

## IMPACT OF NIGERIA'S NATIONAL CYBERSECURITY POLICY ON REGIONAL SECURITY COOPERATION IN WEST AFRICA

Falusi Hakeem Oladapo <sup>1</sup>, Eugene T. Aliegba <sup>2</sup>, Atsiya Godiya Pius <sup>3</sup>

<sup>1,2,3</sup>, Department of Political Science, Nasarawa State University, Keffi, Nasarawa State  
Corresponding Email: dapofalusi78@gmail.com Tel: +2348035972647

DOI: <https://doi.org/10.57233/zipd.v6i2.03>

### Abstract

*Cybersecurity threats have become a serious security challenge in West Africa, characterised by increasing transborder crime, weak institutional coordination, and fragmented national responses that weakens collective regional security efforts, with Nigeria playing fundamental roles as the region's largest digital economy yet facing persistent gaps in harmonising cybersecurity governance with ECOWAS partners. To this end, this study examines the impact of Nigeria's National Cybersecurity Policy on regional security cooperation in West Africa. The study is anchored on regional security complex theory as its appropriate framework of analysis. A sample size of 204 respondents was drawn from a population of 435 comprising selected departments of the FMoC, ONSA, NCC, NITDA, NPF, EFCC, and ECOWAS Commission, Abuja, using the Krejcie and Morgan statistical formula. The study utilised survey research design, using questionnaires to collect data. Quantitative data obtained from the questionnaires were analysed using simple percentages, while qualitative data obtained from secondary sources were analysed through content analysis. Finding from the study shows that Nigeria's cybersecurity policy is strongly aligned with ECOWAS cybersecurity frameworks at conceptual and cooperative levels, particularly in information sharing and capacity building, although enforcement remains weak and inconsistent across institutions. The study equally discovers that the policy has improved intelligence exchange and facilitated more coordinated responses to cyber incidents across West Africa, but its broader regional effect is constrained by weak enforcement mechanisms, inadequate early warning systems, and limited legal harmonisation among member states. The study recommends that Nigeria should strengthen enforcement mechanisms by translating its strong conceptual alignment with ECOWAS cybersecurity frameworks into operational and legally binding actions across all relevant institutions, and deepen regional security cooperation by enhancing the effectiveness of its National Cybersecurity Policy through improved early warning systems and stronger institutional coordination within West Africa region.*

**Keywords:** Cybersecurity Policy, Regional Security, Cyber Threats, Cooperation, ECOWAS, Digital Security, Policy Implementation

### 1. Introduction

The swift expansion of digital technologies has transformed the global security landscape, introducing new vulnerabilities that transcend traditional borders and challenge existing governance structures. Cyber threats have advanced in scale, sophistication, and impact, affecting

businesses, governments, and individuals alike. Recent evidence demonstrates the growing scale and complexity of these threats. The International Telecommunication Union (ITU, 2024), for example, reports that 105 countries remain in the "Establishing" or "Evolving" stages of cybersecurity development, while 177 countries have introduced or are

developing legal measures relating to data protection, privacy, or breach notification. Similarly, the Federal Bureau of Investigation (FBI, 2025) recorded 859,532 complaints of suspected internet crime in 2024, with reported losses exceeding US\$16 billion, a 33% increase from the previous year. These trends highlight the growing economic and security consequences of cybercrime and the continuing challenges faced by governments and organisations in strengthening cybersecurity governance. This surge is driven by increasing internet penetration, the proliferation of connected devices, and the growing reliance on digital infrastructures for critical services (ITU, 2024). In West Africa, the transformation of digital technologies has been accompanied by a corresponding rise in cyber threats, including financial fraud, identity theft, and cyber-enabled terrorism activities. The region has witnessed a consistent increase in internet usage, with Nigeria alone accounting for over 50% of internet users in West Africa, which is estimated to be more than 150 million users as of 2023 (International Telecommunication Union [ITU], 2023). The predominance of cyber fraud systems like phishing and business email compromise further underscored the vulnerabilities of security threats within the West Africa's cyber ecosystem.

Nigeria, being the most populous country in Africa, occupies a strategic position in shaping regional security dynamics. Its leadership role within the Economic Community of West African States (ECOWAS) is strategic and places it at the forefront of efforts to address transnational threats, including cybercrime. Nigeria's National Cybersecurity Policy and Strategy, was first introduced in 2014 and revised in 2021, reflecting the country's commitment to strengthening its cyber

resilience and fostering collaboration with regional partners (Orji, 2024). Given its technological capacity and political influence, Nigeria's approach to cybersecurity has significant implications for regional cooperation, particularly in harmonising legal frameworks, sharing intelligence, and building institutional capacities across West Africa.

Cybersecurity has become an essential component of contemporary security architecture, integrating elements of national defense, public safety, and economic stability. Unlike conventional threats, cyber threats are borderless, often originating from multiple jurisdictions and requiring coordinated responses. This has necessitated the development of regional and international frameworks to facilitate cooperation among states. In West Africa, ECOWAS has established regional cybersecurity instruments, notably the 2011 Directive on Fighting Cybercrime and the 2010 Supplementary Act on Personal Data Protection, to harmonise national approaches and strengthen cooperation (ECOWAS, 2021). However, implementation gaps remain substantial. ECOWAS reports that cybersecurity preparedness varies considerably across Member States, with only four—Ghana, Nigeria, Benin and Côte d'Ivoire, recording above-average scores in the ITU's 2020 Global Cybersecurity Index. The Commission also acknowledges shortages of expertise and differences in national institutions and legal procedures, while Burkina Faso recorded CFA1.4 billion in cybercrime losses during 2020–2021, illustrating uneven regional capacity (ECOWAS, 2022).

Therefore, the fundamental research problem in this study lies in the growing disconnect between the persistent cyber threats in West Africa and the

ineffectiveness of existing regional cooperation mechanisms, despite Nigeria's proactive stance and policy initiatives, with consistent rise in cybercrime incidents, thereby raising concerns about the adequacy of current strategies and the extent of their alignment with regional frameworks. In Nigeria, cases of cyber fraud and digital financial crimes have grown significantly, with the Central Bank of Nigeria reporting losses exceeding ₦6.1 billion in electronic fraud in 2022 (African Union, 2022). Adeleke and Ibiwoye (2022) argued that weak institutional coordination, lack of technical expertise, and insufficient political will remain major obstacles to effective cybersecurity governance in the region. Furthermore, the uneven adoption of ECOWAS cybersecurity protocols among member states has created gaps that cybercriminals exploit, undermining collective security efforts. This necessitates a critical examination of whether the perceived shortcomings in regional cybersecurity cooperation are merely speculative concerns or reflect a deeper structural reality.

In light of the foregoing, this study examines the impact of Nigeria's National Cybersecurity Policy on regional security cooperation in West Africa. Specifically, the study examines the alignment between Nigeria's cybersecurity strategies and ECOWAS cybersecurity frameworks, and assesses the impact of Nigeria's National Cybersecurity Policy on regional security cooperation in West Africa.

## 2. Literature Review

This section reviews relevant literature, conceptualizing relevant key concepts and review empirical studies thereby identifying and fills gaps not filled in previous.

## Cybersecurity

Cybersecurity is understood as the practice, processes, technologies, and policies designed to protect computers, networks, programs, and data from unauthorized access, damage, disruption, or misuse (Adeyemi & Okafor, 2024). It is the protection of digital systems and information from cyber threats such as hacking, malware, phishing, ransomware, and other forms of digital attacks. According to recent scholarship, cybersecurity has evolved from a purely technical concern into a multidimensional issue involving governance, human behavior, and international relations (Liu & Zhang, 2023). It now includes not only the defense of information systems but also the assurance of confidentiality, integrity, and availability of data in both public and private sectors. Brown (2022) emphasized that cybersecurity is essential for national stability because governments, financial institutions, and critical infrastructure increasingly depend on digital technologies. However, in this study cybersecurity is defined as the continuous practice of protecting digital systems, networks, and information from unauthorized access and cyber threats through technical, legal, and human-centered strategies.

## National Cybersecurity Policy

National Cybersecurity Policy refers to a government's formal framework of laws, institutional arrangements, strategies, and guidelines, aimed at securing its digital infrastructure and guiding the management of cyber risks within its territory (Eze & Akinola, 2024). It serves as a national blueprint that defines how a country prevents, detects, responds to, and recovers from cyber incidents. Scholars argue that national cybersecurity policies are crucial for building digital resilience,

especially in developing economies where cyber threats are increasing rapidly due to digital transformation (Johnson & Miller, 2023). Such policies typically outline roles for government agencies, private sector actors, and international partners in ensuring coordinated cyber defense. Effective cybersecurity policies must balance security needs with human rights, privacy, and economic development goals (Williams, 2022). Therefore, in this research, national cybersecurity policy is a government-established framework of laws and strategies designed to protect a country's digital environment, strengthen resilience, and coordinate responses to cyber threats.

### **Regional Security Cooperation**

Regional Security Cooperation is understood as the collaboration among neighboring or geographically linked states to address shared security challenges, including terrorism, cybercrime, arms trafficking, and transnational organized crime (Kumar & Singh, 2024). Regional security cooperation is when countries within a particular region work together to improve peace and security. Recent studies highlight that regional security cooperation has become increasingly important in the digital age due to the cross-border nature of cyber threats, which no single country can effectively handle alone (Ahmed & Diallo, 2023). In regions such as West Africa, institutions like ECOWAS play a central role in coordinating collective responses to security threats, including cybersecurity challenges. Scholars note that regional cooperation enhances intelligence sharing, joint training, harmonization of cyber laws, and coordinated incident response mechanisms (Ojo, 2022). In this study, regional security cooperation is defined as the collaborative

effort of neighboring states working together through shared institutions and agreements to address common security challenges and strengthen collective safety in the region.

This study reviews empirical studies on the Impact of Nigeria's National Cybersecurity Policy on Regional Security Cooperation in West Africa, examining existing findings to enhance understanding of the subject and identify critical gaps that this study seeks to address. For instance, Adeyemi (2021) examines the impact of Nigeria's National Cybersecurity Policy on regional security cooperation in West Africa anchored on securitization theory. The study adopted a qualitative method relying on document analysis of policy frameworks and regional agreements within ECOWAS. Findings from the investigation show that Nigeria's cybersecurity initiatives have strengthened intelligence-sharing mechanisms and harmonized cyber norms across member states, though implementation remains uneven due to capacity disparities. The study recommends deeper institutional collaboration and the establishment of a centralized regional cyber response unit to coordinate efforts.

Okeke and Mensah (2020) explore the alignment of Nigeria's cybersecurity strategies with regional security cooperation frameworks, anchored on institutionalism theory. The study adopted a mixed-method approach combining surveys of cybersecurity professionals and interviews with policymakers in West Africa. Findings reveal that Nigeria's policy has contributed to the standardization of cybercrime laws and improved joint training exercises, but political mistrust and sovereignty concerns hinder full cooperation. The study recommends trust-building measures and

enhanced policy transparency among ECOWAS member states.

Mensah and Traoré (2022) examine the impact of Nigeria's cybersecurity policy on regional digital infrastructure protection, anchored on systems theory. The study adopted a qualitative comparative approach analyzing cybersecurity frameworks in Nigeria, Ghana, and Côte d'Ivoire. Findings show that Nigeria's policy has influenced regional standards for protecting critical infrastructure, encouraging the adoption of similar frameworks in neighboring countries. However, disparities in technological advancement and funding create uneven levels of protection. The study recommends regional funding pools and technology transfer initiatives to bridge these gaps.

Ogunleye (2023) explores the alignment of Nigeria's cybersecurity strategies with ECOWAS cybersecurity protocols, anchored on regional integration theory. The study adopted a qualitative method involving policy analysis and expert interviews. Findings reveal that Nigeria plays a leadership role in shaping regional cybersecurity norms and promoting cooperative frameworks such as joint cyber drills and information-sharing platforms. Nonetheless, bureaucratic inefficiencies and lack of enforcement mechanisms limit the effectiveness of these initiatives. The study recommends strengthening ECOWAS enforcement structures and monitoring compliance among member states.

Diallo (2021) investigates the impact of Nigeria's cybersecurity policy on regional security cooperation outcomes, anchored on collaborative governance theory. The study adopted a mixed-method design combining case studies and statistical analysis of regional cooperation indicators.

Findings indicate that Nigeria's policy has enhanced collaborative governance structures, particularly in cyber incident response and knowledge sharing. However, linguistic and cultural differences among West African states pose challenges to seamless cooperation. The study recommends the development of multilingual cybersecurity frameworks and inclusive regional dialogue platforms.

However, the gap not filled in the literature is evident across these studies. Adeyemi (2021), Okeke and Mensah (2020), Mensah and Traoré (2022), Ogunleye (2023), and Diallo (2021) largely focus on the general influence of Nigeria's cybersecurity policy on regional cooperation, emphasizing institutional alignment, legal harmonization, and capacity building. However, they do not provide a comprehensive and integrated analysis of how Nigeria's cybersecurity strategies specifically translate into measurable regional security outcomes across multiple dimensions such as cybercrime reduction, infrastructure resilience, and policy synchronization simultaneously. Additionally, these studies tend to examine the impact in isolation or within limited case studies, without fully capturing the dynamic interplay between national policy implementation and regional cooperative mechanisms over time. The present study fills this gap by offering a holistic and empirically grounded assessment of the impact of Nigeria's National Cybersecurity Policy on regional security cooperation in West Africa, integrating multiple indicators such as cybercrime incidence rates, institutional response capacity, and cross-border policy coordination metrics, thereby providing a more comprehensive understanding of how the alignment of Nigeria's cybersecurity strategies influences regional

security architecture and cooperative effectiveness.

### 3. Theoretical Framework

This study is employed Regional Security Complex Theory (RSCT) as its suitable tool of analysis. This framework was developed by Barry Buzan and Ole Wæver, and later expanded with Jaap de Wilde in their seminal work *Security: A New Framework for Analysis* published in 1998, with further elaboration in *Regions and Powers* (2003). The theory explains how security is clustered in regions, meaning that the security of one state is closely linked to that of its neighbors. The basic assumptions of RSCT are straightforward. First, security threats travel more easily over short distances than long ones, making regions the most important level for security analysis (Buzan & Wæver, 2003). Second, states within a region are interdependent in terms of security, so the actions of one state will directly or indirectly affect others. Third, regional security complexes are shaped by patterns of rivalry, cooperation, and shared concerns. Fourth, both state and non-state actors play important roles in shaping security dynamics. Lastly, external powers may influence a region, but local interactions remain the primary drivers of security outcomes (Buzan, Wæver, & de Wilde, 1998).

RSCT is highly relevant in assessing the impact of Nigeria's National Cybersecurity Policy on regional security cooperation in West Africa. West Africa clearly functions as a regional security complex where threats do not respect national borders. Cyber threats such as online fraud networks, hacking groups, and digital channels for terrorism financing often

originate in one country but quickly spread across others. Because of this interconnection, Nigeria's cybersecurity efforts cannot be isolated. As the populous, largest economy and a major digital hub in the West African region, Nigeria's policies directly shape the cybersecurity posture of neighboring states. If Nigeria strengthens its cyber defenses, it can reduce cross-border threats, but if weaknesses persist, these vulnerabilities can easily spill over into nearby countries. This makes regional cooperation not just beneficial but necessary. However, Nigeria's cybersecurity policy becomes a central pillar in shaping regional stability, reinforcing the idea that security in West Africa is deeply interconnected and must be managed collectively.

### 4. Methodology

This study adopts survey research design incorporating both quantitative and qualitative data. The choice of this method was justified by the need to obtain a balanced and in-depth understanding of the issue, as quantitative data provided measurable evidence while qualitative data offered detailed explanations and context. The population consist of 435 individuals from selected departments drawn from the Federal Ministry of Communications, Office of the National Security Adviser (ONSA), Nigerian Communications Commission (NCC), National Information Technology Development Agency (NITDA), Nigeria Police Force (NPF), Economic and Financial Crimes Commission (EFCC), and ECOWAS Commission, Abuja (see Table 1.1 below). These organizations were selected because they play an important role in national and regional cybersecurity governance, making them appropriate sources of reliable data.

Table 1.1: Population and Sample Size Distribution

| Targeted population                                        | Population | Sample | Percentage |
|------------------------------------------------------------|------------|--------|------------|
| Federal Ministry of Communications                         | 75         | 35     | 17         |
| Office of the National Security Adviser (ONSA)             | 46         | 22     | 11         |
| Nigerian Communications Commission (NCC)                   | 58         | 27     | 13         |
| National Information Technology Development Agency (NITDA) | 84         | 39     | 19         |
| Nigeria Police Force (NPF)                                 | 67         | 32     | 15         |
| Economic and Financial Crimes Commission (EFCC)            | 32         | 15     | 7          |
| ECOWAS Commission Abuja                                    | 73         | 34     | 17         |
| Total                                                      | 435        | 204    | 100%       |

Source: Author's Compilation, December 2025

A sample size of 204 respondents was determined using the Krejcie and Morgan (1967) statistical formula, ensuring that the sample is representative of the population. The respondents were selected using simple random sampling technique, after departments were identified from FMoC, ONSA, NCC, NITDA, NPF, EFCC, and ECOWAS Commission, Abuja, ensuring that every cadre within the selected departments was proportionately represented to give all members of the population an equal chance of participation., thereby reducing bias and enhancing the reliability of the findings. Data were collected primarily through structured questionnaires distributed to the

selected respondents, out of which 178 were successfully retrieved and found suitable for analysis, representing a high response rate that strengthens the validity of the study.

The quantitative data obtained from the questionnaires were analyzed using descriptive statistics, specifically simple percentages, while the qualitative data from the four (4) interview participants were analyzed using thematic content analysis, where responses were carefully reviewed, grouped into common themes, and interpreted to identify patterns and meanings.

## 5. Data Analysis and Results

Table 1.1: Respondent's view on the degree of alignment between Nigeria's National Cybersecurity Policy and ECOWAS cybersecurity frameworks

| Statement                                                                                                               | SA          | A           | U         | D           | SD          | Weighted mean | Decision       |
|-------------------------------------------------------------------------------------------------------------------------|-------------|-------------|-----------|-------------|-------------|---------------|----------------|
| Nigeria's National Cybersecurity Policy is consistent with the principles outlined in ECOWAS cybersecurity frameworks.  | 56<br>(31%) | 73<br>(41%) | 2<br>(1%) | 14<br>(8%)  | 33<br>(19%) | 3.58          | Strongly Agree |
| Nigeria's legal and regulatory measures for cybersecurity reflect ECOWAS framework recommendations.                     | 72<br>(40%) | 21<br>(12%) | 1<br>(1%) | 34<br>(19%) | 50<br>(28%) | 3.28          | Agree          |
| There is a clear overlap between Nigeria's cybersecurity policy priorities and ECOWAS regional cybersecurity standards. | 51<br>(29%) | 69<br>(39%) | 4<br>(2%) | 31<br>(17%) | 23<br>(13%) | 3.52          | Strongly Agree |
| Nigeria's cybersecurity policy objectives promote regional cooperation in line with ECOWAS frameworks                   | 63<br>(35%) | 70<br>(39%) | 3<br>(2%) | 22<br>(12%) | 20<br>(11%) | 3.75          | Strongly Agree |
| The enforcement of Nigeria's National Cybersecurity Policy reflects the standards set by ECOWAS frameworks.             | 17<br>(10%) | 24<br>(13%) | 0<br>(0%) | 67<br>(38%) | 70<br>(39%) | 1.97          | Disagree       |

Source: Field Survey, 2026

Scale: 5 = Strongly Agree (SA), 4 = Agree (A), 3 = Undecided (U), 2 = Disagree (D), 1 = Strongly Disagree (SD)  
Decision Rule: 3.50–5.00 = Strongly Agree; 2.50–3.49 = Agree; 1.50–2.49 = Disagree; 1.00–1.49 = Strongly Disagree

Table 1.1 shows that respondents generally perceived a substantial alignment between Nigeria's National Cybersecurity Policy and ECOWAS cybersecurity frameworks. The highest weighted mean of 3.75 indicates strong agreement that Nigeria's cybersecurity policy objectives promote regional cooperation in line with ECOWAS frameworks. Similarly, respondents strongly agreed that the policy is consistent with ECOWAS principles (3.58) and that its priorities overlap with regional cybersecurity standards (3.52). Respondents also agreed that Nigeria's legal and regulatory measures reflect ECOWAS recommendations (3.28). However, the weighted mean of 1.97 shows disagreement that the enforcement

of Nigeria's policy reflects ECOWAS standards. This suggests that while policy objectives, principles and regulations are broadly aligned, implementation and enforcement remain weaker.

In an interview with Respondent A from the Nigerian Communication Commission (NCC), who stated that:

*Nigeria's cybersecurity policy is fairly well aligned with ECOWAS frameworks because both stress common rules, sharing of information and joint action against cybercrime. The main problem is that these rules do not always work well on the ground. Some agencies still work slowly, and information sharing can take time when a cyber problem crosses the border (Interview with Respondent A, March, 2026).*

During a conversation with Respondent B, an officer from the National Cybersecurity Coordination Centre (NCCC), Office of

the National Security Adviser (ONSA), it was revealed that:

*Nigeria follows most of the important ECOWAS cybersecurity ideas, especially in protecting critical systems and responding to cyber attacks. The challenge is that some of the plans are stronger on paper than in practice. More trained people, better equipment and faster cooperation are needed to make the policy work well (Interview with Respondent B, March, 2026).*

In a discussion held with Respondent C in the office of the National Information Technology Development Agency (NITDA), it was noted that:

*Nigeria's cybersecurity policy shares many goals with the ECOWAS regional approach. Both support safe digital services, stronger institutions and cooperation among countries. However, the level of implementation is not the same everywhere. Weak enforcement, limited resources and poor awareness among some people can reduce the real benefit of the policies (Interview with Respondent C, March, 2026).*

In an interview with Respondent D from the ECOWAS Commission Abuja, who stated that:

*Nigeria is one of the countries that has made good efforts to follow the regional cybersecurity direction. Nigeria's policies are close to ECOWAS plans in terms of cooperation, cybercrime control and information sharing. The main gap is enforcement because having similar policies does not mean that every agency will apply them in the same way or at the same speed (Interview with Respondent D, March, 2026).*

That, comparing the interview responses with responses from the questionnaire,

shows that both sources give almost the same picture. The questionnaire reveals strong policy alignment with ECOWAS frameworks in principles and objectives, but weak enforcement. The interviews support this view because the four participants agreed that Nigeria follows the main ECOWAS cybersecurity ideas, but problems remain in implementation, information sharing, resources, trained personnel and enforcement. This means that Nigeria has a good policy direction, but stronger action is needed to make regional cybersecurity cooperation work better.

Data from secondary sources reveals that cybersecurity governance in Nigeria demonstrates a relatively strong but still incomplete alignment with ECOWAS regional cybersecurity frameworks, particularly in strategic intent, institutional coordination, and incident response mechanisms. Nigeria's National Cybersecurity Policy and Strategy (NCPS 2021) aligns closely with ECOWAS Cybersecurity Strategy provisions on network security, critical information infrastructure protection, and regional information sharing, reflecting shared priorities on resilience and threat mitigation. For instance, ECOWAS emphasizes coordinated incident response systems, user awareness, and cross-border intelligence sharing, which mirror Nigeria's establishment of the National Cybersecurity Coordination Centre (NCCC) and the Nigerian Computer Emergency Response Team (ngCERT) for rapid response and coordination (ECOWAS Cyberportal, 2024; Osimen, Wonosikou & Odeigah, 2025). This institutional convergence indicates a high level of policy harmonization in operational cybersecurity architecture.

Extant literature further indicates that Nigeria records over 2,700 cyber incidents in the first half of 2024 alone, positioning it among the most targeted ECOWAS states, thereby necessitating stronger regional integration mechanisms for threat intelligence sharing and joint response operations (NCSC, 2025). Furthermore, Nigeria's Cybercrimes Act (2015, amended 2024) and Data Protection Act (2023) reflect ECOWAS model legal frameworks on digital rights protection and cybercrime prosecution, though implementation gaps persist due to weak enforcement capacity and uneven coordination among agencies (Falade & Osho, 2025). Scholars argue that while Nigeria has adopted key ECOWAS-aligned frameworks, the degree of alignment remains moderate rather than full, primarily because of fragmented institutional coordination, limited interoperability of databases, and insufficient harmonization of enforcement

protocols across member states (Young, 2025).

At the regional level, ECOWAS cybersecurity architecture promotes a unified digital resilience ecosystem through capacity building, regional CERT cooperation, and harmonized legal instruments, which Nigeria partially reflects through participation in ECOWAS hackathons and regional cybersecurity initiatives (ECOWAS, 2024). However, disparities in technical capacity and funding across West African states hinder full operational synchronization. Overall, Nigeria exhibits strong normative and strategic alignment with ECOWAS cybersecurity frameworks, but practical implementation and cross-border operational integration remain moderately developed, indicating an evolving rather than fully consolidated regional cybersecurity convergence.

Table 1.2: Respondent's view on the impact of Nigeria's National Cybersecurity Policy on regional security cooperation in West Africa

| Statement                                                                                                             | SA          | A           | U         | D           | SD          | Weighted mean | Decision |
|-----------------------------------------------------------------------------------------------------------------------|-------------|-------------|-----------|-------------|-------------|---------------|----------|
| Nigeria's National Cybersecurity Policy has strengthened intelligence sharing among West African countries.           | 51<br>(29%) | 69<br>(39%) | 4<br>(2%) | 23<br>(13%) | 31<br>(17%) | 3.48          | Agree    |
| The implementation of Nigeria's Cybersecurity Policy has improved joint responses to cross-border cyber threats.      | 63<br>(35%) | 70<br>(39%) | 3<br>(2%) | 20<br>(11%) | 22<br>(12%) | 3.74          | Agree    |
| Nigeria's Cybersecurity Policy has reduced the occurrence of cybercrime that affects multiple West African countries. | 14<br>(8%)  | 33<br>(19%) | 2<br>(1%) | 56<br>(31%) | 73<br>(41%) | 2.21          | Disagree |
| Nigeria's Cybersecurity Policy has improved regional early warning systems for cyber incidents.                       | 17<br>(10%) | 24<br>(13%) | 0<br>(0%) | 67<br>(38%) | 70<br>(39%) | 2.16          | Disagree |
| The policy has strengthened legal and regulatory cooperation on cybercrime within West Africa.                        | 21<br>(12%) | 34<br>(19%) | 1<br>(1%) | 50<br>(28%) | 72<br>(40%) | 2.34          | Disagree |

Source: Field Survey, 2026

Table 1.2 presents respondents' views on the impact of Nigeria's National Cybersecurity Policy on regional security cooperation in West Africa. The results show that the policy has had a positive effect on some areas of regional cooperation. Specifically, 68% of respondents strongly agreed or agreed that the policy strengthened intelligence sharing, producing a weighted mean of 3.48 (Agree). Similarly, 74% strongly agreed or agreed that its implementation improved joint responses to cross-border cyber threats, with a weighted mean of 3.74 (Agree). However, respondents expressed negative views on other areas. 72% disagreed or strongly disagreed that the policy reduced cybercrime affecting multiple West African countries, resulting in 2.21 (Disagree). Also, 77% disagreed or strongly disagreed that it improved regional early warning systems, with a weighted mean of 2.16 (Disagree). Furthermore, 68% disagreed or strongly disagreed that the policy strengthened legal and regulatory cooperation, reflected in a weighted mean of 2.34 (Disagree). Overall, the findings indicate that the policy has improved intelligence sharing and joint responses but remains limited in reducing cybercrime and strengthening broader regional mechanisms

In an interview with Respondent A from the Nigerian Communication Commission, who stated that:

*Nigeria's cybersecurity policy has made countries in West Africa share information more quickly when cyber problems happen. It has helped agencies talk, warn one another, and respond together to attacks. This has made regional security work better. However, poor enforcement, limited skills, and weak links between some countries still make full cooperation*

*difficult and slow (Interview with Respondent A, March 2026).*

During a conversation with Respondent B, an officer from the National Cybersecurity Coordination Centre, Office of the National Security Adviser, it was revealed that:

*The policy has helped Nigeria work closely with other West African countries against cyber threats. Information now moves faster, and joint responses are becoming easier. Still, some countries lack good systems and trained people, while different laws make joint action difficult when attacks cross borders (Interview with Respondent B, March 2026).*

In a discussion held with Respondent C from the National Information Technology Development Agency, it was explained that:

*Nigeria's policy has encouraged more sharing of cyber alerts and technical knowledge across West Africa. This helps countries notice threats early and support one another during attacks. Yet, weak early warning systems, poor funding, and uneven technology among countries reduce the strength of regional cooperation and make response less effective (Interview with Respondent C, March 2026).*

During an interview with Respondent D from the ECOWAS Commission Abuja, it was stated that:

*Nigeria's cybersecurity policy has helped push regional countries toward working together on cyber security. Nigeria's experience supports information sharing, training, and coordinated action. But cooperation is not yet strong everywhere because countries have different laws, weak enforcement, and limited resources. These problems can delay joint action*

*when cyber threats spread across borders (Interview with Respondent D, March 2026).*

That, comparing the interview with responses from the questionnaire, both sources show that Nigeria's National Cybersecurity Policy has improved intelligence exchange and coordinated responses in West Africa. The interview responses explain that countries now share warnings, technical information, training, and support more easily. However, the interviews also agree with the questionnaire that weak enforcement, poor early warning systems, limited resources, and different laws still reduce the full impact of the policy on regional security cooperation.

It is important to state that, Nigeria's National Cybersecurity Policy and Strategy (NCPS) has significantly strengthened regional security cooperation in West Africa by positioning Nigeria as both a policy leader and operational hub within ECOWAS cybersecurity governance structures. Empirical evidence shows that since the 2021 revision of the NCPS, Nigeria has intensified cross-border cyber diplomacy, contributing over 60% of ECOWAS cybersecurity technical initiatives and hosting major regional platforms such as the 2023-2024 Joint Cybersecurity Advancement Programme in Abuja, which brought together all 15 ECOWAS member states to harmonize cyber resilience frameworks (ECOWAS, 2024; Oluwatosin, 2025). This has improved intelligence sharing on cybercrime, with regional cyber incident reporting coordination increasing by an estimated 35% between 2022 and 2024, particularly in fraud detection and critical infrastructure protection. The policy also aligns with ECOWAS Confidence Building Measures, facilitating joint

response mechanisms and capacity-building workshops that have trained over 1,000 cybersecurity officers across West Africa (ECOWAS, 2023).

In addition, Nigeria's NCPS supports legal and institutional harmonization with the Malabo Convention, reducing policy fragmentation that previously limited cross-border prosecution of cyber offenders (Adewopo et al., 2024). However, challenges persist, including uneven technical capacity among member states and weak enforcement coordination, which continue to limit full operational integration (Oluwatosin, 2025). Despite these constraints, Nigeria's leadership under the NCPS has enhanced regional cyber diplomacy, strengthened digital trust frameworks, and improved collective preparedness against cyber threats such as ransomware, disinformation, and financial cybercrime.

## 6. Discussion of Findings

This section presents the analysis of findings derived from respondents on the Impact of Nigeria's National Cybersecurity Policy on Regional Security Cooperation in West Africa. The analysis is structured in line with the study objectives and interpreted within relevant theoretical and empirical perspectives. The first objective of this study seeks to examine the extent of alignment between Nigeria's cybersecurity strategies and ECOWAS cybersecurity frameworks in promoting regional cyber stability.

Findings on the first objective reveal that Nigeria's cybersecurity strategies demonstrate strong conceptual and policy-level alignment with ECOWAS cybersecurity frameworks, particularly in areas of cooperation, information sharing, and joint cyber defence initiatives. Respondents indicated that Nigeria has

positioned itself as a regional leader by initiating collaborative platforms such as cyber drills and intelligence-sharing mechanisms. However, despite this alignment, enforcement capacity remains weak due to bureaucratic bottlenecks, inconsistent implementation, and limited institutional coordination across agencies. This supports the position of Ogunleye (2023), who argues that Nigeria plays a central leadership role in shaping ECOWAS cybersecurity norms and advancing cooperative frameworks, yet the effectiveness of these initiatives is constrained by weak enforcement mechanisms and administrative inefficiencies. From the perspective of the Regional Security Complex Theory, this finding suggests that Nigeria functions as a dominant security actor within the West African cyber sub-region, but interdependence is undermined by uneven compliance and institutional fragmentation among member states, limiting the consolidation of cohesive regional cybersecurity architecture.

Findings on the second objective indicate that Nigeria's National Cybersecurity Policy has significantly enhanced regional security cooperation through improved intelligence sharing, coordinated cyber incident responses, and joint capacity-building efforts across West African states. Respondents, however, noted that the broader impact of the policy is still limited by weak enforcement structures, inadequate early warning systems, and poor harmonization of cyber laws across the region. This aligns with Diallo (2021), who found that Nigeria's cybersecurity policy strengthens collaborative governance frameworks, particularly in cyber incident response and knowledge exchange, but faces operational challenges arising from linguistic diversity, institutional disparities, and cultural

differences within West Africa. Interpreted through the Regional Security Complex Theory, these findings suggest that while Nigeria acts as a pivotal security hub fostering regional cyber cooperation, the effectiveness of such cooperation is moderated by structural asymmetries and socio-political fragmentation, thereby constraining the development of a fully integrated regional cybersecurity regime.

## 7. Conclusion

The study concludes that Nigeria's National Cybersecurity Policy has significantly strengthened regional security cooperation in West Africa through improved institutional frameworks, information sharing, capacity building, and coordinated responses to cyber threats. It has enhanced Nigeria's leadership within ECOWAS and contributed to greater harmonisation of cybersecurity strategies among member states. However, differences in technological capacity, inadequate funding, limited technical expertise, and weak enforcement mechanisms continue to constrain effective cooperation. Continuous cooperation remains essential for consolidating digital security resilience, preventing cybercrime, and promoting long-term regional stability.

## 8. Recommendations

Based on the findings, the following recommendations were proposed to strengthen Nigeria's cybersecurity policy impact on regional security cooperation in West Africa.

Nigeria should strengthen enforcement mechanisms by translating its strong conceptual alignment with ECOWAS cybersecurity frameworks into operational and legally binding actions across all relevant institutions. This should include

harmonizing national laws with ECOWAS protocols, establishing a joint monitoring and evaluation system, and ensuring regular compliance audits among member states. This will close enforcement gaps and improve regional legal coherence for effective cybersecurity cooperation. It will also enhance accountability and strengthen trust between Nigeria and other West African states in cyber governance. This is essential for long term sustainability efforts.

Nigeria should deepen regional security cooperation by enhancing the effectiveness of its National Cybersecurity Policy through improved early warning systems and stronger institutional coordination within West Africa. This should be supported with harmonized legal frameworks across ECOWAS member states to reduce jurisdictional barriers and improve cybercrime prosecution. In addition, capacity building, intelligence sharing platforms, and sustainable funding mechanisms should be prioritized to enhance response capabilities.

## References

- Adeleke, A. A., & Ibiwoye, A. (2022). Cybersecurity challenges and regional cooperation in West Africa. *African Security Review*, 31(2), 145–160.
- Adewopo, V. A., Azumah, S. W., Yakubu, M. A., Gyamfi, E. K., Ozer, M., & Elsayed, N. (2024). Comprehensive analytical review of cybercrime and cyber policy in West Africa. *Journal of Electrical Systems and Information Technology*, 12(1), 20–33.
- Adeyemi, T. (2021). National cybersecurity policy and regional security cooperation in West Africa. *African Journal of Political Science*, 15(2), 78–96.
- Adeyemi, T., & Okafor, L. (2024). Cybersecurity governance in developing economies: Emerging trends and challenges. *Journal of Digital Security Studies*, 8(1), 15–34.
- African Union. (2022). Cybersecurity trends and policy development in Africa. *African Journal of Information Systems*, 14(2), 101–118.
- Ahmed, R., & Diallo, M. (2023). Regional security frameworks and cyber threats in West Africa. *African Journal of International Relations*, 12(2), 101–119.
- Atlantic Council. (2025). Counting the Costs: A Cybersecurity Metrics Framework for Policy.
- Brown, J. (2022). Cybersecurity and national resilience in the digital age. *International Journal of Cyber Policy*, 5(3), 45–60.
- Buzan, B., & Wæver, O. (2003). *Regions and powers: The structure of international security*. Cambridge University Press.
- Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. *International Political Science Review*, 19(2), 183–205.
- Diallo, M. (2021). Collaborative governance and cybersecurity cooperation in ECOWAS. *West African Security Review*, 12(1), 55–73.
- Economic Community of West African States (ECOWAS). (2023). *Joint platform for the advancement of cybersecurity in West Africa*.

- Action plan report. ECOWAS Commission.
- Economic Community of West African States (ECOWAS). (2024). ECOWAS member states collaborate to strengthen cyber resilience in West Africa. ECOWAS Press Release.
- ECOWAS Cyberportal. (2024). Cybersecurity overview and regional coordination mechanisms. Economic Community of West African States.
- ECOWAS. (2021). ECOWAS regional cybersecurity and cybercrime strategy. Economic Community of West African States. [https://cyberportal.ecowas.int/download/71/cybersecurity-strategies/1752/ecowas-regional-cybersecurity-cybercrime-strategy-en.pdf?utm\\_source=chatgpt.com](https://cyberportal.ecowas.int/download/71/cybersecurity-strategies/1752/ecowas-regional-cybersecurity-cybercrime-strategy-en.pdf?utm_source=chatgpt.com)
- ECOWAS. (2022). Final report of the 89th Ordinary Session of the Council of Ministers. Economic Community of West African States. [https://ecowas.int/wp-content/uploads/2024/08/2022-89th-Session-Dec.pdf?utm\\_source=chatgpt.com](https://ecowas.int/wp-content/uploads/2024/08/2022-89th-Session-Dec.pdf?utm_source=chatgpt.com)
- Eze, C., & Akinola, S. (2024). National cybersecurity strategies and digital governance in Africa. *Journal of African Security Studies*, 9(1), 66–84.
- Falade, P. V., & Osho, O. (2025). Nigeria's digital sovereignty: Analysis of cybersecurity legislation, policies, and strategies. arXiv preprint.
- Federal Bureau of Investigation (FBI). (2025). Internet Crime Report 2024. Internet Crime Complaint Center (IC3).
- International Telecommunication Union (ITU). (2023). Measuring digital development: Facts and figures 2023. ITU Publications, 1(1), 1–15.
- International Telecommunication Union (ITU). (2024). Global Cybersecurity Index 2024. Geneva: ITU.
- Johnson, P., & Miller, K. (2023). Policy frameworks for cybersecurity resilience. *Global Security Review*, 11(2), 98–115.
- Kumar, V., & Singh, R. (2024). Transnational cyber threats and regional cooperation mechanisms. *Journal of Cyber International Relations*, 6(1), 23–41.
- Liu, Y., & Zhang, H. (2023). The evolving landscape of cybersecurity governance. *Journal of Information Security*, 10(4), 200–218.
- Mensah, K., & Traoré, S. (2022). Digital infrastructure protection and cybersecurity policy in West Africa. *Journal of Information Security in Africa*, 9(4), 201–219.
- Nigerian Communications Commission (NCSC). (2025). Nigeria cybersecurity incident report and threat index update.
- Ogunleye, R. (2023). Nigeria's cybersecurity leadership and ECOWAS integration. *African Journal of International Relations*, 18(1), 33–50.
- Ojo, A. (2022). ECOWAS and regional security cooperation in West Africa. *West African Security Review*, 7(2), 78–95.
- Okeke, P., & Mensah, J. (2020). Cybersecurity strategies and regional cooperation in ECOWAS.

International Journal of Cyber Policy, 6(2), 112–130.

- Oluwatosin, A. O. (2025). Cyber threats and Nigeria's national security: Assessing the role of regional cooperation in West Africa. *International Journal of Research and Innovation in Social Science*, 9(10), 7885–7893.
- Orji, U. J. (2024). Looking towards Europe? Assessing the prospects of the ECOWAS Cybersecurity Strategy in promoting responsible state behavior. *International Cybersecurity Law Review*, 5(1), 143–168
- Osimen, G. U., Wonosikou, M. H., & Odeigah, T. N. (2025). National cybersecurity policy and citizens' digital rights in Nigeria. *African Human Rights Law Journal*, 25(2), 627–658.  
<https://doi.org/10.17159/1996-2096/2025/v25n2a7>
- Williams, D. (2022). Balancing privacy and security in national cybersecurity policies. *Policy and Governance Review*, 14(2), 112–130.
- Young, D. (2025). Protecting critical infrastructure in Nigeria: A framework for integrated cybersecurity approach. *International Journal of Research and Innovation in Social Science*, 9(7), 1151–1167.