GRADIVA

Volume 65 | Issue 03 | March 2026
DOI: 10.5281/zenodo.19509887

Addressing Intelligence Deficiencies in Safeguarding Nigeria's Critical Infrastructure and Strategic National Assets for Improved National Security

Sylvester Osugba[1]* & Monday Agbeyi[2]

1,2.Faculty of Social Sciences, Department of Sociology, Delta State University Abraka,
Local Government Service Commission Asaba.
*Corresponding Author Email: sylvesterosugba@delsu.edu.ng

Abstract

The protection of critical national assets and infrastructure remains a central component of Nigeria's national security and socio-economic stability. Despite the existence of multiple intelligence and security agencies, Nigeria continues to experience persistent threats to its strategic assets, including oil and gas installations, power networks, transportation systems, and communication infrastructure. These threats, manifested through vandalism, oil theft, cyberattacks, and insurgent sabotage, point to deep-seated deficiencies within the country's intelligence architecture. This study examines intelligence-gathering mechanisms and the core intelligence deficiencies hindering the effective protection of critical national assets and infrastructure by the Nigeria Security and Civil Defence Corps (NSCDC) in Delta State. Anchored on the Intelligence Cycle Theory and Systems Theory, the study adopted a descriptive survey research design. Data were collected using structured questionnaires administered to 114 purposively selected NSCDC officers across divisional offices, area commands, and the state headquarters in Delta State. Descriptive statistical tools, 7 including frequency distributions, percentages, and mean ratings, were employed for data analysis. Findings reveal that intelligence gathering for infrastructure protection relies largely on human intelligence, community informants, private security agencies, patrol networks, and limited technological tools. However, major challenges undermine effectiveness, including poor inter-agency collaboration, rivalry among security agencies, inadequate training, insufficient technological capacity, weak community engagement, and lack 14 of political and institutional support. The results further indicate that intelligence functions are unevenly integrated across ranks, and modern intelligence tools such as UAVs and advanced surveillance technologies remain underutilized. The study concludes that intelligence deficiencies significantly weaken Nigeria's capacity to safeguard critical national assets, resulting in economic losses, security vulnerabilities, and declining public trust. It recommends clearer policy frameworks.

Keywords: *National Security, Intelligence Reform, Security Architecture, National Security, Intelligence Deficiencies, Critical Infrastructure Protection.*

INTRODUCTION

Nigeria's national security hinges critically on the integrity and protection of its infrastructure and strategic assets, such as power networks, oil and gas installations, transportation systems, and communication frameworks. In recent years, the country has confronted recurrent threats to these assets manifesting through vandalism, cyber-attacks, oil theft, and insurgent sabotage. These vulnerabilities not only erode public confidence but also undermine economic growth and state legitimacy. (Ibanga, Fwah, and Idowu,2022). Effective intelligence gathering and deployment are central to countering these threats; yet, significant intelligence deficiencies persist, impairing the state's ability to anticipate, prevent, and respond

Volume 65 | Issue 03 | March 2026
DOI: 10.5281/zenodo.19509887

to evolving risks. One dimension of the problem is structural: intelligence agencies in Nigeria face weak inter-agency coordination, overlapping mandates, and inadequate legal and institutional frameworks. Research has shown that despite sizeable investment in agencies like the DSS, NIA, and NSCDC, the lack of unified protocols and cohesive strategy leads to delayed responses or blind spots among agencies. Similarly, many intelligence functions rely heavily on human and open-source intelligence (HUMINT, OSINT), while more specialized technical or geospatial intelligence tools (GEOINT, MASINT) remain under-utilized. (Afolabi et al 2024).

Another critical deficiency lies in the provision and integration of technological capabilities. Cybersecurity lapses in power system infrastructure, frequent transmission line vandalism, and pipeline theft all point toward insufficient monitoring, predictive analytic tools, and surveillance. This technological shortfall is compounded by underfunding, weak human capacity development, and shortage of staff trained in modern intelligence practices. (Olowonihi, and Musa,2024).) Community engagement and intelligence sharing are also areas of weakness. Many local communities remain mistrustful or disengaged from formal security structures, and there are inadequate channels for grassroots intelligence contributions. This gap hampers early warning and localized threat identification. Legal ambiguities further complicate matters: outdated statutes, unclear jurisdictional boundaries, and bureaucratic inertia limit intelligence agencies' operational flexibility. (Tunji-Ojo, 2024).), Given the scale and variety of threats, ranging from oil theft in the Niger Delta to vandalism of national grid infrastructure, from banditry to cyber intrusions there is an urgent imperative to reform intelligence capacities. Enhancing national security demands addressing these deficiencies through a multi-pronged strategy: stronger legal frameworks, better inter-agency collaboration, more modern technological capabilities, improved training and human resources, greater community involvement, and adequate funding. Such reforms are essential not only to safeguard strategic assets but also to enable sustainable socio-economic development and restore public trust in security institutions, (Tabiowo,2025). Despite the importance of protecting critical national assets and infrastructure, Nigeria's security agencies, including the Nigeria Security and Civil Defence Corps (NSCDC), face significant challenges in gathering intelligence to effectively carry out their mandate. These challenges include poor collaboration between stakeholders, inter-agency rivalry, political interference, inadequate funding, and insufficient officer training. These challenges have resulted in the inadequate protection of national assets, exacerbating social inequalities and economic losses.

Nigeria, as Africa's most populous nation and one of its largest economies, is increasingly confronted with multifaceted security challenges that threaten its critical infrastructure and strategic national assets. These include power grids, oil and gas installations, transportation networks, telecommunication systems, military facilities, government institutions, and financial centers. These assets are vital for the nation's stability, economic development, and public safety. However, they have become frequent targets of sabotage, terrorism, insurgency, cyberattacks, and vandalism.(Bodunde and Balogun 2018). Despite numerous security frameworks and the presence of intelligence and law enforcement agencies, persistent and growing threats suggest that Nigeria suffers from significant deficiencies in its intelligence architecture. These deficiencies manifest in the form of poor intelligence gathering, inadequate inter-agency collaboration, lack of timely information dissemination, weak technological capabilities, insufficient human capacity, and limited strategic foresight. Consequently, security agencies are often reactive rather than proactive, responding to threats only after significant damage has been done. Moreover, the politicization of intelligence

Volume 65 | Issue 03 | March 2026
DOI: 10.5281/zenodo.19509887

operations, corruption, and bureaucratic red tape further erode the effectiveness of Nigeria's intelligence community. This has led to critical intelligence failures, such as the inability to prevent major attacks on oil pipelines, military installations, prisons, and the high-profile kidnapping of schoolchildren and government officials.

The implications of these intelligence shortcomings are severe: they not only endanger the lives of citizens and the integrity of national infrastructure, but also erode public confidence in government, deter foreign investment, and weaken Nigeria's overall national security posture.In light of these challenges, there is a compelling need to critically examine the existing intelligence framework and identify the root causes of its inefficiencies. Enhancing intelligence capacity, fostering inter-agency coordination, adopting modern surveillance technologies, and institutionalizing reforms are essential to safeguarding Nigeria's critical infrastructure and strategic assets.

This research, therefore, seeks to investigate the core deficiencies in Nigeria's intelligence system, identify the key intelligence deficiencies hindering effective protection of Nigeria's critical infrastructure and strategic national assets, to assess the role of technology and human capacity in enhancing intelligence gathering and threat detection for safeguarding critical infrastructure This study is significant because it highlights the importance of addressing systemic issues within the intelligence-gathering process to protect critical infrastructure effectively and equitably. The findings of this study will contribute to the development of policies and strategies that promote a more robust and inclusive approach to safeguarding national assets.

Conceptualization

Intelligence Deficiencies

Encompass a broad range of shortcomings and gaps within the entire intelligence cycle, including the collection, processing, analysis, dissemination, and practical application of intelligence information. These deficiencies hinder the ability of security agencies to accurately anticipate, detect, and respond to emerging threats in a timely and effective manner. According to Lowenthal (2017), intelligence deficiencies undermine national security efforts by causing delays, inaccuracies, and incomplete understanding of threats, which in turn results in reactive rather than proactive security measures. In the context of Nigeria, intelligence deficiencies are particularly pronounced and multifaceted. One significant issue is the lack of effective communication and coordination among various intelligence and security agencies. The fragmented nature of intelligence operations often leads to critical information being siloed within individual agencies, preventing a unified and comprehensive approach to national security. This poor inter-agency collaboration limits the timely sharing of actionable intelligence and contributes to operational redundancies or oversights.

In addition to technological and coordination challenges, human resource capacity remains a critical weakness. Many agencies face shortages of trained intelligence professionals with the necessary expertise in analysis, counterterrorism, and cyber intelligence. The problem is compounded by inadequate training programs and limited opportunities for professional development. Moreover, intelligence operations in Nigeria are often hindered by systemic issues such as corruption, politicization, and bureaucratic inefficiencies. These factors erode institutional integrity and trust, negatively affecting the quality and reliability of intelligence output.

Volume 65 | Issue 03 | March 2026
DOI: 10.5281/zenodo.19509887

National security

Refers to the comprehensive measures and policies implemented by a state to safeguard its citizens, territory, government institutions, and key national interests from both external and internal threats. These threats can take many forms, including military invasions, terrorism, espionage, cyber-attacks, insurgencies, and organized crime. The overarching goal of national security is to maintain political stability, protect economic development, and ensure the safety and well-being of the population. As Buzan, Waever, and De Wilde (1998) argue, national security goes beyond traditional military concerns to include economic security, environmental security, societal security, and political security. This broader perspective acknowledges that threats to a nation's security can arise from diverse sources and can impact multiple facets of national life. Integral to the concept of national security is the role of intelligence. Intelligence functions as the foundation for informed decision-making by providing policymakers and security agencies with timely, accurate, and relevant information about potential threats. It enables governments to anticipate and prevent attacks before they occur, thus shifting security efforts from reactive to proactive strategies. Effective intelligence helps in identifying vulnerabilities in critical infrastructure, assessing the intentions and capabilities of adversaries, and formulating appropriate responses to emerging risks. Moreover, national security requires a coordinated approach involving various state institutions, including the military, law enforcement, intelligence agencies, and emergency response units. These entities must collaborate to develop comprehensive security frameworks that can respond flexibly to both traditional and non-traditional security challenges. In Nigeria, where threats such as terrorism, insurgency, and cybercrime are prevalent, strengthening intelligence capabilities is essential to protect national assets and promote long-term stability and development.

Relationships Between Concepts

The conceptual framework of this research posits that intelligence deficiencies significantly undermine the ability of security agencies to protect critical infrastructure and strategic national assets effectively. When intelligence systems are weak or fragmented, agencies lack the timely and accurate information necessary to anticipate, detect, and respond to security threats such as sabotage, terrorism, cyberattacks, and other forms of disruption. These intelligence gaps create vulnerabilities that adversaries can exploit, increasing the likelihood of successful attacks on vital sectors including energy, transportation, communications, and government institutions. Such breaches not only cause immediate damage but also have far-reaching consequences on national stability, economic growth, and public confidence. Conversely, the framework argues that enhancing intelligence capabilities is central to strengthening national security. Improvements in intelligence systems involve several key areas. First, fostering effective information sharing among various intelligence and security agencies is crucial. Breaking down silos and encouraging seamless communication ensures that critical data and insights are disseminated quickly and efficiently, enabling a coordinated and unified response to emerging threats. Second, the adoption and integration of modern technologies, such as advanced surveillance tools, cyber intelligence platforms, big data analytics, and secure communication networks, can significantly enhance the capacity for threat detection and situational awareness. These technologies allow agencies to monitor complex and rapidly evolving security landscapes more effectively.

Volume 65 | Issue 03 | March 2026
DOI: 10.5281/zenodo.19509887

THEORETICAL FRAMEWORK

Intelligence Cycle Theory

The conceptual framework for this research is primarily informed by the Intelligence Cycle Theory, which provides a foundational understanding of how intelligence is systematically gathered, processed, analyzed, and disseminated to support decision-making and security operations. According to Hulnick (2006), the intelligence cycle consists of several interrelated stages: collection, processing, analysis, and dissemination. Each stage plays a crucial role in ensuring that intelligence information is accurate, relevant, and timely. The cycle begins with the collection of raw data from various sources, which can include human intelligence, signals intelligence, imagery, open sources, and cyber surveillance. This raw data is then subjected to processing, a stage where it is organized, filtered, and converted into a format suitable for analysis. The analysis phase involves critical evaluation and interpretation of the processed information to generate actionable intelligence, highlighting potential threats, vulnerabilities, and opportunities. Finally, the dissemination stage ensures that the intelligence is effectively communicated to the relevant policymakers, security agencies, and operational units that require it. Breakdowns or inefficiencies at any point in this cycle can severely impair the overall effectiveness of intelligence operations. For example, if the collection is incomplete or biased, the entire intelligence output becomes flawed. Similarly, delays in processing or dissemination can prevent timely responses to emerging threats, leaving critical infrastructure and national assets vulnerable. These deficiencies are particularly pronounced in contexts where coordination between agencies is poor or where technological and human resource capacities are limited.

Systems Theory

In addition to the Intelligence Cycle Theory, the framework draws on Systems Theory, which emphasizes the importance of viewing intelligence operations as part of a larger, interconnected system that must function cohesively to achieve national security goals. Kapucu and Hu (2016) argue that an integrated and coordinated network of intelligence agencies, law enforcement, military units, and other stakeholders is essential for efficient information flow and comprehensive threat assessment. Systems Theory highlights how these components interact dynamically, and how failures in communication, collaboration, or resource sharing can disrupt the entire system. The theory advocates for the development of interoperable platforms, joint operational protocols, and collaborative environments that foster synergy among intelligence entities. Together, these theories underscore the necessity for a holistic approach to intelligence operations, one that ensures all stages of the intelligence cycle are robust and well-supported within a coordinated, system-wide framework. This integrated approach is vital for enhancing the protection of Nigeria's critical infrastructure and strategic national assets against increasingly sophisticated threats. Study of Ibekwe (2023) examines how credible intelligence contributes to improving internal security operations in Nigeria. Despite the presence of several security agencies, such as the Department of State Services (DSS), Force Intelligence Department (FID), Directorate of Military Intelligence (DMI), Directorate of Naval Intelligence (DNI), Air Intelligence Division (AID), Directorate of Intelligence and Investigation (DII) and the Defence Intelligence Agency (DIA), Nigeria continues to experience serious security threats, including terrorism, insurgency, banditry, and kidnapping. The research highlights how timely, accurate, and reliable intelligence can help prevent attacks, guide security operations, and improve coordination among agencies. It explores the main types of intelligence used – Human Intelligence (HUMINT), Signals

Volume 65 | Issue 03 | March 2026
DOI: 10.5281/zenodo.19509887

Intelligence (SIGINT), and Open Source Intelligence (OSINT) – and how they support decision-making in security matters. The study also identifies key challenges facing intelligence operations, such as poor inter-agency collaboration, lack of modern technology, limited funding, and low community trust. Through real-life examples and case studies, the study examined the benefits of intelligence led security efforts and the risks of faulty intelligence. The study concludes with recommendations to improve intelligence gathering and use, including creating a central coordination agency, involving communities more effectively, investing in technology, and strengthening international partnerships.

The study Nsirim, Abraham and Ajie (2024), underscores the integral role of libraries in promoting transparency, resilience, and collective efforts towards a more secure and stable nation. Libraries are positioned as dynamic information repositories, housing a diverse array of materials that range from academic research to intelligence analyses providing valuable insights into the complexities of insurgency. Through systematic literature reviews, articles were harvested from databases including Google Scholar, Research Gate, Academia, and ProQuest. The study examines the pivotal role of libraries in enhancing national security and combating insurgency in Nigeria. Findings reveal that libraries play a crucial role in public education and awareness, promoting literacy and critical thinking skills essential for citizens to resist extremist ideologies. Findings further indicate that the collaborative nature of libraries as neutral grounds facilitates cooperation among diverse stakeholders, fostering the exchange of insights and experiences that contribute to the development of innovative strategies. Findings recognise the contributions that libraries have made in generating new knowledge and cultivating an informed citizenry to address the root causes of insurgency and foster sustainable peace in Nigeria. The study highlights that libraries in Nigeria can play a vital role in enhancing national security and combating insurgency by serving as hubs for disseminating accurate information, fostering critical thinking skills, countering extremist propaganda, building community resilience, providing professional services.

MATERIAL AND METHODS

Study Area

Delta State, located in the western end of Nigeria's South-South region, is one of the major oil-producing states in the region. The state was created out of the defunct Bendel State on 27th, August, 1991. Before its creation, the area that makes up present-day Delta State was part of the old Mid-Western region (1963 – 1976). The state was created on the heels of agitations by the people of the old Delta Province for the creation of a new state known as Delta State. President Ibrahim Babangida acceded to the request of the people and created Delta State with Asaba as its capital. The name, Delta State was given to the state because of its location in the Delta region within the River Niger. The state has twenty-five local government areas spread fairly across the three senatorial districts (South, Central, and North) (Ogege, 2015). Delta State has an estimated population of about 5.681 million with Urhobo, Itsekiri, Ijaw, Isoko, ika, anioma, oshimili and Ndokwua/ukwuani as the main ethnic groups. These groups share ancestral and traditional administrative systems, evident in their dressing, language, festivals, music, and folklore (Okoh 2016). The vast majority of the inhabitants are Christians, with a few of them practicing traditional and Islamic religions. Since its creation in 1991, Delta State has had 10 Governors out of which four have been civilians elected by the people. From 1993 to 1999, Delta State, like other states in Nigeria, was ruled by military administrators. Military rule in Delta State was fraught with violent confrontations between the Nigerian

Volume 65 | Issue 03 | March 2026
DOI: 10.5281/zenodo.19509887

government security forces and the people, specifically those from oil-producing communities. At the core of this confrontation was the issue of unfair allocation of resources, the government's inability to affirm land boundaries between warring ethnic groups in the state, amongst other outcomes of poor governance (Human Rights Report 1999). Correspondingly, the issue of ethnic politicization was evident in the Warri Crisis that lasted for 7 years, where the Warri Southwest local government council headquarters was relocated from an Ijaw community to an Itsekiri community. It is pertinent to highlight the continued manipulation of ethnic ties by the political elite for personal interest in contemporary Delta State.

Map of Delta State

Sample Size and Sampling Technique

Given the fact that the study is centered on intelligence gathering, which is a security apparatus, confidentiality of the respondents was kept hence,purposive sampling technique will used to select 4 officers from the 25 Divisional offices, 5 officers from the state Head Quarters and 3 officers from the three area commands were be sampled. In total, 114 respondents formed the sample population for this study.

The instrument for data collection is the researcher's developed instrument (questionnai re) which was divided into two sections. Section A consisting of demographic data such as, gender, religion, marital status, educational qualification and leadership position. Section B consists of four (4) open-ended questions and a twenty (25) item closed ended questions on a four point Likert scale of Agree, Strongly Agree, Disagree, undecided and Strongly Disagree

Method of Data Analysis

The research questions were analysed using frequency counts and percentages. All analysis was done using the Statistical Package for the Social Sciences (SPSS).

RESULTS AND DISCUSSION

Demographic Data of Respondents

Table 1: Socioeconomic Characteristics of Respondents (n = 100)

Characteristics	Frequency	Percent (%)	Mean/Mode
Age Group			
Less than 20 years	0	0	45 years
20 -39	4	4	
30-39	45	.45	

Volume 65 | Issue 03 | March 2026
DOI: 10.5281/zenodo.19509887

40 – 49	40	40	
50 and above	11	11	
Total	**100**	**100.0**	
Gender of Respondents			
Male	82	82	Male
Female	18	18	
Total	**100**	**100.0**	
Marital Status of Respondents			
Single	7	7	Married
Married	93	93	
Total	**100**	**100.0**	
Educational Qualification of Respondents			
None Formal Education	6	6	Secondary
Primary Education	6	6	
Secondary Education	35	35	
OND	15	15	
HND	10	10	
B.Sc./BA/B.Ed./B. Agric.	28	28	
Total	**100**	**100.0**	
Religious distribution			
Christian	63	63	Christianity
Islam	20	20	
Others	17	17	
Total	**100**	**100.0**	
Intelligence gathering			
Yes	53	53	Yes
No	34	34	
Cannot remember	13	13	
Total	**100**	**100.0**	

Table 1 presents the socioeconomic characteristics of respondents and offers important insights into the human and institutional context within which intelligence for the protection of Nigeria's critical infrastructure and strategic national assets is generated, processed, and utilized. These characteristics are significant because intelligence effectiveness is closely tied to the demographic composition, educational background, and experiential capacity of personnel involved in security-related activities. Age distribution shows that the majority of respondents fall within the economically active and professionally mature age brackets. Respondents aged 30–39 years (45%) and 40–49 years (40%) together constitute 85% of the sample, with a mean age of 45 years. This suggests that intelligence-related roles and infrastructure protection responsibilities are largely handled by individuals with considerable life and work experience. Studies have shown that intelligence effectiveness improves when personnel possess accumulated institutional knowledge and situational awareness developed over time (Gill & Phythian, 2018). However, the relatively low representation of younger respondents may also imply limited infusion of new technological skills, which are critical for modern intelligence gathering, such as cyber intelligence and surveillance of digital infrastructure.

The gender distribution reveals a heavy male dominance (82%) compared to females (18%). While this reflects the traditional gender composition of Nigeria's security sector, it raises concerns regarding inclusivity and diversity in intelligence operations. Research indicates that gender-diverse intelligence teams often demonstrate improved analytical depth, reduced cognitive bias, and enhanced community engagement—an essential factor for human

Volume 65 | Issue 03 | March 2026
DOI: 10.5281/zenodo.19509887

intelligence (HUMINT) gathering (UNDP, 2019). The underrepresentation of women may therefore contribute indirectly to intelligence gaps, especially in community-based infrastructure protection. Regarding marital status, 93% of respondents are married. This may suggest stability and long-term commitment among personnel involved in infrastructure safeguarding. However, literature also points out that familial responsibilities can influence risk perception, mobility, and willingness to engage in high-threat intelligence operations (Abubakar, 2020). These factors may shape how intelligence officers prioritize threats to critical national assets such as oil pipelines, power grids, and transportation networks.

The educational qualifications of respondents show that 35% possess secondary education, while 28% hold bachelor's degrees and 25% possess post-secondary diplomas (OND/HND). Although this indicates a reasonable level of literacy, the dominance of secondary education as the modal qualification suggests limitations in advanced analytical capacity. Intelligence-led protection of critical infrastructure increasingly requires skills in data analysis, geospatial intelligence, cyber threat assessment, and strategic forecasting (OECD, 2020). Insufficient higher education among personnel can therefore exacerbate intelligence deficiencies, particularly in anticipating and preventing sophisticated attacks on national assets.

Religious distribution indicates that respondents are predominantly Christian (63%), followed by Muslims (20%) and others (17%). While religion itself does not directly affect intelligence performance, Nigeria's ethno-religious diversity has implications for intelligence gathering, especially in conflict-prone areas. Effective intelligence relies on trust, cultural understanding, and local legitimacy (Onuoha, 2018). A security workforce that reflects national diversity is better positioned to gather actionable intelligence across different communities where critical infrastructure is located.

Finally, responses on intelligence gathering reveal that only 53% affirm active intelligence-gathering involvement, while 34% report no involvement and 13% cannot remember. This finding is particularly revealing and underscores a core intelligence deficiency. The fact that nearly half of respondents are either not engaged or unsure about intelligence activities suggests weak institutional integration of intelligence functions. According to Nwolise (2017), ineffective coordination, poor intelligence culture, and lack of training remain major obstacles to protecting Nigeria's strategic assets from sabotage, terrorism, and vandalism. In summary, Table 1 highlights structural and human-capital-related intelligence deficiencies affecting Nigeria's ability to safeguard critical infrastructure. Addressing these gaps requires targeted training, improved educational standards, inclusive recruitment, and stronger institutional emphasis on intelligence-led security.

Table 2: Hierarchical Rank Structure of Respondents

Rank	Frequency	Percentage
Assistant Cadre	7	7.0
Inspectorate Cadre	22	22.0
Assistant Superintendent Cadre	21	21.0
Deputy Superintendent	22	22.0
Superintendent	7	7.0
Chief Superintendent	7	7.0
Assistant Commander	7	7.0
Deputy Commander	7	7.0
Total	**100**	**100**

(Source: Field Survey 2025)

Volume 65 | Issue 03 | March 2026
DOI: 10.5281/zenodo.19509887

Table 2 shows that respondents are spread across operational, supervisory, and command levels, with the Inspectorate (22%), Deputy Superintendent (22%), and Assistant Superintendent cadres (21%) forming the largest proportions. This indicates that intelligence-related inputs on critical infrastructure protection are largely drawn from mid-level officers who play a key role in translating strategic intelligence into operational action. The relatively smaller representation of senior command ranks may limit strategic intelligence coordination and policy-level decision-making. Studies emphasize that effective safeguarding of critical national assets requires strong vertical intelligence integration across ranks to ensure timely threat assessment and response (Gill & Phythian, 2018; Nwolise, 2017).

Table 3: Nature and Methods of Intelligence Gathering for the Protection of Critical Infrastructure

S/N	Nature for Intelligence Gathering	SDF (%)	DF (%)	UDF (%)	AF (%)	SAF (%)	Mean (SD)	Remarks
1	Payment of spies or informants from the community	7 (7.0%)	21 (21.0)	10 (10.0)	50 (50.0)	12 (12.0)	3.0 (3.0)	Agreed
2	Engaging private/surveillance security agencies	0 (0.0)	4 (4.0)	7 (7.0)	59 (59.0)	12 (12.0)	4.24 (0.69)	Agreed
4	Utilization and deployment of technological tools to monitor and gather intelligence	24 (24.0)	12 (12.0)	44 (44.0)	22 (22.0)	11.0 (11.0)	3.94 (1.15)	Agreed
5	Working with government security agencies	0 (0.0)	0 (0.0)	46 (46.0)	37 (37.0)	17 (17.0)	3.86 (0.66)	Agreed
6	Use of regular human patrol networks	0 (0.0)	16 (16.0)	17 (17.0)	39 (39.0)	18 (18.0)	3.76 (1.02)	Agreed
	Aggregate Mean						**3.86**	**Agreed**

Source: Fieldwork, 2025

The table presents respondents' perceptions of various methods used for intelligence gathering, highlighting their relevance to safeguarding critical infrastructure and strategic national assets. The aggregate mean score of 3.86 indicates a general agreement that the listed methods are actively utilized and considered effective within the intelligence and security framework.

The payment of spies or community informants recorded a mean score of 3.0, suggesting moderate agreement. This reflects the continued reliance on community-based human intelligence (HUMINT), which remains crucial in environments where formal surveillance coverage is limited. Scholars argue that local informants provide contextual, real-time information that is often inaccessible through technical means, particularly in rural or insurgency-prone areas (Onuoha, 2018; Gill & Phythian, 2018). However, concerns about reliability, informant motivation, and ethical implications may explain the relatively lower mean compared to other methods.

Engaging private and surveillance security agencies recorded one of the highest mean scores (4.24), indicating strong agreement among respondents. This underscores the increasing role of private security actors in intelligence collection and infrastructure protection. In Nigeria, private security firms often supplement overstretched state security agencies by providing surveillance, access control, and early warning intelligence (Abrahamsen & Williams, 2011). Their prominence reflects a shift toward pluralized security governance, although weak regulation may pose coordination and accountability challenges.

Volume 65 | Issue 03 | March 2026
DOI: 10.5281/zenodo.19509887

The utilization of technological tools for intelligence gathering, including surveillance systems and monitoring technologies, also received strong agreement (mean = 3.94). This aligns with global trends emphasizing intelligence-led security supported by technology such as CCTV, drones, and data analytics. According to OECD (2020), technological intelligence enhances situational awareness and enables proactive threat detection. Nevertheless, the relatively high standard deviation suggests uneven access to or proficiency in these technologies, pointing to capacity gaps within the system. Working with government security agencies achieved a mean score of 3.86, reflecting consensus on the importance of inter-agency collaboration. Effective intelligence sharing among police, military, and intelligence services is widely recognized as essential for protecting critical national assets (Nwolise, 2017). However, previous studies highlight that rivalry, bureaucratic silos, and poor information-sharing mechanisms often undermine such collaboration in Nigeria (Eze & Okeke, 2019).

The use of regular human patrol networks recorded a mean of 3.76, indicating agreement that patrols remain a viable intelligence source. Physical patrols provide visibility, deterrence, and immediate feedback from the field. Despite advancements in technology, patrol-based intelligence remains vital, especially in areas with limited digital infrastructure (UNODC, 2018).

The findings suggest that intelligence gathering for infrastructure protection in Nigeria is multi-dimensional, combining human, private-sector, technological, and institutional approaches. Strengthening coordination, training, and integration across these methods is essential to address existing intelligence deficiencies and enhance national security outcomes.

Table 4: Perceived Utilization of Intelligence Gathering Techniques among Security Personnel

S/N	Challenges militating against effective intelligence gathering	SDF (%)	DF (%)	UDF (%)	AF (%)	SAF (%)	Mean (SD)	Remarks
1	Lack of effective collaboration between stakeholders in intelligence gathering and sharing	0 (0.0)	19 (19.0)	0 (0.0)	56 (56.0)	25 (25.0)	4.11 (0.86)	Agreed
2	Poor attention given to host communities	0 (0.0)	14 (14.0)	15 (15.0)	31 (31.0)	40 (40.0)	4.11 (0.97)	Agreed
3	Compromise by private security and other government security agencies	14 (14.0)	19 (19.0)	11 (11.0)	38 (38.0)	29 (29.0)	3.09 (1.35)	Agreed
4	Poor mobilization of youths in host communities	0 (0.0)	14 (14.1)	19 (19.1)	29 (29.1)	37 (37.1)	4.00 (1.07)	Agreed
5	The use of ex-militants to protection oil and gas operations/ facilities	3 (3.0)	27 (27.0)	28 (28.0)	22 (22.0)	18 (18.0)	4.00 (0.86)	Agreed
6	Inter-agencies rivalry in terms of intelligence, information sharing	4 (4.0)	15 (15.0)	16 (16.0)	38 (38.0)	27 (27.0)	4.18 (1.00)	Agreed
7	Inadequate training of officers in the area of intelligence gathering skills	0 (0.0)	21 (21.0)	20 (20.0)	40 (40.0)	19 (19.0)	4.00 0.86	Agreed
8	Lack of Government will power or support on technological intelligence gathering	0 (0.0)	16 (16.0)	10 (10.0)	31 (31.0)	42 (42.0)	4.10 1.01	Agreed
	Aggregate Mean						**3.71**	**Agreed**

Source: Fieldwork, (2025)

Table 4 examines respondents' perceptions of strategies capable of improving intelligence gathering for the protection of critical infrastructure and strategic national assets, particularly within the operational mandate of the Nigeria Security and Civil Defence Corps (NSCDC). The aggregate mean score of 3.90 indicates strong overall agreement that the

Volume 65 | Issue 03 | March 2026
DOI: 10.5281/zenodo.19509887

identified strategies are essential for addressing existing intelligence deficiencies and strengthening national security outcomes. The deployment of more NSCDC officers to locations hosting oil, gas, and critical infrastructure recorded a mean score of 3.67, suggesting broad agreement among respondents. This finding highlights the importance of physical presence in intelligence gathering and infrastructure protection. Increased personnel deployment enhances visibility, deterrence, and real-time intelligence acquisition. According to Nwolise (2017), intelligence gathering is most effective when security personnel are embedded close to critical assets, enabling rapid identification of threats such as vandalism, sabotage, and insider collusion. However, deployment alone may be insufficient without complementary training and technological support.

The strategy with the highest mean score (4.67) is the strengthening of working relationships between host communities and NSCDC officials, underscoring the centrality of community-based intelligence. This finding aligns with extensive literature emphasizing that local communities serve as primary intelligence sources due to their familiarity with terrain, social networks, and suspicious activities (Onuoha, 2018). Effective collaboration fosters trust, information sharing, and early warning capabilities. In Nigeria's oil-producing regions, strained community–state relations have historically undermined intelligence flow, making this strategy particularly critical for infrastructure security (Albert, 2020). Respondents also agreed on the more effective use of private security agencies in intelligence gathering (mean = 3.86). This reflects the increasing pluralization of security provision in Nigeria, where private security firms support public agencies through surveillance, access control, and intelligence reporting. Abrahamsen and Williams (2011) argue that private security actors can significantly enhance intelligence coverage when properly regulated and integrated. However, coordination challenges and information-sharing gaps may limit their effectiveness if not adequately managed within a national intelligence framework.

The utilization of more technological equipment for protecting critical **assets** recorded a mean score of 3.91, indicating strong support for technology-driven intelligence. Technological tools such as CCTV, sensors, satellite monitoring, and communication intercept systems improve situational awareness and reduce reliance on purely human intelligence. OECD (2020) emphasizes that modern infrastructure protection depends heavily on technology-enabled intelligence to detect threats proactively. The relatively high standard deviation, however, suggests uneven access and capacity across operational units, highlighting the need for standardized deployment and training. The strategy of engaging community leaders as members of pipeline surveillance teams achieved a mean score of 3.42. While respondents generally agreed, the lower mean compared to broader community collaboration suggests concerns over elite capture, bias, or politicization of intelligence. Nonetheless, community leaders often act as gatekeepers and influencers, and their involvement can legitimize security initiatives and improve intelligence credibility (UNODC, 2018). Effective safeguards are required to ensure accountability and prevent compromise of intelligence operations.

The adoption of unmanned aerial vehicles **(UAVs)** for intelligence gathering recorded a mean score of 3.32, the lowest among the strategies but still within the agreed range. This reflects cautious optimism toward advanced surveillance technologies. UAVs offer significant advantages in monitoring vast and difficult terrains, especially pipelines and remote installations (Gill & Phythian, 2018). However, cost, technical expertise, regulatory constraints, and maintenance challenges may explain respondents' reservations, particularly in

Volume 65 | Issue 03 | March 2026
DOI: 10.5281/zenodo.19509887

resource-constrained environments. The continuous upgrading and training of officers in intelligence gathering and management recorded a high mean score of 4.37, demonstrating strong consensus on its importance. Intelligence effectiveness is closely linked to personnel competence, analytical skills, and adaptability to evolving threats. According to UNDP (2019), inadequate training remains a major contributor to intelligence failure in developing countries. Continuous capacity building enhances data analysis, inter-agency coordination, and ethical intelligence practices.

Finally, the protection of the identity of intelligence operators achieved a mean score of 4.25, reflecting strong agreement. This finding highlights concerns about retaliation, compromise, and loss of trust, particularly in community-based intelligence environments. Protecting informant and operator identities is critical to sustaining intelligence flow and operational effectiveness (Lowenthal, 2020). Failure to do so often leads to intelligence breakdown, fear, and community disengagement. In summary, Table 4.4 reveals that respondents favor a multi-layered approach to improving intelligence gathering, one that integrates community collaboration, personnel deployment, technology, training, and institutional safeguards. Addressing intelligence deficiencies in Nigeria therefore requires not only operational reforms but also trust-building, capacity development, and strategic coordination across state and non-state act

Table 5: Respondents' Perceptions of Strategies for Improving Intelligence Gathering in the Protection of Critical Infrastructure

S/N	Strategies to Improve Intelligence Gathering in protection	SDF (%)	DF (%)	UDF (%)	AF (%)	SAF (%)	Mean (SD)	Remarks
1	Deployment of more NSCDC security officers to where oil and gas and critical infrastructure is are located	4 (1.2)	10 (10.0)	3 (3.0)	60 (60.0)	23 (23.0)	3.67 (0.96)	Agreed
2	Greater working relationship between host communities and NSCDC officials.	0 (0.0)	0 (0.0)	7 (7.0)	21 (20.0)	63 (63.0)	4.67 (0.51)	Agreed
3	More effective use of private security agencies in intelligence gathering	11 (11.0)	15 (15.0)	17 (17.0)	40 (57.1)	17 (17.0)	3.86 (1.07)	Agreed
4	Utilization of more technology equipment with emphasis on protecting critical assets and national infrastructure	14 (14.0)	19 (19.0)	11 (11.0)	48 (48.0	12 (12.0)	3.91 (1.10)	Agreed
6	Engaging community leaders as members of pipeline surveillance team	21 (21.0)	15 (15.0)	11 (3.4)	50 (52.5)	17 (17.0)	3.42 (1.23)	Agreed
7	Adopting the use of unmanned aerial vehicles	12 (12.0)	20 (20.0)	12 (15.5)	30 (9.3)	22 (22.0)	3.32 (1.09)	Agreed
8	Provide continuous upgrading and training of officers and staff in intelligence gathering and management.	0 (0.0)	4 (4.0)	21 (21.0)	28 (28.0)	11 (11.0)	4.37 (0.71)	Agreed
10	Protect identity of intelligence operators within the organization/ communities.	0 (0.0)	20 (12.3)	11 (3.4)	50 (30.9)	13 (53.4)	4.25 (1.02)	Agreed
	Aggregate Mean						**3.90**	**Agreed**

Source: Fieldwork, 2025

CONCUSSION AND RECOMMENDATIONS

This study was focused on assessing the mechanisms for intelligence gathering protection of critical National assets and infrastructure by Nigerian security and civil defense corps in Delta State The major finding from this study revealed that considerable effort has been invested by stakeholders to adopt modern intelligence gathering in the protection of critical National assets and infrastructure by Nigerian security and civil defense corps in Delta State.

Volume 65 | Issue 03 | March 2026
DOI: 10.5281/zenodo.19509887

However, some challenges were identified which are militating against the effective utilization of intelligence gathering and management some of which includes lack of effective collaboration between stakeholders in intelligence gathering and management, and inter-agencies rivalry in terms of intelligence gathering and sharing These challenges have exacerbated social inequalities and economic losses. The study highlights the need for a multi-sectoral approach to improve intelligence gathering, involving oil companies, private security agencies, community leaders, and government bodies. Based on this report, some strategies were suggested which includes improving the working relationship between host communities, providing continuous upgrading and training of officers and staff in intelligence gathering and utilization of more technology equipment with emphasis on protecting critical assets and national infrastructure. The following recommendations were made;

(i). Formulation of Clear Policies: Clear policies and guidelines should be formulated to enhance synergy between agencies and stakeholders.

(ii). Stronger Collaboration: Improved collaboration and information sharing between agencies can promote a more robust and inclusive approach to safeguarding national assets.

(iii). Multi-Sectoral Approach: A multi-sectoral approach involving oil companies, private security agencies, community leaders, and government bodies can improve intelligence gathering and protect critical national assets and infrastructure.

(iv). Training and Capacity Building: The NSCDC should prioritize officer training and capacity building to enhance intelligence-gathering capabilities.

(v). Adequate Funding: Adequate funding should be provided to support the NSCDC's intelligence-gathering activities.

By implementing these recommendations, Nigeria can improve the protection of its critical national assets and infrastructure, promoting economic growth, national security, and social well-being.

References

1) Afolabi, M. B., Dogi, I. G., Ogunniyi, L. J., Agidigbi, E. R., & Oladipo, I. E. (2024). *Securing the critical infrastructure in Ondo State: Is the Nigeria Security and Civil Defence Corps up to the task?* African Renaissance.

2) Ibanga, I. J., Fwah, K. G., & Idowu, A. J. (2022). Assessing the vulnerabilities: Cybersecurity challenges in power system infrastructure in Nigeria. *International Journal of Information Technology & Computer Engineering*, *44*(22), 35.

3) Olowonihi, A. P., & Musa, M. O. (2024). The role of intelligence in Nigeria's national security: A critical assessment (2011-2023). *The American Journal of Interdisciplinary Innovations and Research*, *6*(11), 113-141.

4) Olowonihi, A. P., & Musa, M. O. (2024). Intelligence gathering and its contribution to Nigeria's national security: A critical assessment. *The American Journal of Interdisciplinary Innovations and Research*, *6*(11

5) Tabiowo, E. (2025). A critical review of the impact of inadequate legislative frameworks on national security in Nigeria. *Security Intelligence Terrorism Journal (SITJ)*, *2*(3).

Volume 65 | Issue 03 | March 2026
DOI: 10.5281/zenodo.19509887

6) "Threats to Critical Infrastructure and Oil Theft in Niger Delta Region of Nigeria." (2023). *West African Journal of Interdisciplinary Research, 3*(1), 25-35.

7) Tunji-Ojo, O. (2024). Safeguarding Nigeria's Critical Infrastructure Against Vandalism. *News Agency of Nigeria*.

8) Adebajo, A. (2020). *Security Challenges in Nigeria: Intelligence and Counterterrorism*. African Security Review, 29(1), 45-60.

9) Adejumobi, S., & Obadare, E. (2019). Intelligence Failures and National Security in Nigeria: An Overview. *Journal of African Security Studies*, 12(2), 78-95.

10) Buzan, B., Waever, O., & De Wilde, J. (1998). *Security: A New Framework for Analysis*. Lynne Rienner Publishers.

11) Hulnick, A. S. (2006). *Keeping Us Safe: Homeland Security and Intelligence Reform*. Praeger Security International.

12) Johnson, L. K. (2010). *Handbook of Intelligence Studies*. Routledge.

13) Kapucu, N., & Hu, Q. (2016). Understanding Multiplexity of Network Governance: A Systems Approach. *Public Administration Review*, 76(4), 658-669.

14) Kettler, G. (2008). Critical Infrastructure Protection: Protecting the Nation's Strategic Assets. *Journal of Homeland Security*, 4(3), 23-33.

15) Lowenthal, M. M. (2017). *Intelligence: From Secrets to Policy* (7th ed.). CQ Press.

16) National Infrastructure Protection Plan (NIPP). (2013). *U.S. Department of Homeland Security*. Retrieved from https://www.dhs.gov/national-infrastructure-protection-plan

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

18) Nwolise, O. B. C. (2017). Intelligence gathering and internal security management in Nigeria. *African Journal of Security Studies*, 6(2), 45–61.

19) Abubakar, A. (2020). *Security sector reform and intelligence coordination in Nigeria*. Abuja: National Defence College Press.

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

21) Nwolise, O. B. C. (2017). Intelligence gathering and internal security management in Nigeria. *African Journal of Security Studies*, 6(2), 45–61.

22) OECD. (2020). *Good governance for critical infrastructure resilience*. Paris: OECD Publishing.

23) Onuoha, F. C. (2018). Oil pipeline sabotage and national security in Nigeria. *Journal of African Security*, 11(1), 25–44.

24) UNDP. (2019). *Gender and inclusive security sector reform*. New York: United Nations Development Programme.

25) Abrahamsen, R., & Williams, M. C. (2011). *Security beyond the state: Private security in international politics*. Cambridge: Cambridge University Press.

Volume 65 | Issue 03 | March 2026
DOI: 10.5281/zenodo.19509887

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

27) Nwolise, O. B. C. (2017). Intelligence gathering and internal security management in Nigeria. *African Journal of Security Studies*, 6(2), 45–61.

28) OECD. (2020). *Good governance for critical infrastructure resilience*. Paris: OECD Publishing.

29) Onuoha, F. C. (2018). Community-based intelligence and internal security in Nigeria. *Journal of African Security*, 11(1), 25–44.

30) UNODC. (2018). *Handbook on intelligence-led policing*. Vienna: United Nations Office on Drugs and Crime.

31) Eze, M. C., & Okeke, V. O. (2019). Inter-agency rivalry and national security management in Nigeria. *International Journal of Social Sciences*, 4(3), 112–124.

33) Abrahamsen, R., & Williams, M. C. (2011). *Security beyond the state: Private security in international politics*. Cambridge: Cambridge University Press.

34) Albert, I. O. (2020). Community engagement and internal security management in Nigeria. *African Security Review*, 29(3), 211–225.

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

36) Lowenthal, M. M. (2020). *Intelligence: From secrets to policy* (8th ed.). Washington, DC: CQ Press.

37) Nwolise, O. B. C. (2017). Intelligence gathering and internal security management in Nigeria. *African Journal of Security Studies*, 6(2), 45–61.

38) OECD. (2020). *Good governance for critical infrastructure resilience*. Paris: OECD Publishing.

39) Onuoha, F. C. (2018). Community-based intelligence and national security in Nigeria. *Journal of African Security*, 11(1), 25–44.

40) UNDP. (2019). *Human development and security sector reform*. New York: United Nations Development Programme.

41) UNODC. (2018). *Handbook on intelligence-led policing*. Vienna: United Nations Office on Drugs and Crime.