, intelligence collaboration further shapes Nigeria's security outcomes. Nigeria participates in multilateral counterterrorism initiatives within the Lake Chad Basin and West Africa, particularly through frameworks such as the Multinational Joint Task Force (MNJTF), where intelligence-sharing arrangements are central to addressing cross-border insurgency and transnational crime (African Union, 2025; United Nations, 2025). These collaborative mechanisms facilitate joint military operations, coordinated surveillance, and information exchange among member states confronting groups such as Boko Haram and the Islamic State West Africa Province. However, the success of such collaborations depends on institutional trust, technological interoperability, and sustained diplomatic coordination in an increasingly globalized security landscape. Recent developments indicate that regional political tensions and weak coordination mechanisms can undermine the effectiveness of intelligence sharing and joint operations (The Soufan Center, 2025). Similarly, gaps in trust and cooperation among regional blocs and partners continue to limit the effectiveness of counterterrorism frameworks, highlighting the need for stronger coordination, integrated intelligence systems, and confidence-building measures (United Nations, 2025).

Against this backdrop, this paper argues that while intelligence gathering has become indispensable to Nigeria's security maintenance, its effectiveness is constrained by institutional fragmentation, technological limitations, governance challenges, and insufficient community integration. Achieving sustainable security requires not only enhanced intelligence capabilities but also comprehensive reforms that promote accountability, inter-agency coordination, technological modernization, and public trust. By critically examining the Nigerian case, this study assesses the role, effectiveness, and prospects of intelligence gathering as both a defensive shield and a strategic instrument for national stability and development

METHODOLOGY

The study relies on secondary data, such as journal articles, books, and theses focusing on intelligence, counterterrorism, and national security theory. Also, Policy reports, white papers, media, and open-source intelligence (OSINT) were consulted.

LITERATURE REVIEW

Intelligence Gathering

Lowenthal (2022) defines intelligence gathering as the process by which specific types of information important to national security are requested, collected, and made available to policymakers. Kent (1949) describes intelligence gathering as the systematic collection of information required to support national policy and military planning, emphasizing its role in reducing uncertainty for decision-makers. According to the United States Department of Defense (2021), intelligence gathering is the acquisition of information about foreign nations, hostile or potentially hostile forces, or elements, conducted through overt and covert means to support strategic objectives. Herman (1996) defines intelligence gathering as the organized process of collecting and analyzing information about adversaries to inform government decision-making and safeguard national interests. Johnson (2017) explains intelligence gathering as the systematic acquisition of secret or open-source information by state agencies to anticipate threats and guide foreign and security policy. Intelligence gathering refers to the systematic collection, evaluation, and analysis of information to support informed decision-making, particularly in national security. It is a core function of governments and security institutions, enabling policymakers and military leaders to anticipate threats, assess risks, and develop strategic responses. According to Lowenthal (2017), intelligence is not merely information, but information that has been collected, processed, and analyzed to meet the specific needs of decision-makers. Thus, intelligence gathering is both a process and a product, transforming raw data into actionable insights.

The primary purpose of intelligence gathering is to reduce uncertainty in decision-making. In national security contexts, leaders often operate in environments characterized by ambiguity, incomplete information, and rapidly evolving threats. Intelligence helps bridge information gaps by providing timely and accurate assessments of adversaries' capabilities, intentions, and activities. Effective intelligence enables proactive measures rather than reactive responses, thereby enhancing national security and safeguarding state interests (Lowenthal, 2017).

Intelligence gathering also supports counterterrorism, counterintelligence, cybersecurity, and military operations. Beyond security, intelligence may inform diplomatic negotiations, economic policy, and crisis management. The quality of intelligence directly affects the quality of decisions; flawed or delayed intelligence can result in strategic miscalculations with significant consequences.

Types of Intelligence Gathering

Intelligence gathering encompasses multiple collection disciplines, each contributing unique insights. The integration of these disciplines strengthens overall intelligence analysis.

- ✓ Human Intelligence (HUMINT)

Human Intelligence (HUMINT) involves the collection of information from human sources. This may include interviews, interrogations, undercover operations, and the recruitment of informants or agents (European Intelligence Academy, 2024; U.S. Air Force, n.d.). HUMINT is particularly valuable for understanding intentions, motivations, and plans that may not be evident through technical means, as it provides contextual and qualitative insights that complement technical intelligence (AML Network, n.d.; Threat Intelligence Manual, n.d.). For example, a human source embedded within an organization may reveal strategic intentions that are not detectable through intercepted communications (U.S. Air Force, n.d.). However, HUMINT carries inherent risks, including issues of source reliability, deception, and operational security concerns, since human sources may provide inaccurate or biased information (European Intelligence Academy, 2024). Therefore, effective HUMINT operations require careful validation and cross-referencing with other intelligence sources to ensure accuracy (Lowenthal, 2017).

✓ Signals Intelligence (SIGINT)

Signals Intelligence (SIGINT) involves the interception and analysis of electronic communications and signals. This includes communications intelligence (COMINT), such as phone calls and emails, and electronic intelligence (ELINT), which focuses on non-communication signals, such as radar emissions (National Security Agency, 2023). SIGINT provides large volumes of data that can reveal patterns of activity, communication networks, and operational capabilities (NATO, 2022). Technological advancements have significantly expanded the scope of SIGINT, especially in the digital age (European Union Agency for Cybersecurity, 2023). It is particularly useful for monitoring adversary communications and identifying emerging threats (NATO, 2022). Despite its strengths, SIGINT presents challenges, including encryption, data overload, and legal or ethical constraints related to privacy and surveillance (ENISA, 2023). Effective SIGINT operations require advanced analytical tools and strict oversight to ensure compliance with legal frameworks (National Security Agency, 2023)

✓ Geospatial Intelligence (GEOINT)

Geospatial Intelligence (GEOINT) involves the collection and analysis of imagery and geospatial data to describe, assess, and visually depict physical features and activities on Earth (National Geospatial-Intelligence Agency, n.d.; U.S. Government Accountability Office, 2023). This discipline relies on satellite imagery, aerial photography, and mapping technologies to generate actionable intelligence (NGA, n.d.). GEOINT supports a wide range of applications, including military planning, disaster response, border security, and infrastructure monitoring (GAO, 2023; United Nations Institute for Training and Research, 2022). For instance, satellite imagery can detect troop movements, construction of facilities, or changes in terrain that may indicate strategic developments (GAO, 2023). The visual nature of GEOINT enhances situational awareness and enables precise operational planning (UNITAR, 2022). However, GEOINT interpretation requires skilled analysts, as imagery can be misinterpreted without sufficient contextual understanding, and environmental factors such as weather conditions may limit the effectiveness of imagery collection (NGA, n.d.; Lowenthal, 2017).

✓ Open-Source Intelligence (OSINT)

Open-Source Intelligence (OSINT) refers to the collection and analysis of publicly available information, including news media, academic publications, government reports, social media platforms, and other accessible data sources (NATO, 2023; U.S. Department of Homeland Security, 2022). OSINT has gained increasing prominence in the digital era due to the vast amount of information available online, providing cost-effective and legally accessible insights into political developments, public sentiment, and emerging trends (DHS, 2022; European Union Agency for Law Enforcement Cooperation, 2023). For example, social media analysis can reveal early indicators of unrest or extremist activities (Europol, 2023). Although OSINT is widely accessible, its reliability varies significantly, requiring analysts to critically evaluate source credibility and guard against misinformation, propaganda, and deliberate disinformation campaigns (NATO, 2023). When properly validated and integrated with other intelligence disciplines, OSINT enhances comprehensive threat assessments (Lowenthal, 2017).

Institutional Framework on Intelligence in Nigeria

Nigeria's intelligence structure operates primarily through three key agencies:

- The National Intelligence Agency (NIA) is responsible for foreign intelligence and external threats.
- Department of State Services (DSS) is responsible for domestic intelligence and counterintelligence.
- The Defence Intelligence Agency (DIA) is responsible for military and defense intelligence.

These agencies collaborate with the Nigerian Armed Forces and the Nigerian Police Force in operational matters. Although this architecture appears comprehensive, challenges such as overlapping mandates, bureaucratic competition, limited data-sharing systems, and inadequate funding hinder optimal performance.

The Intelligence Cycle

Intelligence gathering operates within a structured framework commonly known as the intelligence cycle. The cycle typically includes five stages: planning and direction, collection, processing, analysis and production, and dissemination (Lowenthal, 2017).

i. Planning and Direction: Decision-makers identify intelligence requirements and set priorities.
ii. Collection: Relevant data is gathered using HUMINT, SIGINT, GEOINT, and OSINT.
iii. Processing: Collected data are organized, translated, decrypted, or otherwise prepared for analysis.
iv. Analysis and Production: Analysts evaluate the information, identify patterns, and produce intelligence assessments.
v. Dissemination: Finished intelligence products are delivered to policymakers and operational leaders.

Characteristics of Effective Intelligence

For intelligence to be effective, it must possess certain essential qualities:

- Timeliness: Intelligence must be delivered in time to influence decisions. Delayed intelligence, even if accurate, may lose its value.
- Accuracy: Information must be verified and corroborated to minimize errors. Analytical rigor and cross-validation are critical.
- Relevance: Intelligence should address specific policy or operational questions. Irrelevant data can distract or mislead decision-makers.
- Actionability: Intelligence must provide clear implications or recommendations that guide decisions and actions. Lowenthal (2017) emphasizes that intelligence is only valuable when it meets the needs of its consumers. Analysts must therefore understand policymakers' priorities and present findings clearly and objectively.

Ethical and Legal Considerations of Intelligence Gathering

Intelligence gathering involves significant ethical and legal considerations, as activities such as surveillance, interception of communications, and covert operations may raise concerns about privacy, civil liberties, and national sovereignty (United Nations, 2022; Privacy International, 2023). Democratic societies typically establish oversight mechanisms to ensure that intelligence agencies operate within legal boundaries and maintain accountability (U.S. Government Accountability Office, 2023). Balancing security needs with individual rights remains a central challenge in intelligence practice, requiring transparent legal frameworks and institutional checks to prevent abuses while preserving operational effectiveness (UN, 2022).

Intelligence gathering is a foundational component of national security and strategic decision-making, transforming raw data into actionable knowledge through systematic collection, analysis, and dissemination processes (Office of the Director of National Intelligence, 2023). The primary disciplines, HUMINT, SIGINT, GEOINT, and OSINT, each contribute distinct capabilities that, when integrated, provide comprehensive situational awareness (ODNI, 2023; Lowenthal, 2017). Guided by the intelligence cycle, effective intelligence must be timely, accurate, relevant, and actionable (ODNI, 2023). As threats evolve in complexity and scope, the continued refinement of intelligence practices, analytical rigor, and ethical oversight remains essential to safeguarding national interests (GAO, 2023; Lowenthal, 2017).

Role of Intelligence Gathering

The role of intelligence gathering in national security management, particularly in combating asymmetric threats, has attracted considerable scholarly attention. Asymmetric threats, such as terrorism, insurgency, and transnational criminal networks, are characterized by unconventional tactics, decentralized structures, and adaptability. Scholars widely agree that traditional military responses alone are insufficient to address such threats; instead, intelligence-led strategies are essential for early detection, disruption, and prevention (Gill &Phythian, 2018).

Gill and Phythian (2018) argue that intelligence is indispensable in addressing modern security challenges because it enables governments to anticipate and neutralize threats before they materialize into large-scale violence. Unlike conventional warfare, asymmetric conflicts rely heavily on secrecy, surprise, and mobility. Consequently, effective intelligence gathering through Human Intelligence (HUMINT), Signals Intelligence (SIGINT), and other methods forms the foundation of counterterrorism and counterinsurgency strategies. Intelligence, when timely and accurate, enhances precision targeting and reduces collateral damage. In the Nigerian context, the rise of terrorism, particularly by Boko Haram, underscores the relevance of intelligence in asymmetric warfare. Early stages of the insurgency exposed weaknesses in threat anticipation and institutional preparedness. Onuoha (2014) observes that intelligence failures significantly contributed to the rapid expansion of Boko Haram between 2009 and 2013. Inadequate threat assessment, poor information-sharing mechanisms, and underestimation of the group's organizational capacity allowed it to consolidate territorial control in parts of North-East Nigeria. This period illustrates how intelligence shortcomings can exacerbate insecurity and enable extremist movements to entrench themselves.

Beyond operational lapses, scholars highlight structural and institutional weaknesses within Nigeria's security framework. Ebo (2007) identifies systemic deficiencies, including poor coordination among security agencies, overlapping mandates, limited accountability mechanisms, and political interference in intelligence operations. These structural challenges undermine the efficiency of intelligence gathering and dissemination processes. Inter-agency rivalry is frequently cited as a critical barrier to effective intelligence performance. Fragmentation among intelligence and law enforcement bodies hampers seamless information sharing and joint operational planning. In complex security environments, delayed or withheld intelligence can lead to missed opportunities for preventive action. The absence of integrated intelligence databases and standardized communication platforms further compounds these coordination problems. Political interference also weakens intelligence neutrality and professionalism. When intelligence agencies are drawn into partisan politics or used to advance political interests, public trust erodes. Such politicization may compromise objectivity in threat assessment and distort security priorities (Ebo, 2007).

Another recurring theme in the literature concerns technological limitations. Modern intelligence operations increasingly rely on advanced surveillance systems, data analytics, satellite imagery, and cyber capabilities. However, studies suggest that Nigeria's intelligence infrastructure lags behind global standards, particularly in cyber intelligence and electronic surveillance. Insufficient technological infrastructure limits real-time monitoring, predictive analysis, and effective counterterrorism operations. In addition to technological deficits, capacity gaps in training and analytical expertise restrict the transformation of raw data into actionable intelligence. Intelligence effectiveness depends not only on collection but also on rigorous analysis and timely dissemination (Gill & Phythian, 2018). Where analytical capacity is weak, early warning signals may be overlooked or misinterpreted.

Human Intelligence (HUMINT) remains particularly vital in counterinsurgency contexts where local knowledge and community engagement are essential for effective intelligence gathering (United Nations Office on Drugs and Crime, 2022; International Crisis Group, 2023). However, weak community trust in security institutions poses significant obstacles to intelligence collection, as reports of human rights abuses, excessive use of force, and corruption discourage civilian cooperation (Amnesty International, 2023; Human Rights Watch, 2024). Without credible community engagement, the flow of reliable grassroots intelligence becomes constrained (ICG, 2023).Corruption within security agencies further undermines intelligence effectiveness. The misappropriation of funds allocated for intelligence operations, leakage of classified information, and collusion with criminal actors weaken institutional integrity and operational capacity (Transparency International, 2023; UNODC, 2022). Such practices not only reduce operational efficiency but also erode legitimacy and public confidence in security institutions (Transparency International, 2023; Amnesty International, 2023).

Despite these persistent challenges, recent studies indicate measurable improvements in intelligence-led operations. The International Crisis Group (2020) reports that enhanced intelligence coordination and military reforms contributed to territorial gains against Boko Haram and its splinter factions. Improved surveillance, joint task force operations, and regional cooperation within the Lake Chad Basin have disrupted insurgent supply chains and reduced the scale of territorial control previously exercised by extremist groups. These developments suggest that reforms in intelligence coordination and operational planning can yield tangible security improvements. However, while territorial recapture and targeted strikes represent tactical successes, the persistence of insurgent attacks indicates that strategic intelligence challenges remain unresolved. The roles of intelligence gathering in the security of Nigeria are as follows:

- ✓ Counterterrorism and Counterinsurgency

Intelligence gathering has been central to Nigeria’s fight against Boko Haram and ISWAP. Through surveillance operations, informant networks, electronic interception, and aerial reconnaissance, security forces have disrupted planned attacks and targeted insurgent strongholds (International Crisis Group, 2020). Intelligence-driven operations have enabled the rescue of abducted victims and the recapture of territories in the North-East. However, insurgent groups have demonstrated adaptability, exploiting porous borders and local grievances. While intelligence has achieved tactical successes, the persistence of insurgency suggests limitations in strategic forecasting and long-term threat neutralization.

- ✓ Combating Banditry and Kidnapping

The rise of armed banditry and mass kidnapping in North-West Nigeria has necessitated greater reliance on community-based intelligence (HUMINT). Local informants often provide actionable leads on criminal hideouts and movements. Yet, mistrust between communities and security agencies, partly due to allegations of misconduct, weakens intelligence flows and reduces effectiveness. Intelligence supports the Nigeria Police Force in tracking kidnapping syndicates, armed robbery groups, and bandit networks. Predictive intelligence helps security agencies anticipate attacks and deploy forces strategically.

- ✓ Protection of Critical Infrastructure and Economic Assets

Nigeria’s oil infrastructure and maritime domain are vital to national revenue. Intelligence gathering supports surveillance of pipelines, ports, and territorial waters. Intelligence-led monitoring has reduced large-scale pipeline vandalism compared to earlier periods of intense militancy. Nevertheless, illegal oil bunkering and piracy remain persistent challenges. Intelligence gathering assists in identifying sabotage networks and preventing economic disruption (Ebo, 2007).

✓ Cybersecurity and Financial Intelligence

The growth of digital finance and communication technologies has expanded the scope of intelligence gathering. Nigerian agencies increasingly rely on digital surveillance and financial intelligence to combat cybercrime and terrorism financing. However, technological limitations and inadequate cybersecurity infrastructure reduce the country’s capacity to confront sophisticated global cyber threats.

✓ Border Security and Transnational Crime

Nigeria faces porous borders that facilitate arms trafficking and terrorist movement.
Intelligence collaboration with neighboring states enhances border monitoring and regional security.

The Effectiveness of Intelligence Gathering in Nigeria

The effectiveness of intelligence gathering in Nigeria presents a complex and mixed picture. On the one hand, intelligence-led operations have improved tactical military outcomes, particularly in counterterrorism and counterinsurgency campaigns. On the other hand, systemic institutional weaknesses continue to undermine strategic effectiveness and long-term security consolidation. As intelligence scholarship emphasizes, intelligence is most valuable when it is timely, accurate, and actionable (Lowenthal, 2017). In Nigeria, while operational intelligence has yielded measurable successes, deeper structural and governance challenges limit its transformative impact.

In recent years, intelligence-driven operations have strengthened Nigeria’s counterterrorism efforts, particularly against insurgent groups such as Boko Haram and Islamic State West Africa Province (ISWAP). Enhanced surveillance, improved coordination within joint task forces, and better integration of HUMINT and SIGINT have contributed to the disruption of planned attacks and the targeting of insurgent leaders. According to the International Crisis Group (2020), reforms in operational strategy and improved intelligence coordination were instrumental in regaining territories previously controlled by insurgents in the North-East.These improvements demonstrate the critical role of intelligence in enabling precision operations, minimizing collateral damage, and increasing operational efficiency. Intelligence-driven targeting enhances the capacity of security forces to act proactively rather than reactively, consistent with the early warning function emphasized in intelligence theory (Lowenthal, 2017).One of the most significant contributions of intelligence gathering in Nigeria lies in its early warning capacity. Intelligence agencies collect and analyze data related to potential threats, enabling authorities to anticipate violence and mobilize preventive responses. Early warning systems are particularly important in contexts characterized by asymmetric threats and communal tensions.

In the Nigerian context, early detection of insurgent movements, planned kidnappings, or communal clashes can prevent escalation. However, the effectiveness of early warning mechanisms depends not only on intelligence collection but also on timely dissemination and decisive political action. Instances where attacks occurred despite prior warnings reveal gaps in coordination between intelligence producers and policymakers. As Lowenthal (2017) notes, intelligence has limited value if decision-makers fail to act upon it promptly.

Another area where intelligence gathering has demonstrated effectiveness is in disrupting terrorist financing. Modern insurgent and criminal groups rely heavily on financial networks, including ransom payments, illicit trade, and cross-border transactions. Financial intelligence and collaboration with banking institutions have improved the detection of suspicious transactions linked to terrorism and organized crime. By identifying and freezing financial flows, intelligence agencies weaken the operational capacity of extremist networks. This approach aligns with global counterterrorism best practices, which emphasize financial disruption as a strategic tool for dismantling terrorist organizations. Nevertheless, porous borders and informal financial systems in parts of Nigeria complicate sustained financial monitoring efforts.

Intelligence gathering also plays a crucial role in identifying and mapping criminal networks involved in banditry, kidnapping, oil theft, and cybercrime. Through HUMINT and electronic surveillance, security agencies can trace the structure, leadership, and operational patterns of these groups. The identification of criminal supply chains and logistics hubs enhances targeted law enforcement interventions. However, while intelligence has enabled arrests and tactical successes, criminal networks often regenerate due to socio-economic vulnerabilities, weak governance structures, and limited deterrence. This cyclical pattern underscores the distinction between tactical intelligence effectiveness and broader strategic security outcomes.

Despite operational gains, systemic institutional weaknesses continue to undermine intelligence effectiveness in Nigeria. Scholars highlight challenges such as inter-agency rivalry, insufficient technological infrastructure, corruption, and political interference (Ebo, 2007). These structural constraints limit the capacity of intelligence institutions to function cohesively and professionally. Technological modernization remains uneven, particularly in advanced data analytics, satellite surveillance, and cyber intelligence capabilities. In an era where insurgent groups utilize encrypted communication and digital propaganda, technological gaps significantly reduce predictive and analytical capacity. Furthermore, weak community trust constrains the effectiveness of Human Intelligence (HUMINT). Allegations of human rights abuses and lack of accountability discourage local populations from cooperating with security agencies. Since community-based intelligence is often the most immediate and reliable source of information in counterinsurgency operations, distrust severely limits operational reach.

Lastly, effective intelligence must balance security needs with civil liberties. Allegations of unlawful detention and human rights violations undermine public trust and reduce community cooperation. Without public confidence, HUMINT-often the most valuable intelligence source-becomes weakened. Strengthening legislative oversight and judicial review mechanisms can enhance transparency and accountability while preserving operational secrecy.

Theoretical Thrust: National Security Theory

National Security Theory is rooted in the realist tradition of International Relations, which conceptualizes the state as the primary actor in an anarchic global system where survival constitutes the foremost objective. Its philosophical foundations can be traced to Thomas Hobbes, whose seminal work *Leviathan* established the necessity of a strong sovereign authority to prevent societal descent into disorder and violence (Hobbes, 1651/1996). This early conception of security as protection against existential threats laid the groundwork for the modern understanding of national security as a central function of the state. The formal articulation of National Security Theory emerged in the aftermath of World War II, when the devastating consequences of global conflict underscored the importance of organized defense, intelligence systems, and strategic coordination. Within this context, realist scholars such as Hans Morgenthau argued that the protection of national interest, defined in terms of power, is the primary obligation of states (Morgenthau, 1948). Operating in an anarchic international system devoid of a central authority, states must continuously seek to enhance their capabilities to ensure survival.

Building on classical realism, Kenneth Waltz advanced structural realism (neorealism), emphasizing the role of the international system's structure rather than human nature. In *Theory of International Politics*, Waltz (1979) posited that the anarchic nature of the global system compels states to adopt self-help strategies, including military preparedness, alliance formation, and intelligence development. This perspective explains why even states with peaceful intentions engage in security competition and strategic planning. The conceptual scope of national security was further refined by Arnold Wolfers, who described security as an "ambiguous symbol" encompassing both objective and subjective dimensions (Wolfers, 1952). Objectively, security refers to the absence of threats to core values, while subjectively, it reflects the absence of fear regarding such threats. This duality highlights the importance of perception, risk assessment, and intelligence interpretation in shaping national security policies.

In the late twentieth century, Barry Buzan expanded the theoretical framework by introducing a multidimensional conception of security. In *People, States and Fear*, Buzan (1991) argued that national security extends beyond military concerns to include political, economic, societal, and environmental dimensions. This broadened perspective recognizes that threats to state stability may arise from diverse sources such as economic crises, governance failures, social fragmentation, and environmental degradation. Despite this expansion, the core premise of National Security Theory remains the preservation of state sovereignty, territorial integrity, and institutional stability.

At its core, National Security Theory emphasizes the responsibility of the state to safeguard its sovereignty and protect citizens from both internal and external threats. In contemporary contexts, these threats include terrorism, insurgency, cyberattacks, organized crime, and transnational security challenges (United Nations Office on Drugs and Crime, 2022; World Bank, 2023). This responsibility extends beyond reactive defense to encompass proactive strategies centered on preparedness, resilience, and prevention.

Within this theoretical thrust, intelligence serves as a critical instrument of early warning and strategic decision-making. By systematically collecting, analyzing, and disseminating information, intelligence agencies enable policymakers to anticipate threats and implement preventive measures (Lowenthal, 2017; Office of the Director of National Intelligence, 2023). Intelligence supports the identification of risks across multiple sectors, including political instability, economic vulnerabilities, military developments, and societal tensions. For instance, intelligence assessments may detect patterns of radicalization, cyber threats to critical infrastructure, or emerging insurgent activities, thereby facilitating timely intervention. The early warning function of intelligence also contributes to strategic stability by reducing uncertainty and preventing miscalculations among state and non-state actors. Accurate intelligence enhances decision-making in diplomacy, crisis management, and deterrence strategies, reinforcing its role as both a defensive and stabilizing mechanism within the international system. Consequently, National Security Theory distinguishes between reactive and proactive approaches to security. While reactive strategies respond to threats after their occurrence, proactive approaches emphasize anticipation, risk mitigation, and long-term planning. Intelligence gathering is central to this proactive orientation, enabling states to transition from crisis response to risk prevention. However, proactive intelligence practices must be balanced with legal and ethical considerations. Surveillance, data collection, and covert operations often raise concerns regarding privacy and civil liberties, particularly in democratic societies. As such, oversight mechanisms and legal frameworks are essential to ensure that intelligence activities align with constitutional principles and human rights standards (United Nations, 2022; Privacy International, 2023).

In the contemporary security environment, the relevance of National Security Theory has been further reinforced by globalization, technological advancement, and the increasing complexity of threats. Issues such as cyber warfare, transnational terrorism, pandemics, and climate change underscore the multidimensional nature of security challenges. Buzan's framework remains particularly valuable in capturing these dynamics, as it moves beyond a narrow military focus to encompass broader systemic risks. Intelligence systems must therefore evolve by integrating traditional methods with emerging technologies, including data analytics, cyber monitoring, and open-source intelligence, to enhance predictive capacity and situational awareness (ODNI, 2023).

Applying National Security Theory to Nigeria provides critical insights into the role of intelligence in addressing the country's complex security challenges. Nigeria faces a diverse range of threats, including insurgency, banditry, kidnapping, cybercrime, and communal conflict, all of which cut across Buzan's multiple security sectors (International Crisis Group, 2023; UNODC, 2022). Within this context, intelligence gathering is not merely an administrative function but a central instrument of state survival and stability. However, the Nigerian case also illustrates that intelligence effectiveness is contingent upon broader institutional and governance factors. Challenges such as inter-agency rivalry, corruption, technological limitations, and weak public trust constrain the capacity of intelligence systems to operate effectively (Transparency International, 2023). Moreover, the effectiveness of Human Intelligence (HUMINT) is closely linked to community cooperation, which is often undermined by concerns regarding human rights and accountability.

Ultimately, National Security Theory demonstrates that while intelligence gathering is indispensable for threat detection and prevention, sustainable security depends on a holistic approach that integrates institutional reform, technological advancement, and socio-economic development. In Nigeria, strengthening intelligence systems, alongside governance reforms and public trust, offers a strategic pathway for transitioning from reactive crisis management to proactive and sustainable security governance.

Discussion: The Need for Structural Reforms for Enhanced Roles and Effectiveness of National Intelligence Gathering in the Maintenance of Security in Nigeria

Sustainable security in Nigeria requires comprehensive structural reforms that extend beyond intelligence collection to encompass institutional governance, technological capacity, and societal legitimacy. Contemporary intelligence scholarship underscores that effective intelligence systems depend not only on the acquisition of information but also on accountability, coordination, and trust (Lowenthal, 2017; Office of the Director of National Intelligence, 2023). In this context, strengthening institutional accountability mechanisms is critical to ensuring transparency, professionalism, and the depoliticization of intelligence operations. Robust oversight by legislative and judicial bodies enhances checks and balances, reinforces democratic norms, and builds public confidence in security institutions (U.S. Government Accountability Office, 2023; United Nations, 2022).

Technological modernization constitutes another essential pillar of intelligence reform. Investments in cyber intelligence capabilities, advanced surveillance systems, and integrated intelligence databases can significantly improve inter-agency coordination, data sharing, and predictive analytics (International Telecommunication Union, 2023). As security threats increasingly evolve within digital ecosystems, characterized by encrypted communications, online radicalization, and transnational cybercrime, modern technological infrastructure is indispensable for maintaining operational effectiveness. Complementing these investments, specialized training programs focused on analytical rigor, data interpretation, and strategic forecasting are necessary to enhance the quality, timeliness, and relevance of intelligence outputs (United Nations Office on Drugs and Crime, 2022).

Equally significant is the role of community engagement in strengthening intelligence effectiveness, particularly in the domain of Human Intelligence (HUMINT). Building trust through community policing initiatives, adherence to human rights standards, and inclusive dialogue mechanisms can substantially improve the reliability and flow of grassroots intelligence (United Nations Development Programme, 2023; Amnesty International, 2023). In environments where criminal and insurgent networks are deeply embedded within local communities, public cooperation is indispensable. Without such trust, intelligence agencies face significant constraints in penetrating decentralized networks and identifying emerging threats.

While intelligence gathering remains indispensable, it cannot, in isolation, guarantee long-term stability. Foundational insights from security studies, particularly within Security Studies, emphasize the multidimensional nature of security, integrating military, political, economic, and social dimensions (Buzan, 1991). In the Nigerian context, structural drivers such as socio-economic deprivation, unemployment, corruption, and political exclusion continue to fuel insecurity and instability (World Bank, 2023; Transparency International, 2023). Consequently, intelligence-led operations must be complemented by inclusive development policies that address poverty, expand access to education, and reduce regional inequalities.

Moreover, governance reforms aimed at strengthening the rule of law, enhancing public sector accountability, and promoting equitable political participation are essential for mitigating grievances that often underpin insurgency and organized crime. Intelligence systems may identify and monitor emerging threats, but durable peace ultimately depends on addressing the structural conditions that generate insecurity. A holistic approach, integrating intelligence effectiveness with socio-economic development and institutional reform, remains central to achieving sustainable security outcomes in Nigeria.

Conclusion

Intelligence gathering plays an indispensable role in the maintenance of security in Nigeria. Through agencies such as the NIA, DSS, and DIA, the state has leveraged intelligence to combat terrorism, banditry, militancy, and cybercrime. While notable tactical successes have been achieved, structural weaknesses, technological deficits, and governance challenges limit overall strategic effectiveness. For intelligence gathering to fully support national security, Nigeria must address institutional fragmentation, modernize technological capabilities, and strengthen the intelligence-policy nexus. Ultimately, effective intelligence is not merely about information collection but about transforming accurate and timely knowledge into decisive action that ensures long-term national stability.

Recommendations

To improve effectiveness of intelligence gathering in the maintenance of security in Nigeria, Nigeria should:

a. Invest in advanced surveillance, cyber intelligence, and data analytics systems.
b. Establish integrated intelligence-sharing platforms among agencies.
c. Enhance professional training in strategic intelligence analysis.
d. Promote community engagement to strengthen HUMINT reliability.
f. Strengthen democratic oversight mechanisms to ensure accountability and public trust.

References

African Journal of Social Sciences and Humanities Research. (2024). Information sharing with security forces and community trust in North-West Nigeria, 7(3), 282–296. https://abjournals.org/ajsshr/

African Union. (2025). Communiqué of the 1318th meeting of the Peace and Security Council on the Multinational Joint Task Force (MNJTF). https://www.peaceau.org/

Akin, O. (2021). Intelligence and national security management in Nigeria. *Journal of Security Studies*, *8*(2), 45–60.

Amnesty International. (2023). Nigeria: Human rights report. https://www.amnesty.org

American Psychological Association. (2020). *Publication manual of the American Psychological Association* (7th ed.). APA.

AML Network. (n.d.). What is human intelligence (HUMINT) in anti-money laundering (AML)? Retrieved March 20, 2026.

Armed Conflict Location & Event Data Project (ACLED). (2023). Regional overview: Africa 2023. https://acleddata.com/

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

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

Center for Strategic and International Studies (CSIS). (2025). Nigeria: Building citizen-centric security in the middle of conflict. https://www.csis.org/

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approach* (5th ed.). Sage Publications.

Davies, P. H. J., &Phythian, M. (2016). *Intelligence and government in Britain and the United States* (2nd ed.). Praeger.

Department of State Services. (2024). About the DSS. https://www.dss.gov.ng/

Ebo, A. (2007). Security sector reform in Nigeria: Challenges and opportunities. Geneva Centre for the Democratic Control of Armed Forces.

Ebo, A. (2007). Small arms control in West Africa. International Peace Academy.

European Intelligence Academy. (2024). European intelligence report.

European Union Agency for Cybersecurity (ENISA). (2023). Threat landscape report: Cybersecurity and intelligence trends. https://www.enisa.europa.eu

European Union Agency for Law Enforcement Cooperation (Europol). (2023). Internet organised crime threat assessment (IOCTA). https://www.europol.europa.eu

Gill, P., &Phythian, M. (2018). *Intelligence in an insecure world* (2nd ed.). Polity Press.

Global Initiative Against Transnational Organized Crime. (2022). Organized crime and instability in West Africa. https://globalinitiative.net/

Herman, M. (1996). *Intelligence power in peace and war*. Cambridge University Press.

Hobbes, T. (1996). *Leviathan* (R. Tuck, Ed.). Cambridge University Press. (Original work published 1651)

Human Rights Watch. (2024). *World report 2024*. https://www.hrw.org

International Crisis Group. (2020). Violence in Nigeria’s North East: The insurgency and counterinsurgency. https://www.crisisgroup.org/

International Crisis Group. (2020). What role for the military in Nigeria’s counterinsurgency? https://www.crisisgroup.org/

International Crisis Group. (2023). Counterinsurgency and community trust in conflict zones. https://www.crisisgroup.org/

International Crisis Group. (2023). Nigeria’s security challenges and conflict dynamics. https://www.crisisgroup.org/

International Telecommunication Union (ITU). (2023). Global Cybersecurity Index 2023. https://www.itu.int

Johnson, L. K. (2017). *Spycraft and statecraft: Transforming the U.S. intelligence community*. Oxford University Press.

Johnson, L. K. (2017). *Spy watching: Intelligence accountability in the United States*. Oxford University Press.

Kent, S. (1949). *Strategic intelligence for American world policy*. Princeton University Press.

Lowenthal, M. M. (2017). *Intelligence: From secrets to policy* (7th ed.). CQ Press.

Lowenthal, M. M. (2022). *Intelligence: From secrets to policy* (9th ed.). CQ Press.

Morgenthau, H. J. (1948). *Politics among nations: The struggle for power and peace*. Alfred A. Knopf.

National Geospatial-Intelligence Agency. (n.d.). What is GEOINT? Retrieved March 20, 2026, from https://www.nga.mil

National Security Agencies Act. (1986). Laws of the Federation of Nigeria.

National Security Agency (NSA). (2023). Signals intelligence overview. https://www.nsa.gov

North Atlantic Treaty Organization (NATO). (2022). *Allied joint doctrine for intelligence, counter-intelligence and security (AJP-2).* https://www.nato.int

North Atlantic Treaty Organization (NATO). (2023). Open-source intelligence handbook. https://www.nato.int

Olowonihi, O., & Musa, A. (2024). Military intelligence and counterterrorism operations in Nigeria. *International Journal of Advanced Research*, *13*(12), 1437–1449.

Office of the Director of National Intelligence (ODNI). (2023). The intelligence cycle. https://www.dni.gov

Onuoha, F. C. (2014). Why do youth join Boko Haram? United States Institute of Peace, Special Report.

Privacy International. (2023). Surveillance and human rights. https://privacyinternational.org

Soufan Center. (2025). The Islamic State West Africa Province’s tactical evolution fuels worsening conflict in Nigeria’s northeast. https://thesoufancenter.org/

Threat Intelligence Manual. (n.d.). Human intelligence (HUMINT) sources. Retrieved March 20, 2026.

U.S. Air Force. (n.d.). Sources of intelligence (AF PAM 14-210). Retrieved March 20, 2026.

U.S. Department of Defense. (2021). *Joint publication 2-0: Joint intelligence*. U.S. Department of Defense.

U.S. Department of Homeland Security (DHS). (2022). Open-source intelligence and analysis report. https://www.dhs.gov

U.S. Government Accountability Office (GAO). (2023). Geospatial intelligence: Agencies use imagery and data to support national security missions. https://www.gao.gov

U.S. Government Accountability Office (GAO). (2023). Intelligence oversight and accountability. https://www.gao.gov

United Nations. (2022). The right to privacy in the digital age. https://www.un.org

United Nations. (2025). Secretary-General’s remarks to the Security Council on enhancing regional counter-terrorism cooperation in West Africa and the Sahel. https://www.un.org

United Nations Development Programme (UNDP). (2023). Human Development Report 2023. https://www.undp.org

United Nations Office on Drugs and Crime (UNODC). (2021). Firearms trafficking in West Africa. https://www.unodc.org/

United Nations Office on Drugs and Crime (UNODC). (2022). Crime and security in West Africa. https://www.unodc.org

Usman, A. (2022). Defence intelligence and national security in Nigeria. *African Security Review, 31*(3), 210–225.

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

World Bank. (2023). Nigeria development update. https://www.worldbank.org

Wolfers, A. (1952). National security is an ambiguous symbol. *Political Science Quarterly, 67*(4), 481–502.