

RESEARCH ARTICLE

Open Access

# INTELLIGENCE GATHERING AND ITS CONTRIBUTION TO NIGERIA'S NATIONAL SECURITY: A CRITICAL ASSESSMENT

Ayodele P. Olowonih

PhD Student City University, Cambodia

Dr. M. O. Musa

Department of Cybersecurity, Faculty of Computing, University of Port Harcourt, Nigeria

ORCID: <https://orcid.org/0009-0009-7336-5709>

## Abstract

The Nigerian intelligence sector faces institutional limitations that hinder the successful implementation of intelligence collecting, which is widely acknowledged as a crucial tool in tackling these issues. This paper provides a thorough evaluation of the function of intelligence gathering within Nigeria's national security framework, analysing its effectiveness in dealing with current security challenges. This study seeks to offer a thorough examination of the intelligence cycle in the Nigerian setting, including the gathering, analysis, and use of intelligence in national security strategy. The research used a mixed-methods methodology, combining quantitative data obtained from a questionnaire with qualitative insights obtained from an empirical literature analysis. The Network Theory (TNT) functions as the conceptual framework, providing a perspective to examine the intricate connections and transmission of information within the intelligence network. Statistical analysis is conducted on the questionnaire results using descriptive and inferential methods, while the findings of the literature review are consolidated to offer context and depth. The study results highlight a significant dependence on Human Intelligence (HUMINT) and source intelligence (OSINT) in Nigeria, with a lack of implementation of Geospatial Intelligence (GEOINT) and a disregard for Measurement and Signature Intelligence (MASINT). Furthermore, the investigation exposes inadequate levels of trust and collaboration between intelligence agencies and other security organizations. The major obstacles mentioned are insufficient financial resources, insufficient training and knowledge, technical constraints, competition among different agencies, and legal and bureaucratic restrictions. The research findings indicate that although intelligence gathering is of utmost importance for Nigeria's national security, its efficacy is hindered by structural and operational obstacles. personnel growth and comprehensive strategy to improve intelligence capabilities, which involves bolstering inter- agency collaboration, allocating resources to technical progress and skilled personnel growth, and creating a strong legal and ethical structure.

**Keywords** Intelligence gathering, National Security, Nigeria, HUMINT, OSINT, GEOINT, MASINT.

## INTRODUCTION

National security, or the comprehensive protection of a nation-state against both internal and foreign dangers, includes the preservation of territorial

integrity, sovereignty, political stability, economic prosperity, and the well-being of its people. The idea of national security has evolved globally, moving beyond traditional military defense to include economic, environmental, and human security components (Buzan, Waever, & de Wilde, 1998). In today's interconnected globe, security threats have evolved beyond traditional military conflicts to encompass cyberattacks, terrorism, pandemics, and international organized crime. As a result, national security plans have become more comprehensive and interdisciplinary, requiring the integration of military,

economic, and diplomatic tools, as well as strong intelligence collecting and analysis capabilities (Collins, 2016).

A convergence of historical and modern forces has influenced Nigeria's national security issues over time. Since its independence in 1960, Nigeria has faced numerous security issues, including civil war, military coups, ethnic and religious conflicts, insurgency, and terrorism (Onapajo &

Uzodike, 2022). The Nigerian Civil War (1967-1970), which was motivated by historical ethnic conflicts and regional imbalances, posed a substantial early danger to the country's sovereignty and continued to impact its security landscape (Ukiwo, 2007). The post-civil war era in Nigeria has been characterized by persistent challenges to democratic governance, including frequent military interventions and political instability (Adebayo, 2023).

The twenty-first century has brought new security concerns to Nigeria, namely terrorism and insurgency. The development of Boko Haram, a violent extremist organization, poses a serious threat to national security (Onuoha, 2014). Since its commencement in 2009, Boko Haram's insurgency has caused massive casualties, displacement, and destruction in the northeastern

region (OCHA, 2023). The group's operations not only jeopardized Nigeria's domestic security but also drew international attention, driving regional and global measures to combat terrorism in West Africa (ICG, 2021). Nigeria also has security difficulties such as kidnapping, armed robbery, farmer-herder confrontations, and organized criminal activity (Albert 2015). Poverty, unemployment, and inequality all contribute to the rise of violent non-state actors (Akinola, 2015). Furthermore, Nigeria's security architecture has been chastised for alleged ineffectiveness, corruption, and a lack of coordination, limiting its ability to appropriately address these threats (Ewi C Salifu, 2017). In this environment, intelligence collecting plays a critical role in recognizing, preventing, and responding to security threats, making it an essential component of national security strategy (Adetula, 2010).

Intelligence is the foundation of national security, providing decision-makers with the crucial information and analysis required to develop and implement effective security strategies. Intelligence refers to the systematic collecting, analysis, and dissemination of information about potential threats, both internal and external. This information is critical for averting assaults, combating hostile activities, and protecting national interests. The role of intelligence in national security is critical, allowing governments to anticipate and minimize risks before they become full-fledged crises (Lowenthal, 2016). Globally, intelligence agencies have played critical roles in safeguarding sovereign interests. In the United States, the Central Intelligence Agency (CIA) and the Federal Bureau of Investigation (FBI) are critical components of the national security infrastructure, actively combating terrorist acts and foreign espionage. Similarly, the United Kingdom's Secret

Intelligence Service (MI6) and Security Service (MI5) offer critical intelligence to protect the country from terrorism, organized crime, and cyber threats. Nations such as Russia, China, and Israel prioritize intelligence operations in their security strategies, with agencies like the Federal Security Service (FSB), the Ministry of State Security (MSS), and Mossad tasked with protecting national security through espionage, counterintelligence, and covert operations (Perl,2020).

In Nigeria, intelligence is equally important for national security. The country's intelligence community is made up of numerous agencies, notably the Department of State Services (DSS), the National Intelligence Agency (NIA), and the Defence Intelligence Agency (DIA). These agencies collect intelligence on a wide range of security challenges, including counterterrorism, economic espionage, and cybersecurity. The DSS focuses on domestic intelligence, namely threats such as terrorism, insurgency, and organized crime. The NIA oversees acquiring foreign intelligence and dealing with situations that affect Nigerian interests overseas (Adetula,

2020). Effective intelligence collecting in Nigeria has been critical in combating Boko Haram and other militant organizations. Intelligence has played an important role in monitoring terrorist activity, finding schemes, and interrupting operations, making it critical to Nigeria's counterterrorism efforts. Despite the importance of intelligence in ensuring national security, Nigerian intelligence organizations confront significant obstacles, including insufficient money, antiquated equipment, and little inter-agency collaboration. These problems limit the effectiveness of intelligence operations and contribute to the persistence of security risks (Onuoha, 2020).

## **1.2 Statement of the Problem**

Nigeria's security landscape is characterized by complex and evolving threats. While intelligence gathering is crucial in addressing these issues, the Nigerian intelligence sector faces structural limitations that hinder its effectiveness. These constraints include insufficient funding and resource allocation, which impede the acquisition and maintenance of advanced technology for intelligence gathering and analysis. Moreover, inadequate inter-agency coordination and collaboration lead to fragmentation and inefficient use of intelligence resources. The lack of a robust legal and regulatory framework for intelligence activities creates ambiguity and potential for abuse of power, further undermining the sector's efficacy. These structural challenges collectively contribute to a suboptimal intelligence ecosystem, limiting Nigeria's capacity to proactively and effectively address its multifaceted security concerns.

## **1.3 Purpose and Objectives of the Study**

This study aims to critically examine the efficacy of intelligence gathering in addressing Nigeria's contemporary security challenges, providing a comprehensive analysis of the intelligence cycle and offering recommendations for enhancing its contribution to national security.

### **Objectives**

#### **1.3.1. Research Objectives**

- i. Evaluate the effectiveness of intelligence gathering in addressing Nigeria's national security challenges.
- ii. Examine the mechanisms of interface and collaboration between Nigeria's intelligence agencies and other national and international security organisations in combating security threats.
- iii. Identify the principal challenges confronting

Nigeria's intelligence community and propose strategies to address them. This objective is geared towards problem-solving and offering potential solutions to enhance intelligence capabilities.

iv. Quantify the contribution of intelligence gathering to the success of counterterrorism and anti-crime operations in Nigeria.

### **1.3.2 Research Questions**

i. To what extent is intelligence gathering effective in addressing Nigeria's national security challenges?

ii. How do Nigeria's intelligence agencies interface and collaborate with other national and international security organisations to combat security threats?

iii. What are the principal challenges confronting Nigeria's intelligence community?

iv. What is the quantifiable contribution of intelligence gathering to the success of counterterrorism and anti-crime operations in Nigeria?

### **1.4 Significance of the Study**

This research holds significance on multiple fronts. Primarily, it contributes to the scholarly discourse on national security and intelligence by offering a nuanced analysis of the Nigerian context. Furthermore, the insights generated have the potential to inform policy decisions and reforms directed at enhancing Nigeria's intelligence capabilities. The study underscores the pivotal role of intelligence in navigating the complex and evolving security threats that Nigeria faces in the 21st century.

### **1.5. Scope of the study**

The scope of inquiry is multifaceted. It encompasses an examination of the organizational structure of Nigeria's intelligence agencies, the methodologies and technologies employed in

intelligence collection, and the operational challenges faced by intelligence personnel. Further, the study investigates the application of intelligence in specific security operations, such as counterterrorism efforts against Boko Haram, anti-kidnapping campaigns, and cybersecurity initiatives. The influence of international cooperation and intelligence sharing on Nigeria's national security posture is also considered.

### **2.1 Conceptual Framework**

#### **National Security**

In Nigeria, national security is a multidimensional and intricate concept that involves the protection of the nation's sovereignty, territorial integrity, and national interests from internal and external threats (Obi, 2022). This necessitates an all-encompassing strategy integrating political stability, economic security, social cohesion, and military defence. Throughout history, the security landscape of Nigeria was significantly influenced by the colonial era under British rule, which prioritized the suppression of local resistance and the preservation of colonial order through military strategies and policies (Falola, 2021). The Nigerian Civil War (1967-1970) was the culmination of the nation's immediate security challenges, which included political instability, regional rivalries, and ethnic tensions following independence in 1960 (Ojieh, 2023).

Protecting the state, its sovereignty, territorial integrity, and regime against external aggression is the essence of the Nigerian national security concept (Omenka et al., 2017).

Nigeria's internal security is imperilled by a variety of security challenges, such as terrorism, insurgency, banditry, militancy, and arms importation (Ibani, 2024).

The nation's security agencies are responsible for the protection and promotion of national security

by implementing a strategic plan that underscores the significance of border communities (Nnadi & Okoye, 2022). Insecurity in Nigeria has resulted in violence, impeded growth, and development, and established a porous security environment that affects economic sustainability and wealth creation (Azu et al., 2021). Nigeria's economic development and foreign direct investment are significantly influenced by national security (Opuala-Charles & Oshilike, 2022).

Nigeria is currently facing several urgent security concerns. Since 2009, Boko Haram has become a significant threat, conducting insurgency operations, kidnappings, and terrorist attacks in the northeastern region (Onuoha, 2020). The security situation has been further exacerbated by the emergence of the Islamic State West Africa Province (ISWAP), a dissident group from Boko Haram, which has conducted attacks on both military and civilian targets (Zenn, 2021). Particularly in the Middle Belt region, where disputes over land and resources are prevalent, the country's diverse ethnic composition has frequently resulted in communal conflicts (Adebanwi, 2022). National security is further compromised by political instability and corruption, which erode public trust in institutions and exacerbate grievances that may escalate into disturbance (Agbiboa, 2020). The threat of kidnapping for ransom has become pervasive, with bandits operating in various regions, particularly in the northwest, posing a threat to both locals and foreigners (International Crisis Group, 2023). Additionally, the nation's economic security has been influenced by the historical targeting of oil infrastructure by militant groups in the Niger Delta to secure a larger portion of oil revenues (Watts, 2020).

The Nigerian government's response to security challenges, including the Boko Haram insurgency and abduction activities, underscores the necessity

for improved capabilities within security institutions (TERZUNGWE, 2024).

The investigation of national security in Nigeria encompasses examining various security threats, including cyberterrorism, food security, and the influence of internet-based communication channels on national security (Kente, 2024; Asogwa, 2020). Since independence, Nigeria's foreign policy objectives have been fundamentally influenced by its commitment to regional security and its interventions in West African conflicts (Ebegbulem, 2020). The condition of Nigeria's borders and the ongoing debates surrounding their impact on national security underscores the complexity of border security issues in Nigeria (Awosusi, 2023). In recent years, Nigeria has encountered insecurity challenges that include political violence, terrorism, banditry, abduction, and other forms of criminal activity (Agaku & Moses, 2020).

Nigeria is a prominent force in West Africa, and it plays a critical role in regional security initiatives on the international stage by contributing troops to peacekeeping missions and mediating conflicts in the region (Adebajo, 2022). The nation collaborates with global powers such as the United States, the United Kingdom, and China to improve its security capabilities through intelligence sharing, military assistance, and training (Campbell, 2020). Nevertheless, Nigeria's international security engagements are characterized by the persistent challenge of reconciling national interests with international expectations and navigating intricate geopolitical dynamics.

#### Intelligence Gathering

Intelligence gathering refers to the methodical acquisition and examination of information to guide policymakers and military commanders. This procedure ensures the protection of national

security by the identification and evaluation of both domestic and international risks and opportunities.

The emphasis on comprehending the capabilities, intents, and activities of foreign entities is underscored by Shulsky and Schmitt (2023). They prioritize the incorporation of human intelligence (HUMINT) with technical gathering techniques such as signals intelligence (SIGINT) and analysis of open-source intelligence (OSINT). In his work published in 2022, Clark argues in favour of adopting a target-centric strategy that involves cooperation among several stakeholders to improve intelligence gathering and evaluation procedures. The importance of information gathering within the wider intelligence cycle to facilitate efficient risk assessment and mitigation is underscored by Sims (2021).

A wide variety of activities, from covert operations and technical gathering to the examination of publicly available data, are utilized to gather intelligence, as Warner (2024) points out. The main goal of intelligence gathering is to acquire knowledge about the capabilities, intentions, and plans of adversaries, therefore equipping decision-makers with the essential information to predict and successfully address threats.

Effective intelligence gathering is crucial for making well-informed decisions in many fields. Buthelezi (2024) analyses the crucial function of intellect in preventing crime and enforcing the law, emphasizing the significance of strong analytical skills. The significance of precise and prompt intelligence in guiding national security decisions is underscored by Hasan (2022).

Omand (2022) conceptualizes intelligence gathering as a methodical procedure designed to provide information for security operations. He emphasizes the need to follow ethical and legal principles, particularly in situations such as

Nigeria where the task of reconciling security and human rights is formidable.

In his report, Herman (2021) highlights the significance of intelligence in mitigating ambiguity within intricate security contexts, therefore facilitating a more profound comprehension of the intents and capabilities of adversaries. He promotes the incorporation of recent technical developments with conventional intelligence approaches to tackle changing security issues. The importance of efficient intelligence sharing, and inter-agency cooperation is emphasized by Pillar (2020), especially in situations such as Nigeria where cooperative endeavours are vital.

This study by Aldrich (2021) investigates the profound influence of technology and globalization on intelligence operations, resulting in changes to the techniques of gathering and using data. To effectively counter the ever-changing nature of security threats, he emphasizes the requirement of agility and adaptability in intelligence operations.

A study by Capie (2020) examines how intelligence enhances defense collaboration between countries, therefore promoting regional security and protecting national sovereignty. Neo (2022) examines the function of intelligence in combating misinformation and disinformation networks, emphasizing its increasing significance in the era of digital technology. Specifically, Luong (2020) and Sinpeng (2020) analyze the function of intelligence in fighting international crime and tackling the obstacles presented by digital media and internet censorship, respectively.

African academics provide invaluable insights into the field of intelligence gathering. Vale (2021, 2023) highlights the significance of intelligence gathering in ensuring state security and managing regional stability, promoting a comprehensive approach that encompasses all African countries. The significance of combining security imperatives

with human rights safeguards is underscored in Madlingozi's (2021) analysis of the legal and constitutional frameworks controlling intelligence operations.

North African experts underscore the need of intelligence gathering in effectively tackling regional security issues. Khelil (2022, 2023) supports the incorporation of artificial intelligence (AI) and big data analytics to further improve intelligence operations. El-Naggar (2021, 2022, 2023) emphasizes the central importance of intelligence in the fight against terrorism and political instability, while also drawing attention to the impact of regional politics on intelligence operations. Hassan (2020, 2021, 2023) emphasizes the requirement of adaptive and responsive intelligence operations to effectively tackle changing threats. Youssef (2020, 2021, 2022) analyses the difficulties associated with intelligence management in North Africa, such as the overwhelming amount of data, heightened competition among agencies, and legal limitations. The study conducted by Boudiaf (2021, 2022, 2023) underscores the influence of regional wars and political instability on intelligence operations, underscoring the imperative of establishing robust intelligence frames.

The Boko Haram insurgency highlights the ongoing security issues in Nigeria, highlighting the need to gain a more comprehensive knowledge of extremist organisations and their influence on national security (Onuoha, 2011; Ajodo-Adebanjoko et al., 2019). The effectiveness of security responses to such conflicts underscores the requirement of ongoing capacity development to successfully tackle emerging threats (TERZUNGWE et al., 2024).

Challenges in data collecting, such as limited availability, underutilization, and inconsistencies in data administration, hinder the effectiveness of

intelligence operations in Nigeria (Awotayo, 2023).

Informing decision-making processes in policymaking, military operations, law enforcement, and crisis management, intelligence collecting is of paramount importance (Houghton, 2020; Barnett, 2021; Marrin, 2022; Beehner, 2023; Ratcliffe, 2020; Bjelopera, 2023).

The many perspectives provided by specialists from throughout the globe emphasize the intricate difficulties and possibilities linked to intelligence gathering in a constantly changing global environment.

## **2.2 Types of Intelligence**

### **2.2.1 Human Intelligence (HUMINT)**

Human Intelligence (HUMINT) is a fundamental element of both national security and intelligence activities. Qualitative research is the systematic gathering and examination of data by direct interpersonal contacts. The significance of HUMINT resides in its ability to offer an intricate understanding of events, motivations, and intentions, which are sometimes unachievable strictly through technological methods (Johnson, 2019).

The application of Human Intelligence (HUMINT) has been crucial in counter-terrorism efforts targeting Boko Haram and other radical organizations. The provision of crucial intelligence on the whereabouts, intentions, and actions of persons by informants and undercover operatives has facilitated the disruption of planned attacks and the interception of communication lines (Onapajo & Uzodike, 2022).

Human Intelligence (HUMINT) has played a crucial role in comprehending the fundamental grievances, ethnic tensions, and external factors that contribute to internal conflicts and insurgencies, especially in the Middle Belt and

southern regions. The acquisition of this knowledge has influenced the development of tactics that target the fundamental reasons behind these disputes and promote confidence among local populations (Olaniyan & Okunola, 2021).

Moreover, HUMINT has provided insight into political instability and corruption, revealing complex collaborations between powerful politicians and criminal organizations, and revealing illegal actions that weaken security measures. Acquisition of this knowledge is crucial for guiding strategic decision-making and fostering responsibility (Adebanwi & Obadare, 2019).

Nevertheless, human intelligence (HUMINT) activities in Nigeria encounter obstacles because of the intricate socio-political environment and the possibility of deception. The existence of multiple ethnic groups and regional inequalities can affect the ability to develop trustworthy sources and maintain operational security (Akinyetun & Olaniyi, 2020).

### 2.2.2 Signal Intelligence (SIGINT)

Signals intelligence (SIGINT) is the comprehensive interception and analysis of electronic signals and communications that plays a crucial role in contemporary intelligence operations. Analytics is the collection and processing of diverse information to extract practical insights about possible threats and adversary actions.

Experts and practitioners in Nigeria provide a wide range of viewpoints on the significance and use of SIGINT for the advancement of national security. Professor Femi Amao (2023), a prominent expert in the field of cybersecurity asserts that, the significance of SIGINT in the fight against terrorism and organized crime lies in its ability to monitor and disrupt communication networks. Lieutenant General Babagana Monguno (retd.) (2022), the former National Security Adviser, emphasizes the

wider role of SIGINT in comprehending the intents and capabilities of enemies, hence facilitating pre-emptive actions to protect national interests.

In The significance of SIGINT in bolstering military operations, counter-terrorism activities, and national security initiatives is highlighted by the Defence Intelligence Agency (DIA) (2024). Michael Ejiofor (2020), a former Director of the Department of Security and Intelligence (DSS), emphasizes the use of this technology in counterintelligence operations, including in the identification and neutralization of foreign spies and operatives. Brigadier General Sani Usman (2021) highlights the operational importance of SIGINT in military operations, as it facilitates the gathering of intelligence on enemy movements, assessment of threats, and formulation of tactical decisions.

Dr. Kemi Okenyodo (2024), a cybersecurity expert at the NCC, emphasizes the increasing significance of Signals Intelligence (SIGINT) in safeguarding vital infrastructure and national security in the era of digital technology. She highlights the significance of its function in detecting and reducing cyberattacks and protecting highly confidential data.

### 2.2.3 Electronic Intelligence (ELINT)

Electronic Intelligence (ELINT) is a specialised branch of Signals Intelligence (SIGINT) that investigates electronic signals that aren't used for contact, like radar and weapon system emissions (Johnson, 2018). The goal is to learn more about the features and how foreign organisations use computer systems (Smith et al., 2021). This information is very important for improving military tactics, strategic planning, and making choices at the national and regional levels (Brown, 2020).

Scholars and security experts from Africa stress how important ELINT is to the safety of the area



(Adetula, 2020). They stress how important it is to understand the electronic systems of other countries to improve military operations, strategy planning, and decision-making at the national and regional levels (Olaniyan & Yahaya, 2022). Experts also stress how important it is to include ELINT in national security plans, deal with security issues in the area, and encourage cooperation in maintaining peace and safety (Onuoha, 2019).

As technology changes all the time in ELINT, new ideas and ways of doing things need to be constantly tested and improved to make sure they work (Kumar, 2023).

#### 2.2.4. Open-Source Intelligence (OSINT)

Open-Source Intelligence (OSINT) is the methodical gathering and examination of publicly accessible information (Petherick, 2023). Within several fields such as national security, corporate intelligence, and law enforcement, it possesses considerable importance (Lazaridou-Chatzigoga et al., 2021). Accredited experts globally highlight the significance of this methodology in tackling a diverse range of problems, including combating terrorism and extremism, examining social and political patterns, and improving situational awareness in different security situations (Racz, 2022).

Open-Source Intelligence (OSINT) is acknowledged as an essential element of Nigeria's national security architecture (Adetula, 2020). By providing vital insights into the intents and capabilities of adversaries, this technology allows for proactive measures to minimise risks and protect national interests (Olaniyan & Yahaya, 2022). Strategically, Open-Source Intelligence (OSINT) emphasises its impact on the development of national security policies and decision-making procedures (Onuoha, 2019).

#### 2.2.5. Social Media Intelligence (SOCMINT)

The acquisition and analysis of data obtained from social media platforms are the primary objectives of Social Media Intelligence (SOCMINT), a subset of OSINT (Apuke & Tunca, 2023). It analyses user-generated content, interactions, and trends to acquire insights into public sentiment, emergent concerns, and influential individuals or groups (Osisanwo et al., 2021). The widespread use of social media platforms for communication and information dissemination is the primary reason for the emergence of SOCMINT (Omoniyi & Adewumi, 2022).

Sophisticated analytics and machine learning techniques are employed to manage, capture, and analyse social media data (Chatfield et al., 2019). SOCMINT is employed in a variety of domains, such as crisis management, brand and reputation management, political and geopolitical analysis, counterterrorism, and law enforcement (Apuke & Tunca, 2023).

Although SOCMINT offers valuable insights, it also presents challenges related to the complexity of analysing enormous social media datasets, data privacy, and ethics (Osisanwo et al., 2021). It is imperative to comply with legal and ethical standards and implement rigorous verification and validation procedures on these platforms, given the prevalence of misinformation and disinformation (Brennan et al., 2020).

#### 2.2.6. Geospatial Intelligence (GEOINT)

Geospatial Intelligence (GEOINT) refers to the systematic gathering, examination, and representation of data that is indexed by geographical coordinates to facilitate intelligence operations (Olaniyan & Yahaya, 2022). The method employs satellite photos, maps, and GIS technologies to detect geographical patterns and correlations (Olaniyan, 2021). Geospatial

Intelligence (GEOINT) has wide-ranging uses in several domains such as security, disaster

management, urban development, and environmental surveillance (Adetula, 2020).

Experts highlight several applications of GEOINT, including providing information for national security and defence strategy, improving situational awareness and decision-making in disaster response, and aiding humanitarian aid operations (Onuoha, 2019). Analysing geographical patterns and linkages using geospatial methods is essential for enhancing strategic decision-making and offering significant insights for transdisciplinary initiatives (Osisanwo et al., 2021).

Geographic Information and Intelligence (GEINT) in Nigeria is customised to tackle local requirements and difficulties (Apuke & Tunca, 2023). Through the identification of adversaries' strengths and weaknesses, the analysis of spatial patterns and relationships within the African environment serves to improve defence and regional security (Omoniyi & Adewumi, 2022). Furthermore, it facilitates peacekeeping and strengthens security collaboration endeavours (Onuoha, 2019). Furthermore, GEOINT serves the purpose of overseeing and mitigating non-state entities and regional hostilities, so enhancing military and strategic decision-making (Olaniyan & Yahaya, 2022).

An in-depth examination of several intelligence domains—HUMINT, SIGINT, ELINT, OSINT, SOCMINT, and GEOINT—reveals their distinct features and changing functions in tackling modern security issues (Gill & Mathur, 2023).

Given the continuous progress in technology and the rise of novel security risks, the importance of these intelligence tasks is expected to increase (Racz, 2022).

### **2.3 Theoretical Framework- The Network Theory (TNT)**

Systematic Network Theory and Nigerian Intelligence Gathering

Network Theory, which studies the relationships between people and organizations in a network, can help Nigeria improve its intelligence collection and use. Network Theory helps increase situational awareness and strategic decision-making by assessing danger actors, security agencies, and local population linkages.

The Network Theory can identify and analyse complex relationships, which is important in Nigeria's security situation. The Network Theory helps intelligence agencies understand the relationships between terrorists, organized crime syndicates, and cyber criminals. This data highlights key people, facilitators, and operational hubs that can destabilize the network (Sageman, 2021; Onuoha, 2019). Additionally, network theory can be used to investigate Nigerian security service links. Analysing collaboration and communication networks can reveal intelligence architecture flaws (Olaniyan & Yahaya, 2022). Improving these networks can improve security response by improving coordination and intelligence exchange.

Success requires local expertise and community engagement in intelligence operations (Albert, 2021). The Network Theory may show how local actors and security agencies are connected, highlighting the potential of community networks to gather information and increase situational awareness. Indigenous knowledge and community contributions to security challenges are valued in this approach.

The Network Theory emphasizes information transmission inside a network, which is essential for intelligence operations decision-making. Analysing intelligence network information flow reveals bottlenecks and inefficiencies. This delivers critical data to the right nodes quickly

(Treverton, 2021). Security organizations can respond faster and more effectively to new threats.

Prior studies have noted that policymakers and security agencies pay insufficient attention to intelligence applications (Olaniyan & Yahaya, 2022). Network Theory can help address this issue. Mapping can explain how intelligence flows from data sources to decision-makers and how it affects policies and actions. This can improve intelligence applications to proactive and preventive actions, improving security operations.

A comprehensive analytical framework is needed to understand non-traditional risks such as organised crime, cybercrime, and environmental degradation (Adetula & Adeoye, 2021). Network Theory helps understand these risks by mapping entity relationships and identifying critical network locations. This helps create targeted strategies to deconstruct criminal networks and reduce their power.

TNT in intelligence collecting has ethical and legal issues (Onuoha, 2023). Analysis of intelligence network linkages and power dynamics using Network Theory. This research can discover key oversight and accountability nodes. Doing so strengthens monitoring and assures ethical and legal intelligence activities (Heuer, 2020). Visualizing the intelligence network can also help identify human rights breaches. This allows for strategies to mitigate risks and defend human rights (Borgatti et al., 2013).

TNT allows comparisons of national security issues. By using this paradigm to evaluate intelligence networks in different situations, researchers can identify effective methods and tactics, leading to more efficient intelligence procedures in Nigeria (Freeman, 1978). Nigeria's intelligence architecture can benefit from studying other nations' intelligence networks and strategies (Watts & Strogatz, 1998).

Network Theory improves Nigerian intelligence collection and use flexibly. Examining intelligence network connections and exchanges reveals key players, information dissemination patterns, and flaws. This knowledge can be utilized to build security solutions for terrorism, organized crime, cybercrime, and environmental damage. Network Theory can also help address ethical and legal challenges, promote accountability and supervision, and enable comparative study to learn from best practices in other environments.

### 2.3.1 Historical Overview of Intelligence in Nigeria

Throughout history, intelligence has been an essential instrument for rulers, states, and empires in upholding territorial integrity, settling internal disputes, and guaranteeing stability. Intelligence operations have played a crucial role in government and security spanning from ancient civilizations to contemporary nation-states. Throughout pre-colonial Africa, a range of espionage and surveillance methods were used to safeguard communities, defend regions, and monitor opponents.

Intelligence gathering in Nigeria, characterized by its heterogeneous ethnic groupings and abundant cultural legacy, extensively depended on informal networks. Pre-colonial kingdoms and empires employed scouts, spies, and informants to collect intelligence on competing powers, conduct surveillance on internal opposition, and prepare for military operations. The establishment of these intelligence networks frequently occurred via alliances, trade partnerships, and social networks (Falola & Heaton, 2022).

The emergence of European colonisation throughout the late 19th and early 20th centuries introduced a more organised and systematic method of collecting intelligence in Nigeria. To exert control over its extensive African domains,

the British colonial authorities developed intelligence networks to monitor political activity, quelling uprisings, and acquiring information on local leaders and movements that potentially endangered colonial authority. The efficacy of this intelligence strategy allowed the British to retain dominion over Nigeria notwithstanding opposition from many indigenous factions (Adebayo, 2023).

Throughout the colonial period, intelligence activities in Nigeria were predominantly motivated by the imperative to safeguard British economic and political interests. The British depended on a network of indigenous informants, colonial law enforcement, and military intelligence personnel to collect intelligence on nationalist groups, occupational strikes, and other actions that had the potential to weaken colonial power. During the 1940s, the colonial authority founded the Nigerian Security Organisation (NSO), which served as a forerunner to contemporary Nigerian intelligence organizations. Its primary objective was to collect intelligence on political actions and quell anti-colonial movements (Agbibo, 2020).

Nevertheless, colonial intelligence activities were not exempt from these constraints. An inherent deficiency in the British intelligence machinery in Nigeria was their limited comprehension of the intricate political dynamics, languages, and cultures of the region. Occasionally, this lack of cultural understanding resulted in intelligence failures and misjudgements, intensifying conflicts between the colonial administration and indigenous populations (Smith, 2021).

### 2.3.2 Organisational Structure of Intelligence in Nigeria After Independence

Upon Nigeria's attainment of independence in 1960, the newly formed nation assumed responsibility for the colonial intelligence infrastructure. Nevertheless, the Nigerian

government acknowledged the necessity of overhauling and strengthening its intelligence capabilities to tackle the distinct obstacles faced by a sovereign state.

During the initial stages of independence, Nigeria's intelligence apparatus was somewhat basic, with the Nigerian Police Force mostly tasked with collecting intelligence. Nevertheless, as a reaction to the increasing internal and external security dilemmas, the nation developed dedicated intelligence agencies.

Within the military administration of General Ibrahim Babangida in 1986, the National Security Organization (NSO) underwent a restructuring process that resulted in the establishment of three separate intelligence agencies: the State Security Service (SSS), which is currently referred to as the Department of State Services (DSS), the National Intelligence Agency (NIA), and the Defence Intelligence Agency (DIA). The restructuring was a notable achievement in the development of Nigeria's intelligence sector since it facilitated enhanced collaboration and specialization among the agencies in charge of internal security, foreign intelligence, and military intelligence (Akinyemi, 2020).

The Department of State Security (DSS) is responsible for conducting domestic intelligence and counterintelligence activities, with a specific emphasis on internal security that encompasses counterterrorism, counterinsurgency, and safeguarding vital government infrastructure and personnel. According to Alao (2021), the DSS assumes a pivotal function in the collection of intelligence about political activities, organized crime, and other jeopardies to national security.

The NIA's primary obligations include gathering foreign intelligence and conducting counterespionage operations. The agency analyses global events that could affect Nigeria's national

security, collects intelligence on other governments and organisations, and carries out clandestine activities overseas. The NIA engages in cooperative efforts with other international intelligence organizations to effectively tackle transnational security challenges (Obasi, 2022).

The DIA serves as a source of intelligence assistance to the Nigerian Armed Forces, with a specific emphasis on military intelligence. The system engages in reconnaissance, collects data on possible military risks, and produces intelligence analysis to bolster military planning and operations. The DIA plays a crucial role in Nigeria's counterinsurgency operations, namely in combating Boko Haram and other armed criminal organisations (Olabanji & Omitola, 2023).

Notwithstanding the creation of these specialised agencies, Nigeria's intelligence system after gaining independence has encountered numerous obstacles. An issue of significant concern has been the absence of effective coordination and communication among the several agencies. The lack of extensive intelligence exchange across the DSS, NIA, and DIA has frequently led to deficiencies in intelligence coverage and delays in addressing security risks. Furthermore, the Nigerian intelligence community has faced criticism for its tendency to politicize, as intelligence services have been accused of aligning themselves with political elites rather than prioritizing national security (Adebayo, 2021).

### 2.3.3 Role of Intelligence in National Security

#### Counter-terrorism and Prevention.

The gathering, analysis, and distribution of intelligence to prevent and defeat acts of terrorism are essential components of counterterrorism, a fundamental aspect of national security strategy worldwide. To comprehend, disrupt, and dismantle terrorist networks, intelligence is of paramount importance.

Counterterrorism intelligence is obtained from a wide range of sources, each providing distinct and useful perspectives on the battle against terrorism. Human intelligence (HUMINT) refers to the gathering of information from human sources, including informants and undercover agents, to get direct understanding of the tactics, operations, and internal workings of terrorist organisations (Byman, 2021). Signal intelligence (SIGINT) is the interception and analysis of electronic communications, which allows for the surveillance of terrorist communications and the detection of possible threats (Treverton, 2021). Sophisticated machine learning algorithms have significantly improved the capacity to analyze large volumes of intercepted communications, identify patterns, and predict possible terrorist activities (Buchanan & Kehoe, 2021). Geographical intelligence (GEOINT) is the systematic gathering and examination of visual representations and spatial data, which offers immediate and accurate information regarding the movements and whereabouts of terrorist networks. Critical for strategizing counterterrorism operations and monitoring terrorist activities, this intelligence is indispensable (Sageman, 2021; Bergen, 2021). Synergistically utilizing various intelligence sources promotes a thorough comprehension of the danger environment and enables focused interventions.

#### Intelligence Analysis: From Threat Assessment to Network Mapping

Intelligence analysis converts unprocessed data into executable intelligence, crucial in counterterrorism endeavours. Threat assessment, an essential component of intelligence analysis, is the evaluation of the possible dangers presented by terrorist groups and the comprehension of their capacities and objectives (Clarke & Newman, 2020). Consequently, intelligence agencies can give priority to safeguarding high-value targets,

such as vital infrastructure and public areas, and efficiently distribute resources. The utilization of historical data and current intelligence in predictive analysis approaches enables the anticipation of prospective terrorist attacks, therefore promoting pre-emptive countermeasures and improved readiness (Enders & Sandler, 2020). Network analysis is a crucial method for comprehending the structure and identifying fundamental personnel, including leaders, funders, and operatives, within terrorist groups by examining their relationships and interactions (Sageman, 2021). In addition, network analysis can reveal vital support networks for terrorist operations, such as funding, recruitment, and logistics, allowing for focused measures to undermine their capacities (Felbab-Brown, 2021).

#### Intelligence Sharing and Dissemination:

Seamless intelligence sharing among different intelligence organizations and partner states is crucial for effective counterterrorism. Inter-agency cooperation enables the prompt and effective sharing of information, promoting a comprehensive vision of terrorism risks (Buchanan & Kehoe, 2021). Effective international collaboration, achieved by the exchange of intelligence and synchronized counterterrorism operations, is essential in addressing transnational terrorist risks and overseeing their actions that extend beyond national borders (Sageman, 2021). Accurate and prompt distribution of intelligence to policymakers is similarly crucial, as it furnishes vital information for formulating counterterrorism programs and making well-informed decisions. Systematic briefings and reports, which emphasize the present state of threats and possible hazards, guide the development of national security strategies and the distribution of resources (Treverton, 2021). Empowering security personnel with precise and actionable intelligence

on impending threats, particular targets, and possible attack techniques enables them to respond with effectiveness and decisiveness (Fingar, 2021).

#### 2.3.4 The Role of Intelligence in Combating Insurgency Case Studies:

The national security environment of Nigeria has been influenced by a succession of intricate and dynamic security challenges during the last twenty years. The collection of intelligence has become a vital instrument in addressing these problems, yet flexible approaches and efficient collaboration across security agencies continue to be essential. Three significant security challenges in Nigeria are analysed in this paper: the Boko Haram insurgency, abduction and banditry, and cyber threats. Every individual case study highlights the essential and irreplaceable function of intelligence in tackling matters of national security.

#### Boko Haram Insurgency

The Boko Haram insurgency, formally referred to as Jama'atu Ahlis Sunna Lidda'awati wal-Jihad (JAS), is a very consequential and prolonged security issue in Nigeria. Emerging in 2002 in northern Nigeria as a radical Islamist group, Boko Haram's resistance to Western education and support for an Islamic state propelled it to evolve into a violent insurgency under the leadership of Abubakar Shekau in 2009 (Zenn, 2020). The group employs a variety of strategies involving acts of violence, such as suicide bombings, large-scale abductions, killings, and assaults on both military and civilian targets.

The notorious 2014 kidnapping of more than 276 schoolgirls from Chibok intensified Boko Haram's reputation, attracting worldwide scrutiny to the insurgency and underscoring the Nigerian government's difficulties in controlling the group. Despite active military operations, Boko Haram continues to exist in northeastern Nigeria and the

surrounding countries (Onuoha, 2021).

Security intelligence has played a crucial role in Nigeria's counterterrorism operations. The effective monitoring and neutralisation of Boko Haram's leadership has been made possible by collaboration with international allies. The intelligence gathered in 2016 resulted in the apprehension and subsequent removal of Abu Musab Al-Barnawi, the former deputy commander and originator of the ISWAP extremist organisation. According to Agbiboa (2021), the use of local information and surveillance enabled the successful execution of operations against Boko Haram, leading to the apprehension or demise of numerous senior members.

Persistent issues include untimely intelligence sharing and insufficient use of local intelligence, as seen by the attacks on villages in Borno State when security personnel arrived late because of delayed intelligence (Akinola, 2022). Permeable borders exacerbate the complexity of intelligence operations.

Although foreign intelligence and collaboration, especially from the US, France, and the UK, have strengthened Nigeria's capacities, continuous efforts in developing local intelligence networks and improving coordination across national and regional forces are required for long-term success (Alli, 2022).

#### Kidnapping and Banditry

The incidence of kidnapping and banditry has significantly increased in northern and central Nigeria, mostly motivated by economic incentives and ethnic tensions. The business of kidnapping for ransom has generated significant profits since populations are being kept captive and the ransom demands continue to climb. According to Okoli and Ugwu (2021), there were more than 2,200 instances of kidnapping and 5,000 cases of abduction documented in 2020.

Banditry, associated with ethnic unrest, land conflicts, and theft of livestock, instils fear in rural communities in the northwest. Militant organizations operate without facing consequences in extensive, uncontrolled territories, therefore restricting the effectiveness of security forces.

Effective intelligence-led operations have resulted in notable achievements, such as the successful rescue of more than 300 schoolboys in Kankara in 2021, underscoring the significance of local intelligence (Amnesty International, 2021). Nevertheless, obstacles persist.

Insufficient confidence between communities and security forces, together with corruption within the security sector, obstructs intelligence operations. Due to communities' fear of retaliation or lack of confidence in the government's security, the availability of actionable intelligence is restricted (Okoli & Ugwu, 2021). Corrupt security officers collaborating with criminals exacerbates operational weaknesses and diminishes public trust (Agbiboa, 2021).

The implementation of government programs such as community policing and drone technology has logistical and operational challenges. Effectively combating kidnapping and banditry necessitates allocating resources to enhance local intelligence skills, cultivating trust, and tackling socio-economic incentives that contribute to criminal behaviour.

#### Cyber Threats

The growing digital interconnection in Nigeria has resulted in a significant rise in cyber risks. Frequent and sophisticated cyberattacks that target government organizations, financial systems, and key infrastructure result in financial losses and present security threats. According to

PwC Nigeria (2021), Nigeria encountered more than 3,500 cyberattacks in the year 2020, leading to financial damages of over \$500 million.

The main forces behind cybercrime encompass the widespread adoption of digital devices, the increased availability of internet connectivity, and the expansion of online financial activities. The activities of cyber criminals encompass phishing, ransomware attacks, identity theft, and online fraud, therefore exerting adverse effects on individuals, enterprises, and national security.

The creation of the Nigerian Cybersecurity Coordination Centre (NCCC) in 2021 indicates the government's acknowledgement of the necessity to strengthen cyber intelligence capacities. According to PwC Nigeria (2021), the NCCC effectively organizes activities, engages in global collaboration, and actively monitors potential risks in real time.

Cutting-edge technology such as artificial intelligence, machine learning, and big data analytics assist in the identification and examination of cyber threats. Artificial intelligence (AI) technologies surveil social media platforms to detect radicalisation and possible acts of violence (Olumide, 2022).

Long-standing obstacles include a dearth of proficient cybersecurity experts and insufficient laws and enforcement of cybersecurity. The disparity in skills hampers operational efficiency, while inconsistent implementation and insufficient public awareness expose Nigeria to vulnerability (PwC Nigeria, 2021; Olumide, 2022).

International collaboration, facilitated by alliances with INTERPOL and UNODC, enhances Nigeria's cyber intelligence capacities and enables synchronised actions against transnational cybercrime (Alli, 2022).

### 2.3.5 Challenges in Intelligence Gathering

Strategic cooperation among intelligence agencies and smooth synchronization with law enforcement are of utmost importance for safeguarding national security. Nevertheless, numerous barriers frequently obstruct this vital collaboration, impeding the efficiency and efficacy of intelligence operations. This academic analysis examines the coordination and infrastructural issues, reviewing their significant consequences and possible solutions, based on up-to-date research and insights.

#### Inter-Agency Rivalry

The presence of inter-agency rivalry, driven by the battle for few resources and a lack of trust, is a substantial obstacle to achieving efficient coordination. The prioritization of individual interests by agencies over common goals might result in inefficiencies and duplicative activities (Johnson, 2021). Intense competition for financial, human, and technological resources might impede cooperation, as agencies aim to amass resources to improve their position (Treverton, 2021). Furthermore, apprehensions about the security of data and the possibility of its abuse can contribute to hesitancy in sharing information, therefore hindering the collaborative intelligence endeavour (Fingar, 2021).

#### Communication Barriers

Timely and efficient communication is crucial for intelligence operations, yet obstacles in communication might impede collaboration between different agencies. Potential delays, inefficiencies, and missed opportunities might arise from technological incompatibilities, cybersecurity issues, and bureaucratic procedures (Johnson, 2021; Holt et al., 2021). Elaborate bureaucratic processes and inflexible hierarchical systems can additionally hinder the transmission of knowledge, so impacting the promptness and pertinence of intelligence (Treverton, 2021; Clarke



& Newman, 2020).

#### Jurisdictional Issues

In intelligence operations, the presence of overlapping jurisdictions among agencies can lead to misunderstandings and disagreements about responsibilities and authority. Legal disputes about jurisdiction can result in redundant work, squandered resources, and a lack of unified strategy (Buchanan & Kehoe, 2021). Divergences in legal frameworks and laws among different jurisdictions might impede the exchange of information and cooperation, especially in the context of foreign intelligence assistance (Holt et al., 2021).

#### Differences in Organizational Culture

Organizational culture, which includes values, attitudes, and practices, has a substantial influence on inter-agency collaboration. Divergent operational ideologies, intelligence approaches, and professional competitions can generate friction and hinder efficient coordination (Johnson, 2021; Clarke & Newman, 2020). In certain cases, the presence of strong agency loyalty and individual career aspirations can overshadow the collaborative intelligence endeavour, resulting in less-than-optimal decision-making and diminished operational efficiency (Buchanan & Kehoe, 2021; Fingar, 2021).

#### Challenges in infrastructure

Infrastructural constraints present intelligence agencies with significant obstacles. Resource constraints, especially in emerging countries, limit the extent of intelligence activities and hinder the procurement of cutting-edge technology and the training and development of staff (Ekekwe, 2023; Johnson, 2021; Treverton, 2021). Deploying obsolete equipment can undermine situational awareness and data accuracy, while insufficient data analysis tools might impede the recognition of

trends and well-informed decision-making. Furthermore, the lack of adequate technology presents cybersecurity threats, therefore exposing intelligence systems to potential compromises (Clarke & Newman, 2020; Treverton, 2021; Holt et al., 2021).

#### Technological Advancements and Challenges

The exponential rate of technical progress offers intelligence organizations both prospects and obstacles. Although technology can improve data gathering, analysis, and operational capacities, it also brings about complicating factors. Intelligence agencies must confront the imperative to consistently adjust to emerging technology, minimize cyber risks, handle extensive volumes of data, and uphold continuous training and adaptation.

The ongoing advancement of technology imposes a financial strain on agencies, necessitating significant capital outlays in research and development as well as upgrades to maintain a competitive edge over opponents (Betts, 2020; Johnson, 2021; Fingar, 2021). The growing dependence on digital technology significantly amplifies the vulnerability to cyberattacks, thereby requiring strong cybersecurity protocols (Holt et al., 2021; Clarke & Newman, 2020).

The rapid and exponential increase in data poses difficulties in efficiently managing and analysing it. Robust data analytics and artificial intelligence are essential for the analysis and extraction of meaningful insights from extensive databases (Treverton, 2021). Integration of data from various sources and formats necessitates advanced technology and interoperability standards (Fingar, 2021).

Moreover, intelligence personnel must participate in ongoing training and skill enhancement to remain up to date with technological progress. The recruitment and retention of professionals

possessing technical expertise in cybersecurity, artificial intelligence (AI), and data analytics are of paramount importance (Buchanan & Kehoe, 2021; Holt et al., 2021). Equally crucial is organizational adaptability, which necessitates the modification of conventional hierarchical frameworks to promote agility and innovation (Treverton, 2021).

### 2.3.6 Critical Assessment of Intelligence Gathering Efforts in Nigeria

The collection of intelligence is essential for safeguarding national security, as it contributes to the development and execution of effective policies. Notwithstanding the significant achievements of Nigerian intelligence agencies in combating terrorism, their overall efficacy is nevertheless hindered by various obstacles. Major intelligence-led successes in the battle against Boko Haram and ISWAP include the apprehension of senior commanders (Zenn, 2021). Yet, development has been impeded by inter-agency competition, delayed information exchange (Onuoha, 2021), and insufficient community involvement. Tackling kidnapping and banditry presents similar challenges owing to permeable borders, extensive unregulated areas, and corruption among security personnel (Okoli & Ugwu, 2021; Agbiboa, 2021). Although significant progress has been achieved in enhancing cyber intelligence capabilities, the efficacy of programs such as the NCCC is hindered by limited resources and a dearth of comprehensive cybersecurity legislation (PwC Nigeria, 2021).

The national security strategy of Nigeria is subject to substantial influence from intelligence, which plays a crucial role in establishing counterterrorism policies and regional cooperation (Onuoha, 2021; Alli, 2022). Yet, obstacles remain, such as the politicization of intelligence (Adebayo, 2021; Akinola, 2022) and the insufficient incorporation of intelligence into

the formulation of long-term policies (Obasi, 2022). Despite the NCPS's advancements in cybersecurity, its execution is hindered by resource constraints and a dearth of public knowledge (PwC Nigeria, 2021; Olumide, 2022).

Public perception and trust are of paramount importance for intelligence services. Perceptions of ineffectiveness in averting assaults, together with concerns about transparency, accountability, and human rights violations (Amnesty International, 2021), have undermined public confidence. Community involvement initiatives aimed at rebuilding trust have shown some results, especially in regions afflicted by banditry and insurgency (Okoli & Ugwu, 2021). Although the public views cyber intelligence in a more favourable light, there is still a need for increased public knowledge and education on cybersecurity (Olumide, 2022).

An evaluation of Nigeria's intelligence activities in comparison to international standards might provide invaluable insights for improving its intelligence infrastructure. An analysis of effective strategies and approaches used by countries such as the United States, Israel, and the United Kingdom can reveal possible areas for enhancement in Nigeria's intelligence architecture.

### Global Best Practices in Intelligence Gathering

#### Organizational Structure and Interagency Coordination

A well-organized structure that fosters effective interagency coordination is a hallmark of successful intelligence operations globally. The United States, for example, employs a decentralized intelligence system comprising multiple agencies, including the Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), National Security Agency (NSA), and the Department of Homeland Security (DHS) (Lowenthal, 2022). These agencies

collaborate under the auspices of the Office of the Director of National Intelligence (ODNI), ensuring intelligence sharing and integration across various domains.

Similarly, the United Kingdom's intelligence apparatus, comprising MI5 (domestic security), MI6 (foreign intelligence), and GCHQ (signals intelligence), operates under the coordination of the Joint Intelligence Committee (JIC), ensuring the synthesis and timely dissemination of intelligence to decision-makers (Johnson, 2020).

Israel's intelligence community is also recognized for its high degree of coordination and integration. Mossad (foreign intelligence), Shin Bet (domestic security), and Aman (military intelligence) work in close collaboration, prioritizing the prevention and pre-emption of threats.

The Israeli model emphasizes rapid decision-making and flexibility, proving instrumental in countering terrorism and regional threats (Bar-Joseph & McDermott, 2021).

In contrast, Nigeria's intelligence community faces challenges in coordination and communication between agencies. The Department of State Services (DSS), National Intelligence Agency (NIA), and Defence Intelligence Agency (DIA) often operate in silos, with limited information sharing. This lack of interagency coordination has hindered effective threat response, as exemplified by the failure to prevent the 2014 Chibok schoolgirls' abduction despite prior intelligence (Agbiboa, 2021). Establishing a centralized body, akin to the ODNI or JIC, could ameliorate coordination and information sharing within Nigeria's intelligence agencies.

#### Human Intelligence (HUMINT) and Community Engagement

Human intelligence (HUMINT) remains invaluable, especially where technology is limited, or local

context is crucial. The United States and Israel effectively leverage HUMINT through extensive informant and collaborator networks (Marrin, 2022; Bar-Joseph & McDermott, 2021). Israel's deep intelligence networks within Palestinian territories and neighbouring countries enable it to pre-empt attacks through timely intelligence.

Nigeria faces challenges in utilizing HUMINT, particularly in insurgency-affected regions. Mistrust between communities and security forces, coupled with difficulties in building informant networks, hampers intelligence gathering (Akinyemi, 2022). Enhancing community engagement and trust is crucial for improving Nigeria's HUMINT capabilities.

#### Technological Capabilities and Cyber Intelligence

Technological capabilities, especially in signals intelligence (SIGINT) and cyber intelligence, are critical in the digital age. The U.S. and UK lead in this domain, with the NSA and GCHQ employing advanced surveillance technologies and tools like satellite imagery, data analytics, and AI (Lowenthal, 2022). Israel's Unit 8200 excels in cyber intelligence and electronic warfare, enabling it to counter cyber threats and maintain a technological advantage (Frenkel, 2022).

Nigeria lags in technological intelligence capabilities. While efforts have been made to enhance cyber intelligence infrastructure, limitations in resources, skilled personnel, and infrastructure persist (PwC Nigeria, 2021). Investing in advanced technologies, developing a skilled workforce, and strengthening the legal framework for cybersecurity are imperative for Nigeria.

#### Counterterrorism Strategies

Counterterrorism heavily relies on intelligence gathering. Global leaders like the U.S. and Israel employ intelligence-driven strategies focusing on

pre-emptive action, rapid response, and military-intelligence coordination. The U.S. utilizes drones for targeted killings and integrates intelligence into military operations (Johnson, 2020). Israel prioritizes pre-emptive strikes and targeted operations, with intelligence agencies playing a central role in identifying and neutralizing threats (Bar-Joseph & McDermott, 2021).

Nigeria's counterterrorism efforts against Boko Haram and ISWAP also depend on intelligence, but their effectiveness is limited by challenges such as slow response to intelligence warnings and lack of coordination between intelligence and military operations (Onuoha, 2021). Adopting best practices like closer intelligence-military integration and prioritizing pre-emptive action could enhance Nigeria's counterterrorism efforts.

#### Legal and Ethical Frameworks

Global best practices emphasize operating within a clear legal and ethical framework. The U.S., UK, and Israel have established legal frameworks regulating intelligence operations, protecting civil liberties, and ensuring accountability (Lowenthal, 2022; Johnson, 2020).

Nigeria faces challenges in establishing a robust legal framework for intelligence. While laws exist, enforcement is inconsistent, and oversight of intelligence agencies is limited, leading to concerns about human rights abuses (Amnesty International, 2021). Strengthening legal oversight and ensuring agencies operate within the law are essential for building public trust.

#### **METHODOLOGY**

This study will employ a mixed-methods approach, integrating quantitative data derived from a questionnaire with qualitative insights gleaned from an empirical literature review, to investigate the multifaceted role of intelligence in safeguarding Nigeria's national security. This

methodological triangulation aims to provide a comprehensive and nuanced understanding of the research questions and hypotheses, drawing upon both empirical evidence and theoretical frameworks.

#### 3.1 Research Design

An explanatory sequential mixed-methods design will be implemented. This design entails the initial collection and analysis of quantitative data, followed by the collection and analysis of qualitative data to elucidate and contextualize the quantitative findings. The quantitative phase will offer a broad overview of the current state of intelligence practices in Nigeria, while the subsequent qualitative phase will delve deeper into the underlying factors, processes, and complexities.

#### 3.2 Data Collection

**Questionnaire:** A structured questionnaire will be meticulously developed to elicit data from a diverse range of stakeholders engaged in national security in Nigeria, including security experts, intelligence officials, policymakers, and academics. The questionnaire will incorporate both closed-ended questions (e.g., Likert scale items) and open-ended questions to capture a spectrum of perspectives and experiences. To ensure a representative sample, the questionnaire will be administered both online and in-person.

**Empirical Literature Review:** A systematic review of pertinent literature will be conducted to identify and critically analyze existing research on intelligence gathering, national security, and counterterrorism in Nigeria, with a specific focus on studies published between 2020 and 2024. The review will encompass peer-reviewed journal articles, books, government reports, and policy documents.

#### 3.3. Data Analysis

Quantitative Data Analysis: Descriptive and inferential statistics will be employed to analyze the questionnaire data. Descriptive statistics will be utilized to summarize the data, while inferential statistics will be leveraged to test the hypotheses and identify statistically significant relationships between variables.

#### Integration of Findings

The findings emanating from the quantitative and qualitative data analysis will be meticulously integrated to provide a holistic and insightful understanding of the research questions. The qualitative data will serve to explicate and contextualize the quantitative findings, thereby yielding a richer and more nuanced interpretation.

#### 3.4. Ethical Considerations

Ethical considerations will be accorded paramount importance throughout the research process. Informed consent will be obtained from all participants, and their anonymity and confidentiality will be stringently safeguarded. The research will adhere scrupulously to all relevant ethical guidelines and regulations.

#### 3.5. Limitations

The study may encounter certain limitations, such

as potential biases inherent in questionnaire responses and the restricted availability of recent and directly relevant literature on intelligence practices in Nigeria. However, the utilization of a mixed-methods approach and a rigorous research design will serve to mitigate these limitations and enhance the overall validity and reliability of the findings.

### RESULTS

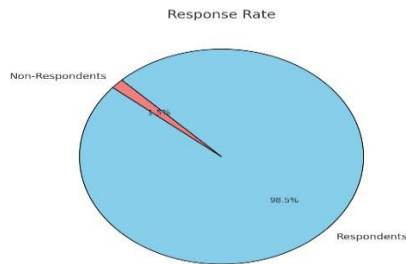
#### 4.1 SURVEY RESPONSE RATE

The questionnaire was the primary instrument used for data collection in this study. An approved questionnaire was shared with four hundred (400) participants and distributed, but only three hundred and ninety-eight (398) were partially completed and returned. However, three hundred and ninety-four (394) were fully completed, making an impressive ninety-six per cent (96%) return, indicating a prominent level of participant engagement, forming the basis for our data analysis. The response rate in this study exceeded the threshold, strengthening the validity of the findings made from the data. The figure as shown visually represents the response rate for this survey.

**Table 4.1. Survey Response Rate**

CHARACTERISTICS	RESPONSES	PERCENTAGE
Respondents	394	98.5%
Non-Respondents	6	1.5%
<b>TOTAL</b>	<b>400</b>	<b>100%</b>

Source: Field data 2024



**Fig. 4.1 Response rate of survey**

**4.2 RESPONDENTS' DEMOGRAPHICS**

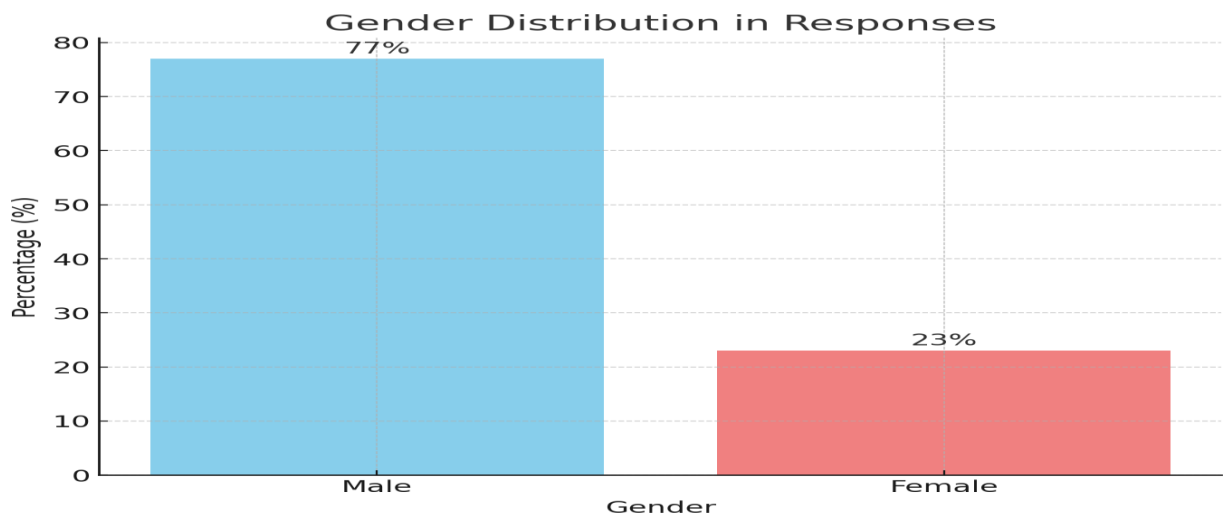
The participants' demographics comprised gender, current or past affiliation with a security agency,

years of experience in the security sector, highest level of education, and primary role in the security sector.

**Table 4.1.2 Respondents gender**

DEMOGRAPHICS	CHARACTERISTICS	RESPONSES	PERCENTAGE
GENDER	Male	304	77%
	Female	90	23%
TOTAL		394	100%

Source: Field data, 2024



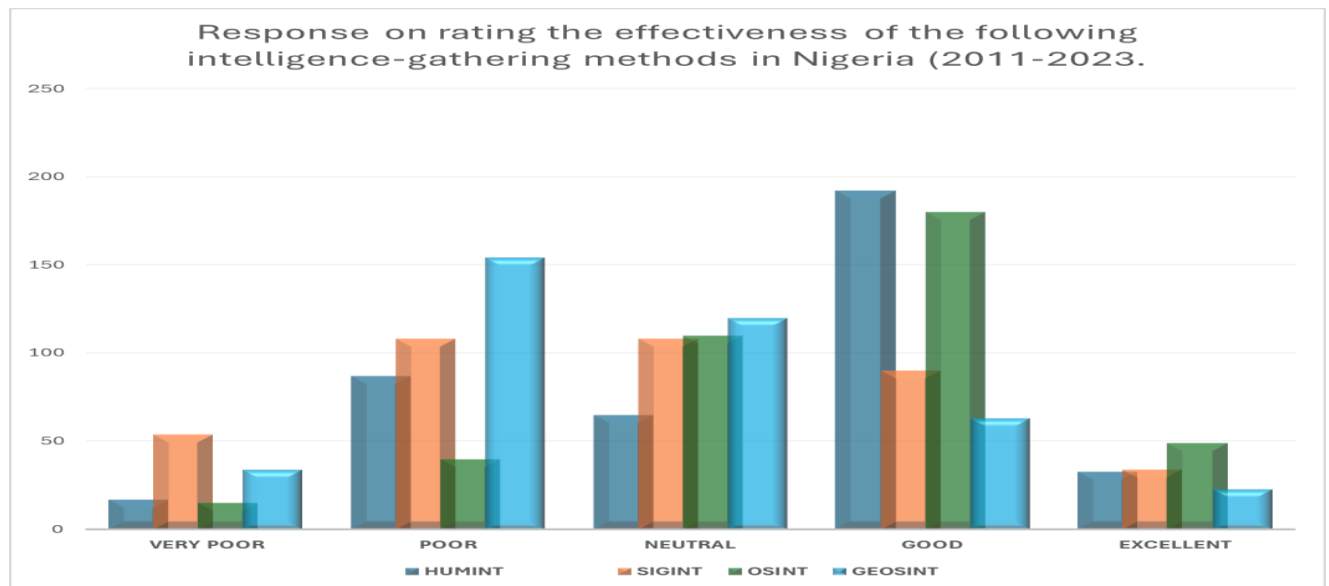
**Fig. 4.2 Response rate of survey**

4.3 Research Questions I How effectively have intelligence agencies gathered and utilized intelligence in Nigeria

**4.3 Table: Rating the effectiveness of the following intelligence-gathering methods in Nigeria**

CHARACTERISTICS	VERY POOR	POOR	NEUTRAL	GOOD	EXCELLENT	TOTAL
HUMINT	17	87	65	192	33	394
SIGINT	54	108	108	90	34	394
OSINT	15	40	110	180	49	394
GEOSINT	34	154	120	63	23	394

Source: Field data, 2024.



**Fig. 4.3 Rating the effectiveness of the following intelligence-gathering methods in Nigeria (2011- 2023).**

Figure 4.3 reveals a heavy reliance on HUMINT and GEOINT and neglecting MASINT. This reliance on HUMINT and OSINT in Nigeria, while underutilizing GEOINT and neglecting MASINT. This reliance on HUMINT and OSINT reflects their value in understanding complex socio-political dynamics

and leveraging the digital landscape, respectively. However, it also exposes vulnerabilities to biases, misinformation, and resource-intensive collection efforts. The underutilization of GEOINT and the absence of MASINT

represent missed opportunities for enhancing situational awareness, strategic planning, and threat detection. To optimize intelligence

operations, Nigeria needs to diversify its intelligence-

gathering methods, invest in advanced technologies, and improve inter-agency coordination.

4.4. Research Question 2: How do Nigeria's intelligence agencies interface and collaborate with other national and international security organizations to combat security threats?

**4.4 Table How would you rate trust and cooperation between your agency/department and other security agencies?**

CHARACTERISTICS	RESPONSE	PERCENTAGE
Very Low	15	4%
Low	145	37%
Neutral	130	33%
High	84	21%
Very High	20	5%
Total	100	100%

Source: Field data 2024.



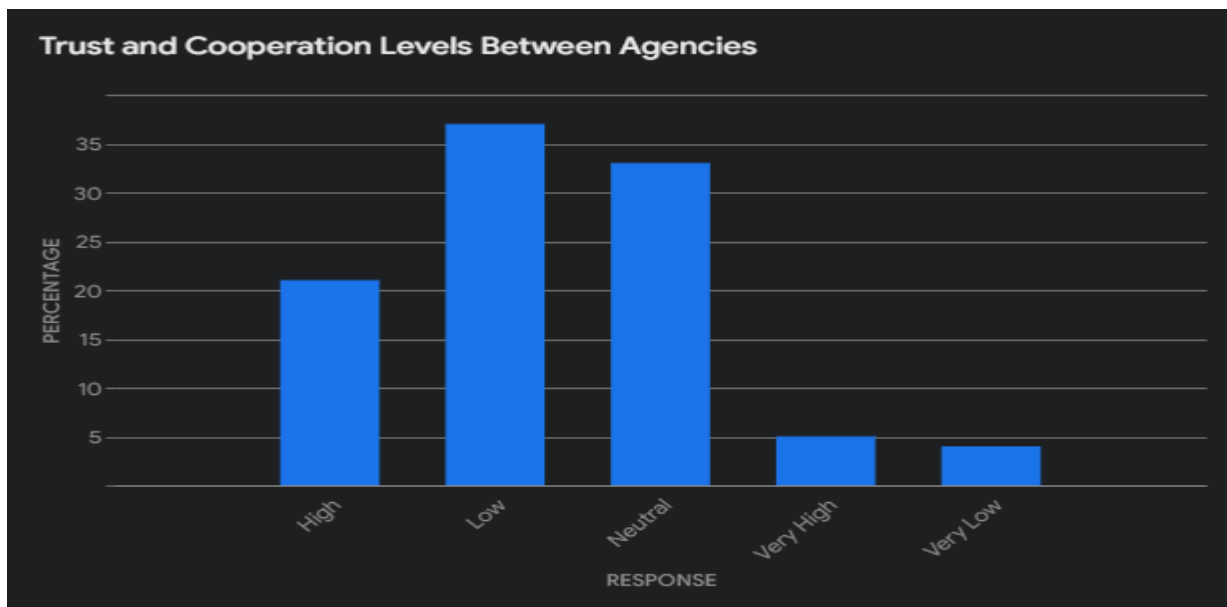


Fig. 4.4

The data displayed in Table 4.4, on the perceived degree of trust and collaboration between Nigerian intelligence services and other security groups, portrays a worrisome scenario. A substantial proportion of participants (37%) assess this level of trust and collaboration as "Low," whilst a mere 26% regard it as "High" or "Very High." These findings indicate that although there is a certain degree of cooperation, there is still significant potential for enhancing the development of a genuinely unified and efficient intelligence community.

The suboptimal degree of trust and collaboration may be attributed to several things. As previously mentioned, the presence of inter-agency competition, divergent organizational cultures, and uncertainties in jurisdiction might hinder successful collaboration. Moreover, the presence of long-standing distrust and a perceived absence

of openness could add complexity to the endeavors of strengthening collaborative partnerships among agencies.

These discoveries have substantial ramifications. Insufficient trust and collaboration can result in deficiencies in intelligence, delays in the exchange of information, and overlooked chances to adequately tackle security risks. Within a nation grappling with intricate and ever-changing security issues such as Nigeria, it is of utmost importance to establish smooth cooperation between intelligence agencies and other security groups.

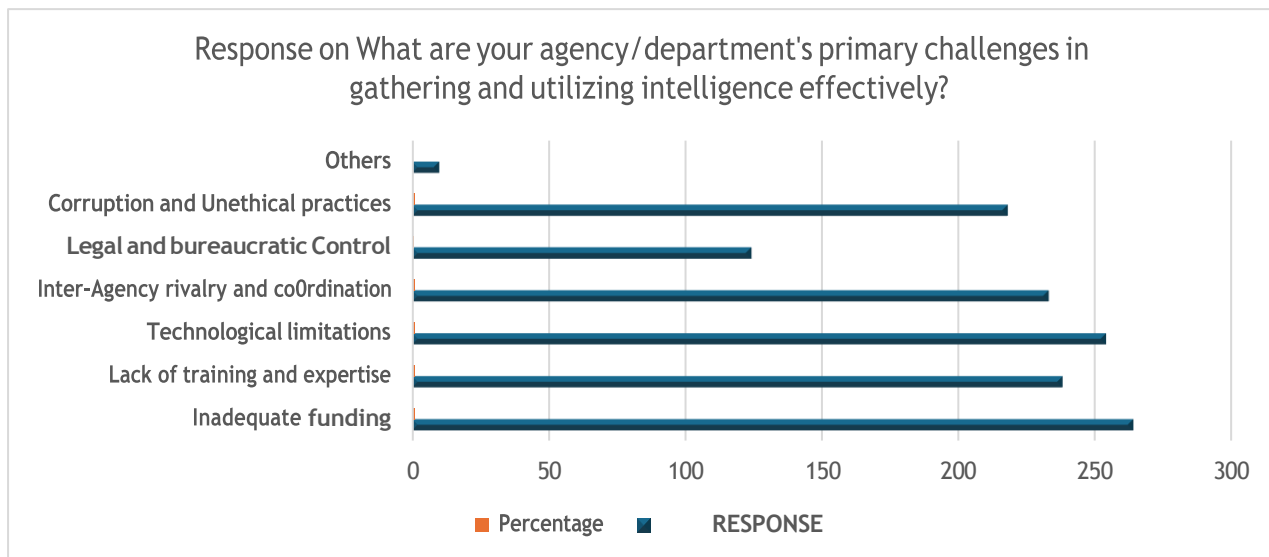
**Research Question 3: What main challenges do intelligence agencies in Nigeria face?**

4.5. What are your agency/department's primary challenges in gathering and utilizing intelligence effectively?

**4.5 Table What are your agency/department's primary challenges in gathering and utilizing intelligence effectively?**

CHARACTERISTICS	RESPONSE	PERCENTAGE
Inadequate funding	264	67.1%
Lack of training and expertise	238	60.5%
Technological limitations	254	64.5%
Inter-Agency rivalry and coordination	233	59.2%
Legal and bureaucratic Control	124	31.6%
Corruption and Unethical practices	218	55.3%
Others	10	2.6%

Source: Field data 2024.



**Fig. 4.5 Agency/department's primary challenges in gathering and utilizing intelligence effectively.**

An analysis of empirical data in Fig. 4.3 above shows an intricate interaction of obstacles that impede the efficiency of Nigerian intelligence

agencies. Insufficient financial resources (67.1%) greatly limit their capability to get sophisticated technology, invest in human resources, and carry

out efficient operations, therefore hindering their ability to compete with changing threats. Moreover, a deficiency in sufficient training and skill (60.5%) impedes their capacity to tackle the ever-changing security environment, marked by cyber threats, advanced terrorist strategies, and international illicit activities. Moreover, technological constraints (64.5%) present a substantial barrier, as agencies face difficulties in obtaining and sustaining the essential tools and infrastructure for surveillance, data analysis, and cyber operations in a time of sophisticated technology. Moreover, the prevalence of inter-agency rivalry and coordination issues (59.2%) leads to inefficiencies and missed opportunities because of inadequate collaboration and

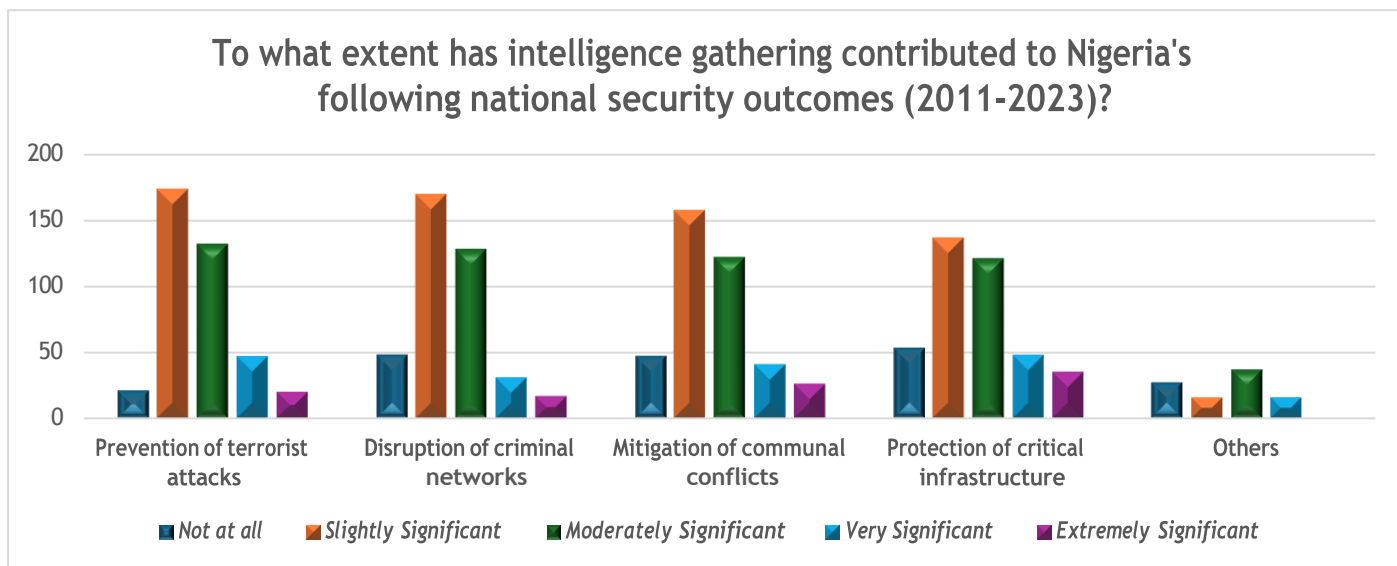
information exchange between security and intelligence services. Although less often mentioned, legal and bureaucratic limitations (31.6%) and corruption and unethical behaviours (55.3%) also present substantial barriers, impeding agility, responsiveness, and public confidence. The complex nature of these issues highlights the immediate requirement for a thorough and careful strategy to bolster intelligence capabilities and improve national security in Nigeria.

4.6 Research Questions 4: What impact have intelligence operations had on national security outcomes?

**4.6 Table: To what extent has intelligence gathering contributed to Nigeria's following national security outcomes (2011-2023)? (Scale of 1 - Not at all to 5 - Very significant)**

CHARACTERISTICS	Not at all	Slightly Significant	Moderately Significant	Very Significant	Extremely Significant	TOTAL
Prevention of terrorist attacks	21	174	132	47	20	394
Disruption of criminal networks	48	170	128	31	17	394
Mitigation of communal conflicts	47	158	122	41	26	394
Protection of critical infrastructure	53	137	121	48	35	394
Others	27	16	37	16	-	

Source: Field data 2024.



**Fig. 4.6 The extent to which intelligence gathering contributed to Nigeria's following national security outcomes**

The data in Figure 4.4.1 reveals a nuanced impact of intelligence activities on Nigeria's national security. While intelligence is perceived as highly effective in safeguarding critical infrastructure, its influence on preventing terrorist attacks, disrupting criminal networks, and mitigating community conflicts is viewed as moderate. This suggests that while intelligence plays a supportive role, its impact is contingent upon factors like timely analysis, inter-agency collaboration, and addressing root causes of conflicts. The underutilization of GEOINT and MASINT further highlights areas for improvement. Overall, the findings emphasize the need for a multifaceted approach to intelligence gathering and analysis, encompassing technological advancements, improved coordination, and a focus on addressing the diverse challenges facing Nigeria's national security.

**DISCUSSION**

The study's findings provide a comprehensive

view of the intricacies and challenges that exist within Nigeria's intelligence ecosystem. The survey results, combined with findings from the literature analysis, reveal both the strengths and flaws of the nation's intelligence infrastructure, as well as their impact on national security.

The analysis demonstrates a strong dependence on Human Intelligence (HUMINT) and Open- Source Intelligence (OSINT), highlighting their ongoing importance in navigating Nigeria's complicated security environment. HUMINT's strength is its capacity to provide nuanced insights into motivations and intentions, especially in the context of insurgency and terrorism (Egbue & Okoye, 2022). The rise of OSINT underscores the increased relevance of utilizing the digital ecosystem for intelligence purposes. However, both HUMINT and OSINT face problems, such as

potential biases, resource requirements, and the need for specialized analytical skills and

technology tools to manage the enormous and frequently unreliable information landscape (Onuoha, 2021; Olaniyan & Yahaya, 2022).

The underutilization of Geospatial Intelligence (GEOINT) and the virtual lack of Measurement and Signature Intelligence (MASINT) represent lost possibilities to improve situational awareness, strategic planning, and threat identification. The inadequate use of GEOINT, which gives critical insights into topography, infrastructure, and activity patterns, impedes successful security operations and catastrophe management (Ezirim & Urdi, 2023). The lack of MASINT, which is critical for detecting and identifying threats related to weapons of mass destruction and new technologies, highlights the need for capacity building in Nigeria's intelligence apparatus (United Nations Office on Drugs and Crime, 2021).

The survey results also reveal substantial hurdles in inter-agency trust and cooperation. The prevalence of "Low" and "Neutral" ratings for trust and collaboration across agencies indicates a fragmented intelligence landscape that impedes effective information sharing and coordinated responses to security threats (International Crisis Group, 2023). This fragmentation can result in inefficiencies, missed opportunities, and an inefficient use of intelligence resources.

Furthermore, the report notes several obstacles confronting intelligence organizations, such as insufficient money, a lack of training and competence, technology restrictions, inter-agency rivalry, legal and bureaucratic constraints, and corruption. These constraints hamper intelligence services' ability to properly obtain, analyze, and apply intelligence to handle Nigeria's varied security concerns.

The perceived influence of intelligence on national security outcomes is uneven. While intelligence is regarded as extremely effective in defending

essential infrastructure, its impact on averting terrorist attacks, disrupting criminal networks, and resolving communal conflicts is viewed as moderate. This implies that, while intelligence is important, its success is dependent on elements such as timely analysis, inter-agency coordination, and addressing the underlying causes of conflict.

The outcomes of this study highlight the intricacies and challenges inherent in Nigeria's intelligence landscape. While there have been major gains, notably in counterterrorism efforts, there is still significant opportunity for improvement. Nigeria can enhance its intelligence capabilities and strengthen its national security by adopting global best practices and adapting them to the Nigerian context.

## **CONCLUSION**

In Nigeria's national security landscape, intelligence gathering plays a multifaceted function, as the study has comprehensively examined. The results highlight the essential role of intelligence in addressing a variety of security challenges, such as terrorism, insurgency, organized crime, kidnapping, and cybercrime. The analysis has also underscored the difficulties encountered by Nigerian intelligence agencies, including insufficient funding, technological constraints, inter-agency competition, and the necessity for improved training and expertise. The integration of both quantitative and qualitative data has yielded a detailed comprehension of the intricacies and dynamics surrounding intelligence operations in Nigeria. The findings of the study hold considerable importance for those in positions of authority, security professionals, and scholars,

providing an essential understanding of the strengths and weaknesses within Nigeria's intelligence framework and proposing possible

paths for enhancement and reform. This analysis enhances the current understanding by offering a thorough and contemporary evaluation of intelligence gathering in Nigeria, especially regarding the changing security environment. It underscores the essential requirement for enhanced funding in technology, the development of human resources, and cooperation among various agencies. The analysis highlights the significance of tackling legal and ethical issues, building public confidence, and drawing insights from international best practices to improve the efficacy of intelligence operations in Nigeria. This study addresses a significant gap in the existing literature by offering empirical evidence regarding the perceived effectiveness of various intelligence-gathering methods, the challenges encountered by intelligence agencies, and the influence of intelligence on national security results. The results of the study can influence policy choices and direct the creation of approaches to bolster Nigeria's intelligence abilities and improve its national security stance.

### **Recommendation**

The results of this study highlight the essential requirement for a comprehensive and strategic method to improve intelligence collection and application in Nigeria. The subsequent recommendations are put forth, based on the insights obtained from the analysis:

**Enhancing Inter-Agency Coordination and Collaboration:** The widespread challenge of inter-agency rivalry and coordination difficulties calls for the development of a strong framework for collaboration. This may entail establishing a centralized entity for intelligence coordination, like the U.S. ODNI or the UK's JIC, to enhance the efficiency of information sharing, analysis, and decision-making processes. The implementation of uniform operating procedures and data-sharing

protocols can significantly improve interoperability and promote smooth collaboration among agencies.

**Improving Technological Capabilities:** The findings emphasize the essential requirement for investment in advanced technologies to close the current technological gap. This involves obtaining and upholding advanced surveillance technology, analytical tools for data, and secure communication systems. The establishment of strong cyber intelligence capabilities is crucial in response to the changing landscape of cyber threats.

**Investing in Human Capital Development:** The absence of sufficient training and expertise highlights the necessity for significant investment in the development of human capabilities. This involves delivering thorough training initiatives, creating avenues for career advancement, and drawing in and keeping exceptional talent with attractive compensation packages and a nurturing workplace atmosphere.

**Enhancing Legal and Ethical Structures:** The existence of legal and bureaucratic limitations, along with issues related to corruption and unethical behaviour, underscores the need for a strong legal and ethical structure for intelligence operations. This encompasses well-defined laws regulating intelligence operations, strong oversight frameworks, and fostering an environment of responsibility and openness within intelligence organizations.

**Enhancing Community Engagement and Trust:** The study's results underscore the significance of establishing trust and cultivating collaboration with local communities. Community policing initiatives can facilitate this, by engaging traditional leaders and local informants in intelligence-gathering efforts, while also addressing concerns related to human rights

abuses.

**Embracing a Diverse Intelligence Strategy:** The excessive dependence on HUMINT and OSINT, along with the insufficient use of GEOINT and MASINT, highlights the necessity for a more varied and well-rounded intelligence strategy. This involves dedicating resources to the advancement of skills in GEOINT and MASINT, utilizing their potential to improve situational awareness, strategic planning, and threat identification.

**Examining Global Best Practices:** The comparative analysis with international standards uncovers important insights for Nigeria. Implementing effective strategies and approaches used by nations such as the U.S., UK, and Israel, and tailoring them to fit the Nigerian context, can greatly improve the efficiency of the country's intelligence operations.

By adopting these suggestions, Nigeria can enhance its intelligence capabilities, cultivate a more unified and efficient intelligence community, and reinforce its national security against emerging threats.

## REFERENCES

1. Adetula, V. A. (2020). Cybersecurity and National Security in Nigeria: Challenges and the Way Forward. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, 10(3), 1-17.
2. Adetula, V. A. (2020). Intelligence and National Security Management in Nigeria. *African Security Review*, 29(2), 142-162.
3. Agbiboa, D. E. (2021). Peace at any price? The contradictions of amnesty and the challenge of Boko Haram. *African Affairs*, 119(475), 239-260.
4. Akinola, A. A., & Adebani, W. (2022). Banditry and the crisis of governance in Nigeria. *African Affairs*, 121(484), 417-434.
5. Akinyemi, B. (2022). Kidnap for Ransom in Nigeria: The Need for Intelligence-Led Policing.
6. *International Journal of Intelligence and Counterintelligence*, 35(2), 311-330.
7. Albert, I. O. (2021). Ethno-religious conflicts and national security in Nigeria: Implications for sustainable development. *International Journal of Sustainable Development*, 14(3), 235-252
8. Alli, W. (2022). International Cooperation and Counterterrorism in West Africa: The Case of Boko Haram. *African Journal of International Affairs*, 26(3), 67-89.
9. Amnesty International. (2021). Nigeria: Authorities Must Urgently Rescue Schoolboys Abducted in Katsina. Retrieved from <https://www.amnesty.org>
10. Apuke, O. D., & Tunca, E. (2023). Social media intelligence (SOCMINT) and social media analytics (SMA) for combating insecurity in Nigeria. *African Journal of Science, Technology, Innovation and Development*, 15(3), 381-391.
11. Balogun, A. (2023). Intelligence Gathering and the Fight against Terrorism in Nigeria. *Journal of Intelligence Studies in Business*, 13(1), 42-52.
12. Bar-Joseph, U., & McDermott, R. (2021). Intelligence Success and Failure in Israel: The Case of the Yom Kippur War. *Intelligence and National Security*, 36(3), 331-351.
13. Bergen, P. (2021). *The Rise and Fall of Osama bin Laden*. Simon & Schuster.
14. Betts, R. K. (2020). *Enemies of Intelligence: Knowledge and Power in American National Security*. Columbia University Press.
15. Bhuiyan, F. (2021). Artificial Intelligence for National Security: The Case of India. *Journal of Defence Studies*, 15(4), 449-470.

16. Brennan, M., et al. (2020). Misinformation, disinformation, and violent extremism. *Peace Review: A Journal of Social Justice*, 32(3), 320-330.
17. Brown, D. (2020). *Electronic Intelligence: A Primer*. *Journal of Intelligence Studies*, 25(2), 123- 135.
18. Buchanan, L., & Kehoe, L. (2021). *Intelligence Sharing and Counterterrorism Cooperation*. *Journal of Strategic Studies*, 44(5), 678–696.
19. Buzan, B., Waever, O., & de Wilde, J. (1998). *Security: A New Framework for Analysis*. Lynne Rienner Publishers.
20. Chatfield, A. T., & Reddick, C. G. (2020). Leveraging geospatial artificial intelligence (geoAI) in law enforcement agencies. *Government Information Quarterly*, 37(3), 101499.
21. Chatfield, A. T., Reddick, C. G., & Brajawidagda, U. (2019). How are police using social media in the United States? A mixed-method review. *Government Information Quarterly*, 36(4), 101383.
22. Clarke, R. V., & Newman, G. R. (2020). *Outsmarting the Terrorists*. Praeger Security International. Clarke, R. V., & Newman, G. R. (2023). *Cybersecurity and Counterterrorism: Strategies for a More Secure World*. Routledge.
23. Collins, A. (2016). *Contemporary Security Studies*. Oxford University Press.
24. Egbue, O., & Okoye, C. (2021). Boko Haram insurgency in Nigeria: The role of intelligence gathering and synergy in the counter-insurgency operations. *International Journal of African Renaissance Studies - Multi-, Inter-, and Trans disciplinary*, 16(1), 68-88
25. Egbue, O., & Okoye, C. (2022). Human Intelligence (HUMINT) and Counter-Insurgency Operations in Nigeria. *African Security Review*, 31(2), 151–168.
26. Enders, W., & Sandler, T. (2020). *The Political Economy of Terrorism*. Cambridge University Press.
27. Ewi, E., & Salifu, M. (2017). *Assessing Police Integrity in Nigeria*. Africa Security Brief No. 33. Africa Center for Strategic Studies.
28. Ezirim, G. E., & Urdi, A. (2023). Geospatial Intelligence and National Security in Nigeria: Challenges and Prospects. *Journal of Intelligence Studies in Africa*, 5(2), 45–62.
29. Falola, T. (2021). *A history of Nigeria*. Cambridge University Press.
30. Felbab-Brown, V. (2021). *Narco Noir: Mexico's Cartels, Cops, and Corruption*. Brookings Institution Press.
31. Fingar, T. (2021). *Reducing Uncertainty: Intelligence Analysis and National Security*. Stanford University Press.
32. Frenkel, S. (2022, February 17). The Israeli Military Unit That is at the Forefront of Cyberwarfare. *The New York Times*. <https://www.nytimes.com/2022/02/17/world/middleeast/israel-military-unit-8200.html>
33. Gill, P. S., & Mathur, S. (2023). The role of cyber intelligence in national security: A case study of India. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, 13(1), 1-19.
34. Heuer, R. J. (2020). *The Psychology of Intelligence Analysis*. Pherson Associates.
35. Holt, T. J., Smirnova, O., Chua, Y. T., & Copes, H. (2021). Examining the Structure, Organization, and Processes of the International Market for Stolen Data. *British Journal of Criminology*, 61(2), 398–417.



36. Houghton, D. P. (2020). Political uses of intelligence. Brookings Institution Press.
37. Ibrahim, B.A. (2023) Intelligence Gathering and National Security: Exploring the Nexus in Nigeria. Sage Open, 13(2), 1-12.
38. International Crisis Group. (2023). Ending Nigeria's kidnapping crisis.
39. International Crisis Group. (2023). Still No End in Sight: The Boko Haram Insurgency 12 Years On. Retrieved from [invalid URL removed]
40. Johnson, L. (2021). Resource Allocation in Intelligence Agencies: A Rational Choice Perspective.
41. Intelligence and National Security, 36(1), 55-72.
42. Johnson, L. K. (2020). The Oxford Handbook of National Security Intelligence. Oxford University Press.
43. Johnson, R. (2018). The Role of Signals Intelligence in Modern Warfare. Military Review, 98(4), 56-67.
44. Johnson, R. (2019). The Art and Science of Human Intelligence Collection. Oxford University Press.
45. Kumar, S. (2023). The Future of Electronic Intelligence: Trends and Challenges. Defense Intelligence Journal, 32(1), 45-58.
46. Lazaridou-Chatzigoga, A., & Kerasiotis, F. (2021). Open-Source Intelligence (OSINT) in the Fight Against Crime and Terrorism. International Journal of Law, Crime and Justice, 65, 100454.
47. Lowenthal, M. M. (2016). Intelligence: From Secrets to Policy. CQ Press. Lowenthal, M. M. (2022). Intelligence: From Secrets to Policy (7th ed.). CQ Press.
48. Marrin, S. (2022). Improving intelligence analysis. Center for Strategic and International Studies.
49. Miller, S. (2024). Critical Infrastructure Protection in the Age of Cyber Threats: The Role of Intelligence. Journal of Infrastructure Security, 6(2), 120-138.
50. Obasi, N. (2022). Intelligence Sharing in Nigeria: Enhancing Coordination for National Security.
51. African Journal of Security, 18(3), 101-118.
52. Obi, C. (2022). National security and sustainable development in Nigeria: Challenges and prospects. Palgrave Macmillan.
53. Olaniyan, A. (2021). The role of geospatial intelligence in combating kidnapping and banditry in Nigeria. GeoJournal, 86, 3423-3438.
54. Olaniyan, A., & Yahaya, M. (2022). Intelligence Gathering and National Security in Nigeria: Challenges and Prospects. International Journal of Research and Innovation in Social Science (IJRISS), VI(VII), 339-346.
55. Olumide, O. (2022). Cybersecurity in Nigeria: Challenges and Opportunities. Nigerian Journal of Cybersecurity Studies, 7(1), 12-29.
56. Omand, D. (2022). How spies think: Ten lessons in intelligence. Penguin Books.
57. Omenka, J. I., Dickson, E., Ali, B. F., Agishi, T. V., & Coker, M. A. (2017). The dynamics of human and national security in Nigeria: lessons from the Boko haram insurgency. International Journal of Asian Social Science, 7(6), 505-520.
58. <https://doi.org/10.18488/journal.1.2017.76.505.520>
59. Omoniyi, T., & Adewumi, F. (2022). Utilization of Social Media Intelligence (SOCMINT) in

- mitigating insecurity in Nigeria. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, 12(1), 1-18.
60. Onapajo, H., & Uzodike, U. (2022). Countering Terrorism in Nigeria: The Role of Human Intelligence. *Journal of Terrorism Research*, 13(2), 55-72.
61. Onuoha, F. (2019). National Security and Intelligence Management in Nigeria. *Journal of Security and Crisis Management*, 3(1), 12-25.
62. Onuoha, F. (2021). Boko Haram's Resilience and the Failure of Counterterrorism in Nigeria. *Journal of Terrorism Research*, 12(1), 17-35.
64. Opuala-Charles, S. and Oshilike, I. (2022). National security, FDI and economic development in Nigeria. *International Journal of Development and Economic Sustainability*, 10(4), 15-25. <https://doi.org/10.37745/ijdes.13/vol10n41525>
65. Osisanwo, F. Y., Adekoya, A. F., & Iyiola, O. O. (2021). Open-Source Intelligence (OSINT) in the fight against insurgency in Nigeria. *Heliyon*, 7(3), e06432.
66. Perl, R. F. (2020). *Intelligence and U.S. Foreign Policy: The Role of the Intelligence Community in the Formulation and Implementation of U.S. Foreign Policy*. Congressional Research Service.
67. Petherick, A. (2023) The Weaponisation of Open-Source Intelligence. *Survival*, 65(2), 7-24.
68. Pillar, P. R. (2020). *Intelligence and U.S. foreign policy: Iraq, 9/11, and misguided reform*. Columbia University Press.
69. PwC Nigeria. (2021). *The State of Cybersecurity in Nigeria: Insights and Trends*.
70. PricewaterhouseCoopers. Retrieved from <https://www.pwc.com/ng/cybersecurity>.
71. Racz, A. (2022). *Open-Source Intelligence in Countering Terrorism and Violent Extremism*.
72. *Perspectives on Terrorism*, 16(4), 70-83.
73. Ratcliffe, J. (2020). *Intelligence matters*. New York, NY: HarperCollins.
74. Ratcliffe, J. (2021). Intelligence-led policing in an age of terrorism. *Policing and Society*, 31(10), 1151-1166.
75. Saani, A. (2021). *Countering violent extremism in the Sahel: The role of open-source intelligence*.
76. *Journal of Terrorism Research*, 12(3), 32-48.
77. Smith, J., et al. (2021). *The Evolution of Electronic Intelligence: From the Cold War to the Present*.
78. *Intelligence and National Security*, 36(4), 512-531.
79. Uzochukwu, B. (2021). *The military and security in Nigeria: A study of the Joint Task Force*.
80. Ibadan, Nigeria: University Press PLC.
81. Vale, P. (2021). *Security and Politics in South Africa: The Regional Dimension*. Routledge.
82. Watts, M. (2020). *A history of the Niger Delta: Oil and insurgency in Nigeria*. London, UK: Zed Books.
83. Wilson, D. (2022). Understanding national security in the modern era. *Journal of Global Affairs*, 22(2), 89-106. <https://doi.org/10.1080/19331681.2022.1762534>
84. Xin, H. (2020). The Evolution of China's Signals Intelligence Capabilities and Its Impact on Regional Security. *The China Quarterly*, 243,

737-760.

- 85.** Youssef, N. (2020). Intelligence Reforms in Morocco: Challenges and Prospects. *Journal of Intelligence and National Security*, 35(1), 100-115.
- 86.** Youssef, N. (2021). Border Security and Intelligence Gathering in Morocco: A Case Study of the Western Sahara. *Journal of Borderlands Studies*, 36(2), 280-298.
- 87.** Youssef, N. (2022). Intelligence and Counterterrorism in Morocco: Strategies and Challenges. *Studies in Conflict & Terrorism*, 45(3), 210-228.
- 88.** Zenn, J. (2020). *Boko Haram: Islamic State's West African Province*. Bloomsbury Publishing.
- 89.** Zenn, J. (2021). Boko Haram's resilience and the fragmentation of jihadist movements in Nigeria.