



Counterintelligence Effectiveness in Nigeria: Legal Framework and Intelligence Governance Assessment

Muhammad Auwal Sule^{1*}

Makieze International, Abuja, Nigeria¹

*Corresponding author: albalagu1@gmail.com

Received: 18 May 2026 | Revised: 20 June 2026 | Revised: 25 June 2026 | Published: 25 July 2026

Abstract

Purpose: This study aims to examine the legal framework, intelligence governance, and institutional conditions influencing counterintelligence effectiveness in Nigeria, with particular attention to the National Intelligence Agency (NIA).

Research Methodology: This study employed a qualitative documentary research design. Data were collected from legislation, national policy documents, official publications, international assessments, and scholarly literature. The data were analysed using thematic analysis focusing on legal adequacy, institutional capacity, inter-agency coordination, technological and human-capital preparedness, and accountability within legitimate secrecy requirements.

Results: The study finds that Nigeria has established a substantial legal and policy foundation for intelligence and information protection through the Official Secrets Act 1962, National Security Agencies Act 1986, National Cybersecurity Policy and Strategy 2021, Nigeria Data Protection Act 2023, Cybercrimes Amendment Act 2024, and Critical National Information Infrastructure framework. However, emerging cyber-enabled espionage, digital threats, and transnational challenges require continuous legal reform, stronger coordination, technological improvement, and specialised human-capital development.

Conclusions: Counterintelligence effectiveness should be understood through institutional capacity, including legal adequacy, secure information management, professional expertise, coordination, and accountable governance, rather than solely through disclosed operational outcomes.

Limitations: The study is limited by the restricted availability of classified intelligence information and therefore assesses enabling conditions rather than direct operational performance.

Contributions: This study contributes to intelligence governance literature by providing an integrated perspective on legal, institutional, technological, and governance factors supporting counterintelligence effectiveness.

Keywords: *Counterintelligence, Intelligence Governance, National Intelligence Agency, National Security, Official Secrets Act*

How to Cite: Sule, M. A. (2026). Counterintelligence Effectiveness in Nigeria: Legal Framework and Intelligence Governance Assessment. *Advanced Studies in Law, Policy Innovation, and Institutional Reform (ASLPI)*, 1(3), 137-149.

1. Introduction

National security increasingly depends on the ability of states to obtain, analyse, protect, and responsibly manage information in an environment where security threats are no longer limited to conventional military confrontation. Contemporary threats increasingly involve terrorism, organised crime, cybercrime, hostile information activities, and transnational security challenges that operate

across physical and digital boundaries ([Knierp, Ewert, Tréguer, McCluskey, & Aradau, 2024](#); [Cascavilla, Tamburri, & Van, 2021](#)). The rapid expansion of digital connectivity has increased the volume and complexity of information available to governments while simultaneously creating new vulnerabilities related to unauthorised access, manipulation, and exploitation of sensitive information ([Sarker, Kayes, Badsha, Alqahtani, Watters, & Ng, 2021](#)). Consequently, intelligence institutions are required to integrate traditional intelligence capabilities with technological, analytical, and information-security capacities.

Counterintelligence represents an essential component of modern intelligence systems because it focuses on protecting intelligence capabilities, sensitive information, personnel, and institutions from hostile penetration, compromise, exploitation, and unauthorised disclosure. Although counterintelligence activities are often associated with classified operations, their effectiveness is also shaped by broader institutional conditions, including legal authority, governance structures, technological preparedness, and professional expertise ([Knierp et al., 2024](#)). The increasing use of digital technologies has further expanded counterintelligence challenges because hostile actors can exploit cyber vulnerabilities, compromised credentials, malicious software, and other technology-enabled methods to access protected information ([Cascavilla et al., 2021](#)). Therefore, effective counterintelligence requires not only operational capability but also a strong institutional foundation.

In Nigeria, the intelligence architecture is primarily established through the National Security Agencies Act 1986, which created the Defence Intelligence Agency (DIA), National Intelligence Agency (NIA), and State Security Service, currently known as the Department of State Services (DSS). Under this legal framework, the NIA is responsible for external intelligence concerning non-military matters and other responsibilities assigned according to law ([Federal, 1986](#)). The protection of official information is further supported by the Official Secrets Act 1962, which provides legal provisions against unauthorised communication, obtaining, reproduction, and retention of protected government information ([Federal, 1962](#)).

However, the contemporary security environment has changed significantly from the period when many traditional secrecy frameworks were developed. The emergence of cyber-enabled espionage, digital information systems, cloud-based storage, and interconnected networks has created new challenges for protecting sensitive information. Although Nigeria has introduced additional legal and policy instruments, including the National Cybersecurity Policy and Strategy 2021, Nigeria Data Protection Act 2023, Cybercrimes (Prohibition, Prevention, etc.) Amendment Act 2024, and Critical National Information Infrastructure framework, continuous adaptation is required to ensure that existing frameworks remain relevant to evolving security threats ([Federal, 2021](#); [Federal, 2023](#); [Federal, 2024a](#)).

Beyond legal frameworks, counterintelligence effectiveness is also influenced by institutional coordination, technological capability, and human capital. Contemporary security threats often cross institutional and national boundaries, requiring effective cooperation among intelligence and security institutions. Nigeria national security structure involves multiple institutions, including the NIA, DSS, DIA, Armed Forces, Nigeria Police Force, and Office of the National Security Adviser (ONSA). Although government initiatives have emphasised stronger intelligence sharing and institutional cooperation, broader assessments of Nigeria cybersecurity environment indicate continuing challenges related to coordination, duplication, and fragmented operations. These conditions demonstrate the importance of strengthening governance mechanisms that enable secure and effective intelligence coordination.

Technological capability and specialised human resources are also increasingly important components of counterintelligence effectiveness. Modern intelligence environments require personnel with expertise in cybersecurity, digital forensics, data analytics, information security, and emerging technologies. The complexity of cyber-related threats requires intelligence institutions to continuously develop professional capabilities and technological infrastructure. The World Bank also highlights the

global shortage of cybersecurity skills, demonstrating the importance of investing in specialised human capital to support information protection and digital security.

Nevertheless, evaluating intelligence effectiveness presents a methodological challenge because intelligence operations are conducted under legitimate secrecy requirements. Information regarding sources, methods, investigations, vulnerabilities, and operational outcomes is generally classified and unavailable to public researchers. Therefore, the absence of publicly disclosed operations cannot be interpreted as evidence of either success or failure. Instead, counterintelligence effectiveness should be examined through publicly observable institutional conditions, including legal adequacy, governance arrangements, technological preparedness, human-capital capacity, coordination mechanisms, and accountability structures ([Kniep et al., 2024](#); [Muchwa, 2021](#); [Olayinka & Kaka, 2025](#))).

Although previous studies have discussed intelligence governance, national security institutions, and cybersecurity challenges, limited research has examined counterintelligence effectiveness in Nigeria through an integrated perspective that combines legal frameworks, institutional capacity, technological readiness, human capital, coordination, and accountability. This gap is particularly relevant because intelligence effectiveness cannot be assessed solely through operational outcomes but requires an understanding of the institutional environment that enables intelligence organisations to function effectively.

Based on this context, this study aims to examine the legal framework, intelligence governance, and institutional conditions influencing counterintelligence effectiveness in Nigeria, with particular attention to the National Intelligence Agency. The study contributes to intelligence governance literature by providing a framework for assessing counterintelligence effectiveness through publicly observable institutional factors while recognising legitimate secrecy requirements. Practically, the findings provide insights into how legal reform, stronger coordination, technological development, professional capacity building, and accountable governance can strengthen Nigeria counterintelligence capability.

2. Literature Review and Hypothesis/es Development

2.1 Concept of Counterintelligence

Counterintelligence may broadly be understood as the organised effort of a state to identify, prevent, disrupt and mitigate activities intended to compromise its intelligence capabilities, sensitive information, personnel, institutions or national security interests. Unlike intelligence collection, which is primarily concerned with obtaining information about relevant threats and environments, counterintelligence is concerned with protecting the intelligence system and the state from hostile intelligence activities and information compromise ([Putter & Dov, 2023](#)).

The contemporary meaning of counterintelligence has expanded because hostile intelligence activity can occur through both physical and digital channels. Cyber intrusion, credential compromise, malicious software, unauthorised access to databases and manipulation of digital information can create vulnerabilities comparable to more traditional forms of espionage and information compromise. Nigeria's cybersecurity strategy consequently identifies the protection of national information systems and strengthening of cybersecurity governance as important components of national security ([Federal, 2021](#); [Heriyanto, Alie, CN, Desmon, Oktaria, Megasari, & Bakti, 2026](#))).

Counterintelligence effectiveness should therefore not be reduced to the number of publicly announced arrests, disrupted espionage activities or disclosed operations. Intelligence institutions frequently operate under secrecy, and successful counterintelligence may be reflected precisely in events that never become public. For this reason, effectiveness is better examined through enabling conditions such as legal authority, information protection, professional capacity, coordination, technological preparedness and institutional governance ([David, Yigitcanlar, Li, Corchado, Cheong, Mossberger, & Mehmood, 2023](#)).

2.2 Intelligence Governance and National Security

Intelligence governance refers to the legal, institutional and administrative arrangements through which intelligence agencies receive mandates, exercise authority, coordinate activities and are subject to lawful oversight. Intelligence governance is particularly important because intelligence organisations possess powers and access to information that can affect national security, privacy and individual rights ([Watt, 2017](#); [Nwosu, Obalum, & Ananti, 2024](#)).

[Kniep, Ewert, Tréguer, McCluskey, and Aradau \(2024\)](#), argue that democratic intelligence oversight involves managing the tension between secrecy and public accountability. This suggests that effective intelligence governance should not seek to eliminate secrecy but should establish mechanisms through which secrecy is exercised within a lawful institutional framework. [Muchwa \(2021\)](#) similarly identifies legal and institutional challenges affecting intelligence oversight in Uganda, illustrating broader difficulties experienced by intelligence systems in balancing operational secrecy with accountability.

In Nigeria, the National Security Agencies Act provides a formal basis for the establishment and coordination of national intelligence agencies ([Federal, 1986](#)). The Act's coordination provisions are particularly significant because intelligence effectiveness depends not only on the capability of individual agencies but also on the capacity of institutions to exchange relevant information while protecting sensitive sources and methods ([Olowonihi & Musa, 2024](#)).

2.3 Legal Framework for Nigerian Intelligence and Counterintelligence

The Official Secrets Act constitutes an important component of Nigeria's information-security legislation. It criminalises specified forms of unauthorised communication, obtaining, reproduction and retention of protected official information and contains provisions relating to protected government and defence establishments ([Federal, 1962](#)). The legislation therefore provides a statutory foundation for protecting official information from unauthorised disclosure. The National Security Agencies Act 1986 complements this framework by establishing the country's principal intelligence agencies and assigning responsibilities among them. The NIA's statutory mandate is principally external and non-military, while the DIA focuses on defence intelligence and the DSS on internal security responsibilities ([Federal, 1986](#)).

The legal environment has subsequently become more complex as information security has expanded beyond conventional classified documents. The National Cybersecurity Policy and Strategy 2021 provides a national policy framework for cybersecurity, while the Nigeria Data Protection Act 2023 regulates personal-data processing and establishes a broader governance framework for data protection ([Federal, 2023](#)). The Cybercrimes Amendment Act 2024 and Critical National Information Infrastructure Order 2024 further strengthen the legal environment for protecting digital systems and responding to technology-enabled threats ([Federal, 2024a](#)).

The implication is that counterintelligence effectiveness increasingly depends on the interaction between traditional secrecy legislation and newer cybersecurity, data-protection and critical-infrastructure frameworks. The legal question is therefore not simply whether Nigeria has legislation protecting official information, but whether the various legal instruments are sufficiently harmonised to address contemporary forms of information compromise. A coordinated legal framework is required to reduce regulatory gaps, strengthen institutional responsibilities, and ensure that intelligence agencies can respond effectively to evolving technological threats. Furthermore, continuous legal adaptation is necessary to maintain the balance between national security requirements, information protection, and accountable governance ([Okoli, & Aina, 2024](#); [Olowonihi, & Musa, 2024](#)).

2.4 Inter-Agency Coordination

Inter-agency coordination is essential because intelligence threats frequently cross institutional and jurisdictional boundaries. Terrorism, cybercrime, transnational organised crime and other complex

threats can generate intelligence requirements for multiple institutions simultaneously. Evidence from Nigeria's contemporary security environment demonstrates continued government emphasis on intelligence sharing and institutional cooperation. Presidential engagements have involved the NIA, DSS, DIA, Armed Forces, Police and ONSA in coordinated security discussions. Nigeria's international security cooperation has also incorporated intelligence institutions into broader bilateral and multilateral mechanisms ([Farber, 2025](#); [Khan, Zakir, Tayyab, & Ibrahim, 2024](#)).

However, coordination should not be understood simply as physical meetings among agencies. Effective coordination requires secure information-sharing procedures, compatible information systems, clearly defined responsibilities, timely dissemination and mechanisms for resolving duplication or institutional competition. The United Nations UNODC assessment and subsequent UN reporting identify siloed operations, duplication and coordination difficulties within Nigeria's wider cybercrime-response environment, demonstrating the continuing importance of institutional integration ([Peacock, Bruno, Gisev, Degenhardt, Hall, Sedefov, & Griffiths, 2019](#)).

2.5 Technology and Counterintelligence

Technology has transformed both the capabilities available to intelligence institutions and the vulnerabilities they must manage. Digital communication, networked databases, cloud systems, mobile devices and artificial intelligence can improve information processing while simultaneously increasing the attack surface available to hostile actors. Nigeria's National Cybersecurity Policy and Strategy recognises the need to protect critical information infrastructure and strengthen national cybersecurity capacity ([Federal Republic of Nigeria, 2021](#)). The UNODC assessment similarly demonstrates that contemporary cybercrime investigations require specialised technical knowledge and digital forensic capability. These developments are relevant to counterintelligence because sensitive intelligence information may exist, move or be processed through digital systems.

Technological preparedness should therefore encompass secure communications, cyber-resilient infrastructure, digital forensics, threat analysis, data analytics and continuous vulnerability assessment. Technology alone, however, cannot produce effective counterintelligence. Its value depends upon professional personnel, sound procedures and institutional coordination ([Ezeagwuna, 2026](#)). Therefore, technological capabilities must be integrated with effective governance mechanisms and continuous improvement strategies to ensure that intelligence institutions can anticipate, detect, and respond to emerging threats. In this context, technology serves as an enabling factor that strengthens, rather than replaces, human expertise and organisational capacity ([Luna-Reyes, Juiz, Gutierrez-Martinez, & Duhamel, 2020](#)).

2.6 Human Capital and Intelligence Effectiveness

Human capital is a central component of intelligence capability because intelligence work requires analytical judgement, technical expertise, discretion, contextual knowledge, and professional ethics. The increasing complexity of cyber threats has expanded the expertise required within security institutions, requiring personnel who can integrate intelligence knowledge with technological capabilities. Therefore, intelligence effectiveness depends not only on institutional structures but also on the competence and professionalism of its personnel. Continuous development of human resources is necessary to ensure that intelligence organisations can respond effectively to evolving security challenges ([Pomaza-Ponomarenko, Taraduda, Kravchuk, Moroz, Akhmedova, & Poroka, 2025](#)).

The growing reliance on digital technologies has increased the need for specialised skills in intelligence institutions. The World Bank highlights a global shortage of cybersecurity professionals and the importance of skills in incident response, cybercrime investigation, and critical infrastructure protection. This condition shows that traditional intelligence capabilities must be strengthened through continuous training and technological expertise. Therefore, professional development and competency improvement are essential for maintaining intelligence effectiveness ([Boikanyo, 2024](#); [Erhimu, 2026](#)).

Human-capital development should also include ethical standards and information-security awareness because insider threats may arise from misuse, negligence, or unauthorised disclosure of sensitive information. Personnel security is therefore an important element of counterintelligence, as information protection depends on both technological systems and responsible human behaviour. Intelligence institutions need to strengthen security awareness, professional integrity, and compliance with confidentiality requirements. Consequently, human-capital development should be viewed as a strategic component of counterintelligence capability ([Ussher-Eke, 2025](#)).

2.7 Secrecy, Accountability and Oversight

Secrecy is an operational necessity in intelligence work because disclosure of sources, methods, investigations, or vulnerabilities can compromise national security. The Nigerian Government has publicly recognised that operational details concerning ongoing security activities cannot always be disclosed. This condition reflects the unique nature of intelligence institutions, where confidentiality is required to protect operational integrity and prevent exploitation by hostile actors. Therefore, secrecy remains an essential element in maintaining effective intelligence and counterintelligence capabilities ([Moses & De, 2018](#)).

Nevertheless, secrecy does not remove the need for accountability. Intelligence oversight scholarship indicates that democratic governance requires institutional mechanisms for reviewing the legality and performance of intelligence agencies while protecting information that legitimately requires classification ([Kniep et al., 2024](#)). Nigeria's defence and security governance literature similarly emphasises the importance of appropriate legislative oversight ([Adelani & Ukwani, 2024](#)). Effective oversight enables intelligence institutions to maintain public trust while ensuring that security powers are exercised within legal and institutional boundaries. Thus, accountability should function as a mechanism to strengthen, rather than weaken, intelligence effectiveness ([Anochiwa, 2021](#)).

The appropriate objective is therefore not maximum disclosure but controlled accountability. Oversight mechanisms should have authorised access to classified information where necessary, operate through secure procedures, and focus on legality, expenditure, institutional performance, and compliance without exposing operational sources and methods ([Erhimu, 2026](#)). Such an approach allows intelligence organisations to preserve necessary secrecy while ensuring responsible governance and institutional integrity. Consequently, a balanced relationship between confidentiality and accountability is essential for sustainable counterintelligence effectiveness ([Khan & Mita, 2023](#)).

2.8 Theoretical Framework

2.8.1 Intelligence-Led Security Theory

This study is principally anchored in the intelligence-led security perspective, which views timely, accurate, and systematically analysed information as a fundamental basis for preventive security decision-making. The central assumption of this perspective is that security institutions are better able to anticipate, identify, and manage emerging threats when intelligence is effectively collected, analysed, coordinated, shared, and transformed into actionable decisions. Therefore, intelligence is not merely considered as information gathering, but as a strategic capability that supports institutional responses to complex security challenges.

Applied to counterintelligence, the intelligence-led security perspective suggests that effectiveness depends not only on the existence of intelligence agencies but also on the broader institutional conditions that enable intelligence functions to operate effectively. These conditions include adequate legal authority, competent human resources, secure information systems, analytical capabilities, inter-agency coordination, and mechanisms that ensure intelligence findings can contribute to appropriate security decisions. Consequently, counterintelligence effectiveness should be understood as an integrated capability involving legal, organisational, technological, and governance dimensions.

This theoretical perspective is particularly relevant to the Nigerian context because the National Security Agencies Act establishes distinct intelligence institutions while also emphasising the

coordination of intelligence activities among security agencies ([Federal Republic of Nigeria, 1986](#)). The continued government emphasis on intelligence sharing, institutional cooperation, and inter-agency synergy further demonstrates the importance of coordinated intelligence governance in strengthening national security capabilities. Therefore, the intelligence-led security perspective provides an appropriate foundation for analysing how legal frameworks, governance arrangements, institutional capacity, and coordination mechanisms influence counterintelligence effectiveness in Nigeria.

2.8.2 Human Security Perspective

This study also draws upon the human security perspective, which expands the traditional understanding of security beyond the protection of territorial sovereignty to include the protection of individuals, communities, and institutions from threats that may affect their safety, stability, and wellbeing. This perspective emphasises that security should not only focus on state survival but also on creating conditions that enable societies and institutions to function safely and effectively. In this context, intelligence and counterintelligence serve broader national security objectives by identifying, preventing, and mitigating threats that may undermine social stability, institutional integrity, and public trust.

From this perspective, effective intelligence governance should protect national security while respecting legality, privacy and institutional accountability. The Nigeria Data Protection Act 2023 illustrates the importance of reconciling information management with rights-protection requirements ([Federal Republic of Nigeria, 2023](#)). The study therefore considers counterintelligence effectiveness within a governance framework in which security and lawful institutional conduct are complementary rather than competing objectives.

3. Research Methodology

This study employed a qualitative documentary research design to examine the legal framework, intelligence governance, and institutional conditions influencing counterintelligence effectiveness in Nigeria, with particular attention to the National Intelligence Agency (NIA). A qualitative approach was considered appropriate because significant aspects of intelligence and counterintelligence activities are classified and cannot be responsibly assessed through direct observation or unsupported claims regarding operational outcomes. Documentary research enables systematic examination of publicly available legal, institutional, and policy materials to understand the structural conditions that shape intelligence effectiveness.

The study utilised secondary data obtained from authoritative documentary sources. The primary documents analysed included the Official Secrets Act 1962, National Security Agencies Act 1986, National Cybersecurity Policy and Strategy 2021, Nigeria Data Protection Act 2023, Cybercrimes (Prohibition, Prevention, etc.) Amendment Act 2024, and Critical National Information Infrastructure Order 2024 ([Federal, 2021](#); [Federal, 2023](#); [Federal, 2024a](#)). These legal and policy documents were complemented by official government publications, international institutional reports, and relevant academic literature to provide broader contextual understanding of intelligence governance, cybersecurity challenges, institutional coordination, and human-capital requirements.

Additional documentary evidence was collected from official Presidency materials concerning national security coordination, inter-agency cooperation, and international security engagements involving Nigerian intelligence institutions. Reports from international organisations, including the UNODC, the World Bank, and the ISS, were also examined to contextualise broader challenges related to cyber threats, technological preparedness, intelligence capacity, and governance arrangements.

The collected documents were analysed using thematic analysis. The analysis process involved identifying, organising, and interpreting recurring themes related to counterintelligence effectiveness. The analysis focused on five main themes, including legal adequacy, institutional capacity,

inter-agency coordination, technological and human-capital preparedness, and accountability and governance. The analysis focused exclusively on publicly observable institutional conditions and deliberately avoided speculation regarding classified intelligence sources, operational methods, intelligence targets, or undisclosed counterintelligence activities.

A key limitation of this study relates to the restricted availability of classified intelligence information. Publicly accessible documents cannot provide a complete assessment of operational counterintelligence performance because sensitive information concerning intelligence activities remains protected. Therefore, the study does not attempt to determine whether NIA counterintelligence operations have succeeded or failed; instead, it evaluates the legal, institutional, technological, and governance conditions that enable effective counterintelligence. This approach ensures that the analysis remains evidence-based while respecting legitimate secrecy requirements within intelligence operations.

4. Results and Discussions

4.1 Legal Foundation and the Need for Counterintelligence Legal Modernisation

The findings indicate that Nigeria possesses a substantial legal foundation for intelligence governance and information protection. The National Security Agencies Act 1986 provides the statutory basis for the establishment and responsibilities of the NIA, particularly regarding external intelligence functions, while the Official Secrets Act 1962 establishes legal provisions against unauthorised disclosure and handling of protected official information ([Federal, 1986](#)). These legal instruments demonstrate that Nigeria has long recognised the importance of protecting sensitive information as part of national security governance.

However, the contemporary intelligence environment differs significantly from the context in which these earlier legal instruments were developed. The emergence of cyber-enabled espionage, digital information systems, cloud-based data storage, and interconnected communication networks has expanded the nature of information-security risks faced by intelligence institutions. In response, Nigeria has introduced additional legal and policy frameworks, including the National Cybersecurity Policy and Strategy 2021, Nigeria Data Protection Act 2023, Cybercrimes (Prohibition, Prevention, etc.) Amendment Act 2024, and Critical National Information Infrastructure Order 2024 ([Federal, 2021](#); [Federal, 2023](#); [Federal, 2024a](#)).

These developments suggest that the primary legal challenge is not the absence of intelligence-related legislation, but rather the need to ensure greater coherence between traditional secrecy regulations and emerging digital-security frameworks. Effective counterintelligence requires legal clarity regarding electronic information protection, cyber-enabled espionage, digital evidence management, secure information exchange, and responsibilities among relevant institutions. Therefore, legal modernisation should focus on harmonising existing instruments to ensure that intelligence institutions can respond effectively to contemporary threats.

The National Cybersecurity Policy and Strategy provides an important foundation for this process by identifying legal strengthening, national information protection, and data governance as strategic priorities ([Federal, 2021](#)). This finding supports the intelligence-led security perspective, which emphasises that effective intelligence capability depends not only on operational agencies but also on supportive legal and institutional frameworks.

4.2 Institutional Coordination as a Foundation of Counterintelligence Effectiveness

The findings demonstrate that institutional coordination is a critical component of counterintelligence capability. Intelligence activities require cooperation among multiple security institutions because contemporary threats frequently extend beyond the jurisdiction of a single agency. The National Security Agencies Act 1986 recognises the importance of coordination within Nigeria intelligence architecture by

establishing different agencies with complementary responsibilities ([Federal Republic of Nigeria, 1986](#)).

Government practices also indicate continued emphasis on intelligence cooperation involving institutions such as the NIA, DSS, DIA, Armed Forces, Nigeria Police Force, and ONSA. Such coordination is essential because effective counterintelligence depends on the ability to collect, integrate, analyse, and distribute relevant information among authorised institutions. Nevertheless, broader assessments of Nigeria security environment indicate that coordination challenges may remain, particularly in areas involving cybersecurity responses and institutional cooperation. Reports from UNODC and United Nations in Nigeria highlight challenges associated with fragmented responsibilities, duplication, and coordination difficulties among agencies involved in addressing cyber-related threats. These observations should not be interpreted as direct evidence of NIA operational weaknesses, but they demonstrate the importance of strengthening governance mechanisms for intelligence coordination.

Therefore, effective counterintelligence requires a balance between information accessibility and information protection. Intelligence-sharing mechanisms must ensure that relevant information reaches authorised institutions in a timely manner while preventing unnecessary exposure or unauthorised dissemination. This finding reinforces the importance of intelligence governance structures that promote cooperation while maintaining security controls.

4.3 Technological Preparedness and the Transformation of Counterintelligence

The findings indicate that technological preparedness has become an essential component of contemporary counterintelligence effectiveness. The increasing use of digital technologies has transformed the nature of security threats, requiring intelligence institutions to develop capabilities beyond conventional information collection. Nigeria cybersecurity framework recognises the importance of protecting critical information systems and strengthening national cybersecurity capacity ([Federal, 2021](#)).

Contemporary counterintelligence increasingly requires secure communication systems, cyber-resilient infrastructure, digital forensics, threat analysis, data analytics, and continuous vulnerability assessment. These capabilities enable intelligence institutions to identify emerging threats, protect sensitive information, and respond to technology-driven security challenges. The UNODC assessment further demonstrates that cybercrime and digital threats require specialised technical capabilities and advanced investigative approaches.

However, technology alone cannot guarantee effective counterintelligence. The effectiveness of technological systems depends on the availability of skilled personnel, appropriate procedures, institutional coordination, and governance mechanisms. Therefore, technological preparedness should be understood as an enabling capability that strengthens human expertise and organisational capacity rather than replacing them.

4.4 Human Capital Development as a Strategic Intelligence Capability

The findings highlight human capital as a fundamental element of modern intelligence effectiveness. Intelligence activities require personnel with analytical judgement, technical expertise, discretion, contextual understanding, language capability, and professional ethics. The increasing complexity of cyber-enabled threats has expanded the range of skills required within intelligence institutions, particularly in areas such as cybersecurity, digital analysis, and information management. The global shortage of cybersecurity professionals identified by the World Bank further demonstrates the challenge faced by governments in developing specialised security capabilities. Although this evidence is not specific to NIA, it reflects a broader challenge in ensuring that intelligence institutions possess adequate technical expertise to address evolving threats ([Pomaza-Ponomarenko, Taraduda, Kravchuk, Moroz, Akhmedova, & Poroka, 2025](#)).

For Nigeria, this finding highlights the importance of continuous professional development within intelligence institutions. Human-capital development should include cybersecurity training, digital intelligence capabilities, data analytics, strategic assessment, information-security management, and ethical standards. Professional competence is particularly important because intelligence personnel operate within sensitive environments where negligence, misuse, or unauthorised disclosure of information may create significant security risks.

4.5 Secrecy and Accountability as Complementary Elements of Intelligence Governance

The findings demonstrate that secrecy remains an operational necessity in counterintelligence, but it must operate within an appropriate accountability framework. Intelligence institutions require confidentiality because disclosure of sources, methods, investigations, or vulnerabilities may compromise national security. The Nigerian Government has also recognised that certain operational security information cannot be publicly disclosed due to legitimate security considerations.

Nevertheless, secrecy does not eliminate the need for accountability. Intelligence governance scholarship emphasises that democratic systems require mechanisms capable of reviewing legality, resource utilisation, institutional performance, and compliance while protecting information that legitimately requires classification ([Knier et al., 2024](#)). Similarly, Nigerian security governance literature highlights the importance of appropriate oversight mechanisms within defence and security institutions ([Adelani & Ukwani, 2024](#)).

Therefore, the appropriate approach is not maximum disclosure but controlled accountability. Oversight institutions should have authorised access to classified information when necessary and operate through secure procedures that protect sensitive operational details. This balance allows intelligence agencies to maintain effectiveness while ensuring institutional legitimacy and public trust.

4.6 Finding Six: Public Evidence Does not Justify a Definitive Operational Judgment on NIA Counterintelligence

The findings indicate that publicly available evidence does not allow a definitive operational judgment regarding whether NIA counterintelligence activities are highly effective or ineffective. Available evidence demonstrates the statutory mandate of the NIA, its position within Nigeria intelligence architecture, and its involvement in broader national and international security engagements ([Federal, 1986](#)). These findings suggest that the assessment of intelligence effectiveness requires careful consideration of institutional capabilities rather than relying solely on visible operational outcomes. In this regard, publicly observable evidence provides important insights into the enabling environment that supports intelligence performance.

However, direct evaluation of operational counterintelligence performance requires access to classified information, including intelligence sources, methods, investigations, threat assessments, and operational outcomes. Such information is not publicly accessible and cannot be responsibly inferred from available documents. Attempting to measure effectiveness based on incomplete or unofficial information may result in inaccurate conclusions regarding intelligence capability. Therefore, research on intelligence institutions must recognise the methodological limitations created by legitimate secrecy requirements.

Therefore, this study evaluates counterintelligence effectiveness through observable institutional conditions, including legal adequacy, governance structures, coordination mechanisms, technological preparedness, and human-capital development. This approach provides a more academically responsible assessment because it avoids unsupported assumptions while recognising the legitimate secrecy requirements of intelligence institutions. By focusing on institutional foundations, the study contributes to a broader understanding of how intelligence effectiveness is enabled through legal, organisational, and technological capacities. Such an approach also allows meaningful academic analysis while respecting the operational boundaries of intelligence organisations.

5. Conclusions

The study examined the legal framework, intelligence governance, and institutional conditions influencing counterintelligence effectiveness in Nigeria, with particular attention to the National Intelligence Agency. The findings indicate that Nigeria has established a formal foundation for intelligence and information protection, while the development of cybersecurity and data-protection frameworks has expanded the approach to managing contemporary information-security challenges. The study also highlights that modern counterintelligence effectiveness extends beyond the protection of conventional classified information and increasingly requires secure information management, technological preparedness, specialised expertise, and effective institutional coordination.

The study concludes that Nigerian counterintelligence effectiveness should be understood as a multidimensional institutional capacity involving legal adequacy, governance structures, technological capability, professional human capital, inter-agency coordination, and accountable practices. Due to the classified nature of significant intelligence activities, publicly available evidence does not allow a definitive assessment of the operational success or failure of the National Intelligence Agency's counterintelligence missions. Therefore, strengthening the institutional conditions that support counterintelligence capability remains essential to improving the ability to prevent, detect, and manage emerging security threats while maintaining legitimate operational secrecy.

Acknowledgement

The authors would like to express their appreciation to the institutions, researchers, and official sources that provided publicly available documents and information supporting this study. The authors also acknowledge the contribution of previous scholarly works and policy reports that enriched the analysis of intelligence governance, cybersecurity, and counterintelligence effectiveness in Nigeria.

Conflict of Interest

The author declare that there is no conflict of interest regarding the research, authorship, or publication of this article.

References

- Adelani, S., & Ukwani, M. (2024). Governance and defence sector management in Nigeria: X-raying legislative oversight of the defence sector. *World Journal of Advanced Research and Reviews*, 23(2), 570-578. <https://doi.org/10.30574/wjarr.2024.23.2.2245>
- Anochiwa, L. (2021). A contribution to the human capital investment debate vis-à-vis economic growth: The case for Nigeria. *Annals of Human Resource Management Research*, 1(1), 15-28. <https://doi.org/10.35912/ahrmr.v1i1.364>
- Boikanyo, D. H. (2024). Utilization of 4IR Technologies to enhance strategic intelligence and dynamic capabilities for a sustainable competitive advantage. *Business Excellence and Management*, 14(1), 5-24. <https://doi.org/10.24818/beman/2024.14.1-01>
- Cascavilla, G., Tamburri, D. A., & Van Den Heuvel, W. J. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. *Computers & Security*, 105, 102258. <https://doi.org/10.1016/j.cose.2021.102258>
- David, A., Yigitcanlar, T., Li, R. Y. M., Corchado, J. M., Cheong, P. H., Mossberger, K., & Mehmood, R. (2023). Understanding local government digital technology adoption strategies: A PRISMA review. *Sustainability*, 15(12), 9645. <https://doi.org/10.3390/su15129645>

- Erhimu, K. O. (2026). Systemic Barriers and Demographic Disparities in Youth Entrepreneurship: Evidence from Nigeria. *Advances in Management and Business Studies*, 1(3), 137-154. <https://doi.org/10.35912/ambus.v1i3.4117>
- Ezeagwuna, D. (2026). Enhancing Organizational Cyber Resilience Through the NIST Cybersecurity Framework. *International Journal of Technology, Management and Humanities*, 12(01), 124-140. <https://doi.org/10.21590/>
- Farber, S. (2025). The globalization of threat: A systematic review of crime-terror convergence. *Journal of Money Laundering Control*, 28(3), 533-549. <https://doi.org/10.1108/JMLC-12-2024-0198>
- Federal Republic of Nigeria. (1962). *Official Secrets Act*.
- Federal Republic of Nigeria. (1986). *National Security Agencies Act*.
- Federal Republic of Nigeria. (2021). *National cybersecurity policy and strategy 2021*.
- Federal Republic of Nigeria. (2023). *Nigeria Data Protection Act, 2023*.
- Federal Republic of Nigeria. (2024a). *Cybercrimes (Prohibition, Prevention, etc.) Amendment Act, 2024*.
- Heriyanto, T., Alie, M. S. ., CN, Y., Desmon , D. ., Oktaria, E. T. ., Megasari , M. ., & Bakti, U. (2026). The Role of Corporate Governance and Financial Performance on Financial Distress. *Journal of Multidisciplinary Academic and Practice Studies*, 4(1), 19-39. <https://doi.org/10.35912/jomaps.v4i1.3838>
- Khan, S. H., Zakir, M. H., Tayyab, A., & Ibrahim, S. (2024). The role of international law in addressing transnational organized crime. *Journal of Asian Development Studies*, 13(01), 283-294. <https://doi.org/10.62345/jads.2024.13.1.24>
- Khan, F., & Mita, T. A. B. (2023). Cybersecure documentation and record-keeping protocols for safeguarding sensitive financial information across business operations. *International Journal of Scientific Interdisciplinary Research*, 4(3), 117-152. <https://doi.org/10.63125/cz2gwm06>
- Kniep, R., Ewert, L., León Reyes, B., Tréguer, F., McCluskey, E., & Aradau, C. (2024). Towards democratic intelligence oversight: Limits, practices, struggles. *Review of International Studies*, 50(1), 209-229. <https://doi.org/10.1017/S0260210523000013>
- Luna-Reyes, L., Juiz, C., Gutierrez-Martinez, I., & Duhamel, F. B. (2020). Exploring the relationships between dynamic capabilities and IT governance: Implications for local governments. *Transforming Government: People, Process and Policy*, 14(2), 149-169. <https://doi.org/10.1108/TG-09-2019-0092>
- Moses, L. B., & De Koker, L. (2018). Open secrets: Balancing operational secrecy and transparency in the collection and use of data by national security and law enforcement agencies. *Melbourne University Law Review*, 41(2), 530-570. <https://doi.org/10.3316/informit>
- Muchwa, S. A. (2021). Intelligence oversight systems in Uganda: Challenges and prospects. *Intelligence and National Security*, 36(2), 1-13. <https://doi.org/10.1080/02684527.2021.1888201>
- Nwosu, C. C., Obalum, D. C., & Ananti, M. O. (2024). Artificial Intelligence in Public Service and Governance in Nigeria. *Journal of Governance and Accountability Studies*, 4(2), 109-120. <https://doi.org/10.35912/jgas.v4i2.2425>
- Okoli, A. C., & Aina, F. (Eds.). (2024). Contemporary security governance in Nigeria: Themes and perspectives. *Bloomsbury Academic*.

- Olayinka, A. A. ., & Kaka, E. J. (2025). A panel regression analysis of corporate governance mechanism and financial performance of listed cement industries in Nigeria. *International Journal of Financial, Accounting, and Management*, 7(2), 245-259. <https://doi.org/10.35912/ijfam.v7i2.2812>
- Olowonihi, A. P., & Musa, M. (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. <https://doi.org/10.37547/tajiir/Volume06Issue11-08>
- Peacock, A., Bruno, R., Gisev, N., Degenhardt, L., Hall, W., Sedefov, R., ... & Griffiths, P. (2019). New psychoactive substances: Challenges for drug surveillance, control, and public health responses. *The Lancet*, 394(10209), 1668-1684. [https://doi.org/10.1016/S0140-6736\(19\)32231-7](https://doi.org/10.1016/S0140-6736(19)32231-7)
- Pomaza-Ponomarenko, A., Taraduda, D., Kravchuk, O., Moroz, S., Akhmedova, O., & Poroka, S. (2025). National Security Management: Organizational, Legal, Informational and Human Resource Dimensions. *OIDA International Journal of Sustainable Development*, 18(12), 1519-1532. <https://doi.org/10.26565/1992-2337-2023-2-06>
- Putter, D., & Dov Bachmann, S. D. (2023). Scoping the future counterintelligence focus. *International Journal of Intelligence and CounterIntelligence*, 36(2), 358-385. <https://doi.org/10.1080/08850607.2022.2091414>
- Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2021). Cybersecurity data science: An overview from machine learning perspective. *Journal of Big Data*, 8, 173. <https://doi.org/10.1186/s40537-020-00318-5>
- Ussher-Eke, D. (2025). Insider Threats: The Role of HR in Mitigating Internal Cyber Risks. *Futurity Proceedings*, (5), 70-82. <https://doi.org/10.5281/zenodo.17317577>
- Watt, E. (2017). The right to privacy and the future of mass surveillance. *The International Journal of Human Rights*, 21(7), 773-799. <https://doi.org/10.1080/13642987.2017.1298091>