Journal of Cyberspace Studies
eISSN: 2588-5502
http://jcss.ut.ac.ir
University of Tehran

Establishing a Nigerian Centralized Cybersecurity Enforcement Agency: An Evaluation of Governance and Capacity Building

Aminu Ola Rasaq[1*], Monday O. Adenomon[2], Emmanuel S. Chaku[3], Usman Ibrahim[4]

1. Centre for Cyberspace Studies, Nasarawa State University, Keffi, Nigeria. (*Corresponding author: aminurasaq@gmail.com, https://orcid.org/0009-0002-1828-012X)

Article Info

Original article

Main Object: Computer science & Technology, Cybersecurity

Received: 22 June 2025
Revised: 28 July 2025
Accepted: 29 July 2025
Published online: 04 August 2025

Keywords:
capacity expansion, cybersecurity, enforcement agency, legal reforms, Nigeria.

Abstract

Background: As Nigeria continues to experience rapid digital transformation, cybersecurity threats have become increasingly sophisticated, necessitating robust institutional frameworks for effective enforcement.
Aims: The Objective of this study is to evaluate Nigeria's current cybersecurity enforcement landscape and analyze the potential benefits of establishing a centralized enforcement agency.
Methodology: Mixed methods are used: Quantitative surveys (600 respondents) and qualitative interviews (20 experts). Data analyzed via SPSS and thematic analysis is also employed.
Findings: Key findings include gaps in coordination, low policy awareness, fragmented institutional structure, international models favor centralization.
Conclusion: Nigeria's fragmented cybersecurity governance structure hampers effective policy implementation, incident response, and capacity building. Recommendations include Legal reforms, capacity expansion, policy articulation, inter-agency coordination, international collaboration.

Cite this article: Rasaq AO, Adenomon MO, Chaku ES, Ibrahim U. (????). "Establishing a Nigerian Centralized Cybersecurity Enforcement Agency: An Evaluation of Governance and Capacity Building". *Cyberspace Studies*. ?(?): 1-11. doi: https://doi.org/10.22059/jcss.2025.397487.1173.

Website: https://jcss.ut.ac.ir/| Email: jcss@ut.ac.ir |
EISSN: 2588-5502
Publisher: University of Tehran

Cyberspace Studies, Vol ?, No ?, ????

1. Introduction

Digital transformation in Nigeria offers economic growth but increases cyber threats. The rapid digitalization of global economies has fundamentally transformed the nature of security threats, elevating cybersecurity governance to a critical national priority. In an interconnected world where digital infrastructure underpins economic growth, social development, and national security, the ability to effectively govern and protect cyberspace has become a defining characteristic of modern statehood. Cybersecurity governance encompasses the comprehensive framework of policies, laws, institutions, and strategies that guide how nations manage, coordinate, and mitigate cyber risks while fostering innovation and digital economic growth (ITU, 2023).

The global cybersecurity landscape presents a complex tapestry of challenges and opportunities, with nations at varying stages of digital maturity facing increasingly sophisticated and persistent cyber threats. Advanced economies such as the United States, the United Kingdom, Estonia, and Singapore have established themselves as leaders in cybersecurity governance, demonstrating that proactive, multi-stakeholder approaches supported by robust institutional frameworks are essential for building resilience against evolving cyber threats (*World Economic Forum*, 2024). These nations have invested significantly in developing comprehensive cybersecurity strategies that integrate legal frameworks, technical capabilities, organizational structures, and international cooperation mechanisms.

The International Telecommunication Union's Global Cybersecurity Index (GCI) provides a standardized framework for assessing national cybersecurity readiness across five pillars: legal measures, technical measures, organizational measures, capacity development, and cooperation (ITU, 2023). The 2023 GCI rankings reveal significant disparities in cybersecurity governance capabilities, with developed nations consistently outperforming developing countries across all assessment dimensions. This disparity reflects not only differences in technological infrastructure and financial resources but also variations in institutional capacity, regulatory frameworks, and strategic approaches to cybersecurity governance. Within the African context, cybersecurity governance faces unique challenges stemming from rapid digital transformation occurring alongside limited institutional capacity, resource constraints, and evolving threat landscapes. The continent's increasing digital connectivity, driven by mobile technology adoption and expanding internet infrastructure, has created new opportunities for economic growth while simultaneously exposing nations to sophisticated cyber threats (African Union Commission, 2022). African countries have begun recognizing the critical importance of cybersecurity governance, with initiatives such as the African Union's Convention on Cybersecurity and Personal Data

Protection (Malabo Convention) representing efforts to harmonize regional approaches to cyber governance.
gaps in coverage.

2. Literature review

2.1. Concept of enforcement

The concept of centralized cybersecurity enforcement represents a potential solution to many of the coordination and effectiveness challenges facing Nigeria's current governance structure. A centralized enforcement agency could provide unified oversight of cybersecurity policy implementation, coordinated incident response capabilities, centralized threat intelligence gathering and sharing, and consistent enforcement of cybersecurity standards across all sectors. Such an agency could also serve as the primary interface for international cooperation and coordination, enhancing Nigeria's ability to participate effectively in global cybersecurity initiatives.

2.2. Nigeria's regulatory landscape

Nigeria's cybersecurity governance framework is characterized by a multiplicity of agencies with overlapping roles and responsibilities, which complicates effective enforcement and coordination (Ojo & Abubakar, 2023). The primary institutions involved include the Nigerian Communications Commission (NCC), the Office of the National Security Adviser (ONSA), the National Information Technology Development Agency (NITDA), and law enforcement agencies such as the Economic and Financial Crimes Commission (EFCC).

While the presence of multiple agencies reflects Nigeria's recognition of cybersecurity as a vital national issue, this fragmented structure often results in duplication of efforts, jurisdictional conflicts, and inconsistent policy implementation (Amadi & Ekpe, 2020**).** For instance, the NCC oversees telecommunications and has a significant role in regulating digital communication, but its enforcement powers are limited without clear coordination with other agencies like NITDA, which is responsible for IT policy development and infrastructure.

Scholars argue that Nigeria's regulatory landscape suffers from a lack of a unified legal framework that consolidates cyber laws and enforcement authority under a single agency (Ojo & Abubakar, 2023). The Nigeria Data Protection Regulation (NDPR) of 2019, overseen by NITDA, is an example of sector-specific regulation, but its enforcement lacks the coherence and authority needed to effect systemic change across sectors.

2.3. International models

Globally, countries have adopted various centralized and integrated

approaches to cybersecurity governance, recognizing the importance of clear coordination, specialized agencies, and legal frameworks to protect critical infrastructure and digital assets effectively. These models serve as benchmarks for Nigeria's reform efforts.

2.3.1. United States: Cybersecurity and Infrastructure Security Agency (CISA)

The United States exemplifies a centralized model through the establishment of the Cybersecurity and Infrastructure Security Agency (CISA) under the Department of Homeland Security. CISA is tasked with safeguarding federal networks, coordinating national cybersecurity efforts, and collaborating with private sector actors to foster resilience (U.S. Department of Homeland Security, 2020). Its legal authority and dedicated resources enable swift incident response, information sharing, and strategic planning, making it a model for how structured, well-funded agencies can coordinate national cybersecurity efforts effectively (CISA, 2023).

2.3.2. United Kingdom: The National Cyber Security Centre (NCSC)

The UK operates a highly integrated centralized model via the NCSC, which provides threat intelligence, incident management, and policy advice to both government and critical industries (NCSC, 2024). The NCSC functions as an operational hub, working with intelligence agencies, law enforcement, and private sector partners under a legal mandate that confers authority and operational independence (Royal United Services Institute, 2021). This model emphasizes proactive threat mitigation and stakeholder collaboration.

2.3.3. Singapore: Cyber Security Agency (CSA)

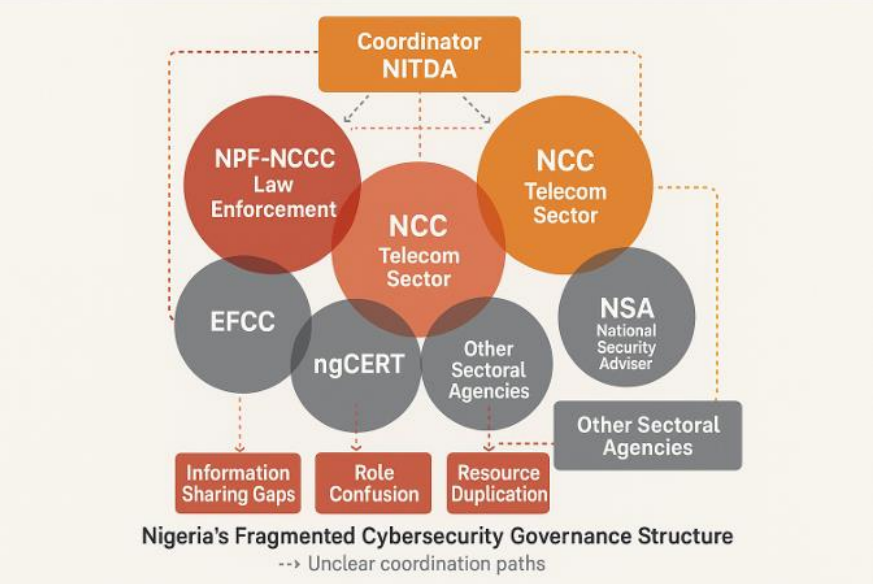
Singapore's CSA functions as a dedicated, agency-wide body overseeing national cybersecurity strategies, incident response, and capability development. Its model is characterized by a strong legal mandate, close public-private sector collaboration, and continuous capacity building, which have contributed to Singapore's reputation as a regional cybersecurity hub (Cyber Security Agency of Singapore, 2022). The agency's approach highlights the importance of embedding cybersecurity within national policy and infrastructure planning.

2.3.4. Implications for Nigeria

These international models demonstrate that effective cybersecurity governance benefits from clear legal mandates, dedicated agencies with sufficient authority and resources, and strong cooperation frameworks across sectors. Countries with centralized agencies can respond more swiftly and coherently to cyber threats, as evidenced by their structured incident response mechanisms and strategic planning.

2.4. Theoretical framework

Challenge includes fragmented governance hampering effective response and enforcement. Proposal involves establishing a centralized cybersecurity enforcement agency modeled after international best practices.



Source: Authors (Illustrate multiple agencies with overlapping roles, 2025)
Figure 1. Nigeria's current fragmented cybersecurity governance structure

This framework illustrates the current cybersecurity governance structure in Nigeria, highlighting the fragmentation and coordination challenges that characterize the existing system. The diagram shows the multiple agencies with cybersecurity responsibilities and the overlapping mandates that create coordination difficulties.

2.5. Central coordination challenges

The framework shows NITDA positioned as the primary coordinator for cybersecurity governance, but with limited authority and resources to effectively coordinate the activities of other agencies. The dotted lines indicate weak coordination relationships and unclear authority structures that limit coordination effectiveness. The positioning of agencies in overlapping circles demonstrates the problem of overlapping mandates and unclear role definitions that create confusion and inefficiency in cybersecurity governance. Multiple agencies have responsibilities for similar activities, leading to duplication of effort and gaps in coverage.

2.6. Agency-Specific roles and challenges

NPF-NCCC (Nigeria Police Force National Cybercrime Center) is

responsible for cybercrime investigation and prosecution but operates with limited coordination with other cybersecurity agencies. The agency has developed significant capabilities but faces challenges in information sharing and coordination with non-law enforcement agencies.

NCC (Nigerian Communications Commission) regulates cybersecurity in the telecommunications sector but has limited coordination with agencies responsible for other sectors. The agency has developed comprehensive cybersecurity requirements for telecommunications operators but faces challenges in coordinating with broader cybersecurity governance efforts.

CBN (Central Bank of Nigeria) regulates cybersecurity in the financial sector and has developed sophisticated cybersecurity oversight capabilities. However, the agency operates largely independently of broader cybersecurity governance coordination efforts.

EFCC (Economic and Financial Crimes Commission) investigates financial crimes including cybercrime but has limited coordination with specialized cybersecurity agencies. The agency's focus on financial crimes creates some overlap with NPF-NCCC's cybercrime mandate.

ngCERT (Nigerian Computer Emergency Response Team) provides technical incident response capabilities but has limited authority and resources for broader coordination activities. The team operates primarily as a technical service provider rather than a coordination mechanism.

NSA (National Security Adviser) has overall responsibility for national security including cybersecurity but has limited operational involvement in cybersecurity governance coordination. The office provides strategic oversight but limited operational coordination.

2.7. Coordination problems identified

The framework highlights three major coordination problems that result from the current fragmented structure:

a) **Information Sharing Gaps** occur because agencies have different information sharing policies, security requirements, and technical systems. These gaps limit the effectiveness of threat intelligence and incident response activities.

b) **Role Confusion** results from overlapping mandates and unclear authority relationships among different agencies. This confusion leads to inefficient resource allocation and gaps in cybersecurity coverage.

c) **Resource Duplication** occurs when multiple agencies develop similar capabilities or conduct similar activities without coordination. This duplication reduces the overall efficiency of

cybersecurity governance and limits the resources available for addressing.

2.8. Materials and Methods

Design mixed-methods: Quantitative surveys + Qualitative interviews

Participants: 600 respondents across government, academia, private, NGOs

2.9. Data presentation

Table 1 shows a balanced distribution of respondents across key sectors. The government sector had the highest representation at 28.17%, followed by the private sector at 25.50%, indicating their strong involvement in the study's subject, likely related to cybersecurity or data regulation. Academia/research contributed 24.50%, reflecting scholarly interest, while NGOs and development partners made up 21.83%, highlighting their role in advocacy and capacity building. This diversity of respondents enhances the study's credibility and ensures a wide range of perspectives.

Table 1. Respondents current employment sector

Response option	Frequency	Percentage
Academia/Research	147	24.50
Government	169	28.17
NGO/Development partner	131	21.83
Private sector	153	25.50

Source: Authors Field Survey Result 2025, Computed Using SPSS

Interpretation. The distribution indicates a diverse respondent base, with the government sector having the highest representation (28.17%)**,** which underscores its primary role in Nigeria's cybersecurity landscape. The substantial presence of private sector (25.50%) and academia (24.50%) suggests active engagement from industry and scholarly institutions. NGOs and development partners (21.83%) also form a significant segment, highlighting their advocacy and capacity-building contributions.

Implication. This balanced demographic boosts the credibility of the study, as it captures perspectives from key stakeholders involved in policy formulation, enforcement, technical implementation, and advocacy. It enhances the generalizability of the findings, ensuring that recommendations are informed by a wide spectrum of experiences and insights.

3. Results and Discussion

3.1. Data analysis and Results

Table 2 summarizes the professional roles of respondents in the study.

The largest group, making up 26.00%, falls under "Other (Non-technical role)", indicating diverse participation beyond core technical or executive positions. Both Executive/Senior Management and IT/Cybersecurity Staff each represent 25.67%, showing a strong presence of leadership and technical expertise in the study. Compliance/Legal Officers account for 22.67%, reflecting important input from those responsible for regulatory adherence. Overall, the data reflects a well-rounded mix of technical, managerial, legal, and general roles, ensuring comprehensive perspectives on the topic under investigation.

Table 2. Respondents role in their organization

Response option	Frequency	Percentage
Compliance/Legal officer	136	22.67
Executive/Senior management	154	25.67
IT/Cybersecurity staff	154	25.67
Other (Non-technical role)	156	26.00

Source: Authors Field Survey Result 2025, Computed Using SPSS

Interpretation. The distribution shows a well-rounded representation across different organizational levels and functions. The largest group (26%) is in 'Other' roles, indicating participation from non-technical, administrative, or support staff—these perspectives are valuable because they reflect the breadth of organizational awareness and engagement beyond technical teams. The near-equal proportions of senior management and IT/cybersecurity staff (each at 25.67%) suggest that both strategic decision-makers and specialists are actively involved in the discussion.

Implication. This diversity ensures that policy and enforcement recommendations are shaped by insights from both technical experts and organizational leaders, fostering a more comprehensive understanding of institutional readiness and challenges.

Table 3 shows the distribution of respondents based on their years of professional experience. Those with 2–5 years of experience form the largest group at 25.50%, closely followed by individuals with less than 2 years (25.17%) and those with 6–10 years (25.00%). Respondents with more than 10 years of experience make up 24.33%. The relatively even spread across all categories indicates a diverse range of experience levels among participants, ensuring that insights reflect both early-career and seasoned professionals' perspectives.

Table 3. Respondents years of experience in cybersecurity or IT governance

Response option	Frequency	Percentage
2–5 years	153	25.50
6–10 years	150	25.00
> 2 years	151	25.17
< 10 years	146	24.33

Source: Authors Field Survey Result 2025, Computed Using SPSS

Interpretation. The data indicates a relatively even distribution of experience levels among respondents, with a slight concentration in the less-than-two-years and 2–5-year brackets (~25% each). This suggests a mix of early-career, mid-career, and experienced professionals.

Implication. Having a diverse experience spectrum ensures that insights incorporate fresh perspectives from newer entrants as well as deep expertise from seasoned professionals. This multiplicity enhances the reliability of conclusions related to capacity gaps, training needs, and the maturity of Nigeria's cybersecurity landscape.

Table 4 illustrates respondents' levels of awareness of a specific subject, likely a policy or regulation. The largest group, 25.67%, indicated they are not aware at all, suggesting a significant gap in awareness. This is followed closely by 25.50% who have heard of it but are not familiar, and 24.83% who are somewhat familiar. Only 24.00% reported being very familiar. Overall, the data reveals that while awareness exists to some extent, a majority of respondents lack deep familiarity, highlighting the need for improved education, communication, or outreach efforts.

Table 4. Respondents awareness of Nigeria's national cybersecurity strategies or policies

Response option	Frequency	Percentage
Yes, very familiar	144	24.00
Somewhat familiar	149	24.83
Heard of it but not familiar	153	25.50
Not aware at all	154	25.67

Source: Authors Field Survey Result 2025, Computed Using SPSS

Interpretation. The data reveals a significant awareness gap, as over 50% of respondents either are not aware or only heard of Nigeria's cybersecurity policies. Only 24% are very familiar with the national strategies.

Implication. This low level of deep awareness indicates that current communication and dissemination efforts are insufficient. It suggests a critical need for improved outreach, education, and capacity building to ensure that stakeholders are well-informed, which is essential for effective policy enforcement and organizational compliance.

3.2. Overall insights

- Nigeria's cybersecurity governance landscape is characterized by fragmentation, with diverse stakeholder participation but low policy awareness.
- There is a need for stronger communication and training initiatives to deepen understanding of national strategies.

- The diversity in respondents' roles and experience levels enhances the robustness of the data, providing a comprehensive picture of institutional readiness, capacity gaps, and stakeholder perspectives.
- These findings underscore the importance of establishing a centralized enforcement agency that can streamline policy, improve coordination, and boost capacity across sectors.

4. Conclusion and Recommendations

4.1. Conclusion

Nigeria's fragmented cybersecurity governance structure hampers effective policy implementation, incident response, and capacity building. The collected data, stakeholder perceptions, and international best practices indicate that establishing a centralized cybersecurity enforcement agency constitutes a strategic pathway to address systemic gaps. Such an agency would serve as the cornerstone of Nigeria's broader cybersecurity architecture, fostering coordination, resource optimization, and policy clarity.

4.2. Recommendations

- **Legal and Institutional reform:** Develop legislation to establish a dedicated National Cybersecurity Enforcement Agency with clear mandates, operational independence, and enforcement authority.
- **Capacity building:** Invest in specialized training, technical infrastructure, and human resource development to enhance operational effectiveness.
- **Policy development and Communication:** Formulate a comprehensive national cybersecurity strategy and increase stakeholder awareness through targeted outreach.
- **Inter-agency coordination:** Create formal mechanisms for collaboration among existing agencies, supported by the new centralized body.
- **International collaboration:** Engage with global cybersecurity organizations and adopt best practices.
- **Monitoring and Evaluation:** Implement routine assessments of the enforcement agency's performance to ensure continuous improvement.

Conflict of interest

The authors declared no conflicts of interest.

Ethical considerations

The authors have completely considered ethical issues, including informed consent, plagiarism, data fabrication, misconduct, and/or falsification, double publication and/or redundancy, submission, etc. This article was not authored by artificial intelligence.

Data availability

The dataset generated and analyzed during the current study is available from the author on reasonable request.

Funding

This research did not receive any grant from funding agencies in the public, commercial, or non-profit sectors.

References

African Union Commission. (2022). *Digital Transformation Strategy for Africa (2020-2030)*. Addis Ababa.

Amadi & Ekpe (2020). Reforming Nigeria's cybersecurity governance: Challenges and prospects. *African Journal of Information Systems*. 12(3): 45-60.

CISA. (2023). *Strategic Plan 2023–2028*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/news/2023/07/15/cisa-strategic-plan-2023-2028.

Cyber Security Agency of Singapore. (2022). *Annual Report 2022*. CSA. https://www.csa.gov.sg/-/media/csa/documents/publication-info/annual-reports.

ITU. (2023). "Geneva: Global Cybersecurity Index". ITU Publications. https://www.itu.int/en/ITU D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

NCSC: National Cyber Security Centre. (2024). *Annual Review*. UK Government. https://www.ncsc.gov.uk/files/NCSC%20Annual%20Review%202024.pdf.

Ojo, A.I. & Abubakar, M.N. (2023). "Challenges and opportunities in Nigeria's cybersecurity governance". *African Journal of Information Systems*. 15(2): 45-68. https://doi.org/10.2298/AJIS220045AB.

Royal United Services Institute. (2021). *UK's National Cybersecurity Strategy: An Analysis*. RUSI Publications. https://rusi.org/publication/analysis/uk-national-cybersecurity-strategy.

U.S. Department of Homeland Security. (2020). *DHS's Role in Cybersecurity*. DHS Publications. https://www.dhs.gov/cisa.

World Economic Forum. (2024). "Global Cybersecurity Outlook 2024". Geneva: World Economic Forum. https://www.weforum.org/reports/global-cybersecurity outlook-2024/.