Cyber Threats and Nigeria's National Security: Assessing the Role of Regional Cooperation in West Africa

Adesuyi Ololade Oluwatosin

University of Ibadan, Nigeria

DOI: https://dx.doi.org/10.47772/IJRISS.2025.910000645

Received: 26 October 2025; Accepted: 04 November 2025; Published: 20 November 2025

This study evaluates the intersection of cyber threats, national security, and regional collaboration in West Africa, and specifically how the cybersecurity architecture in Nigeria is changing. It discusses the way the growing digitization of the Nigerian economy and government has made the country more susceptible to cybercrime, disinformation, and espionage, as these problems are now considered critical concerns related to national security. The paper is based on the theory of securitization and regional security complex framework to evaluate the policy reactions of Nigeria, institutionalization and the importance of regional collaboration within the framework of ECOWAS and Malabo Convention of the African Union. Based on content analysis of secondary data and policy documents, the study shows the presence of institutional weaknesses, lack of technical capacity, and legal harmonization as the key obstacles to effective cyber governance. Sustainable cyber resilience requires national coordination, capacity building and enhanced regional collaboration. Study findings highlight the fact that the leadership of ECOWAS in Nigeria should transition to policy supremacy to facilitate cooperation so as to establish a collective cyber defense and digital stability in West Africa.

Keywords: Cybersecurity, National Security, Regional Cooperation, West Africa

INTRODUCTION

Over the past few years, cyber threat in national security has turned out to be a two-sided sword of such a state like Nigeria (Clarke & Knake, 2010; Sule et al, 2021). The more the services, infrastructure and governance functions shift to the cyber domain, the more the country is exposed to cyber threats. What used to be solely presented as an information-technology issue is gradually being perceived as a national security issue. In the case of Nigeria, the development of cybercrime, cyber-espionage and digital disinformation are not only technical inconveniences but are reverberations in economic, political and strategic aspects. Based on the paradigm of cyber power, Nye (2010) underlines that power distribution in cyberspace complicates the state power and makes it more vulnerable. Simultaneously, as the digital infrastructure and state operations merge in Nigeria, cyber disruptions can be felt much further than the ICT departments into the very national security sectors.

The initial significant vulnerability has been the massive rise in cybercrime, cyber-espionage and digital disinformation. Nye (2010) supports this argument by saying that cyberspace presents unprecedented strength to non-state actors across all regions of the globe by lowering power disparities. On the same note, Clarke and Knake (2010) cautions that the use of cyber-weapons, espionage and state sponsored hacking has created a thin line between crime, war and national security. Empirical studies in the situation with Nigeria point at how financial crime, identity theft, malware attacks and large-scale breaches of data are currently being directed not at individual victims but at the whole system of finance, governance, and public services (Sule et al., 2021). Online disinformation campaigns also increase threats to political stability, trust and legitimacy of governance. The phenomena bring the issue of cyber threats out of the technological sphere into the national security strategy.

Strategic vulnerability is further enhanced by the rapid digitalisation of national infrastructure and governance system. The economy of Nigeria has been more dependent on the digital platform: banking and financial services, energy grids, telecommunications networks and public-sector responses are becoming more and more dependent on interconnected systems and streams of data. Cybercrime and national security studies in Nigeria

highlight that the institutional capacity is weak, there is no forensic skill and disjointed laws undermine the response to cyber-attacks (Yusuf, 2014; Okoru & Oluku, 2023). To illustrate, studies on cyber-risk coordination in Nigeria have shown that, although the country has formally instituted a national Computer Emergency Response Team (CERT) and Sectoral Computer Security Incident Response Teams (CSIRTs), the coordination between agencies is still poor (Ikuero, 2022). Moreover, the wider scholarly body on the topic of development and cybercrime demonstrates that cybercrime decreases investor confidence, harms national image, and cripples sustainable development (Atalor and Fakunle, 2023). Collectively, these results indicate that the digital transformation in Nigeria should be accompanied by equally important resilience efforts in case the cyber threats are to be addressed as the issues of national-security.

The policy significance of cyber threats to the internal and regional stability of Nigeria cannot be overestimated. At the internal level, an effective cyber-attack on financial infrastructure or government services may undermine the level of trust, create governance crises and deteriorate state capacity. Nigeria being a key player in the West African region and a pillar to regional security, its cyber vulnerability has spill over effects to neighbouring states and the overall regional security complex. Those scholars who have used the securitisation theory have pointed out that by presenting a phenomenon as a security concern, states are able to mobilise resources, legitimise extraordinary actions and coordinate institutional responses (Buzan, Waever and de Wilde, 1998). The change in perception of cyber-threats as an ICT problem to a national security problem is necessary in the Nigerian context in mobilising the correct policy and institutional frameworks (Tella, 2022). In the meantime, studies about the place played by Nigeria in fighting against transnational digital threats emphasize the value of legal frameworks and regional collaboration in West Africa (Jude, 2024). With this kind of framework, policymakers in Nigeria and the region would be in a better position to place cyber threat in broader frameworks of stability, state sovereignty and collective governance.

Conceptual and Theoretical Framework

The fast-changing digital space has significantly broadened the boundaries of security cognition, which has led to the necessity to frame how the problem of cybersecurity, national security, regional security complex, and digital sovereignty converge within regional frames of governance and technological sovereignty. The core of this exploration is made of three related ideas, namely, **cybersecurity** as the defense of information systems, networks and data against malicious digital intrusions; **national security** as a broader construct to encompass the political autonomy and territorial integrity of a state and the critical infrastructure; and **regional security** complex as the idea that security relations occur in the most intense form at the regional level with inter-dependencies clustering around the states. Digital sovereignty is thus the desire of states and regional blocs to dominate their digital environments, data streams, and infrastructure and regimes. The combination of these ideas allows a more in-depth discussion of how states and regional entities of the West African location pursue attempts to cope with cyber-threats, secure national interests and regional coordination.

The theory of securitization as represented by Barry Buzan, Ole Waever and Jaap de Wilde (1998) provides a rich platform on which cyber operations can be interpreted as being advanced to the level of technical or policy problems to that of security imperative that require extraordinary solutions. Securitization theory underlines that security is not the objective state of affairs but a socio-constructed activity where an issue is put in terms of a speech act as an existential threat to a specified referent object usually the state, society or identity (Buzan et al., 1998; Waefer, 1995). Within the cyberspace, researchers have demonstrated that states are growing to describe cyber-attacks on critical infrastructure, data network or digital sovereignty as similar to conventional threats of war or espionage, warranting increased efforts, extraordinary expenditure or constraining regulatory frameworks. This can be applied to a West African or African regional context and it is in this context that governments are connected to cybersecurity in terms of it being a survival of the nation, social cohesion and security of the digital economy, thus justifying a stronger state action (Gaidaev, 2020). In this framing, in reference to the regional security complex concept, the argument is presented that the perception of threat and response to it is not limited within the borders of the individual state: the security of one state is closely interwoven with its neighbours through shared cyberspace realities, data-flows, cross-border incidents and infrastructural dependencies (Buzan et al., 1998).

In opposition to the theory of securitization, a collective security approach offers a normative and institutional means of how regional actors seek to structure collective actions to cyber-threats and digital governance issues. In collective security, states assume the responsibility of collaborating to maintain peace and security to all members of the group by usually restricting the sovereign action of the state to intervene when a state is threatened or attacked. This is reflected in infrastructures and systems that are aimed at sharing capacities, aligning regulatory regimes, sharing cyber-intelligence and establishing common resilience in the framework of regional institutions like the African Union (AU) and Economic Community of West African States (ECOWAS). A case in point is the Malabo Convention, which is a supra-national legal tool that seeks to tackle cybercrime, data protection and digital sovereignty in Africa, developed by the AU (Bouke et al., 2023; AU, 2014). On the same note, ECOWAS has held high-level cyber-diplomacy briefings to facilitate resilience and online collaboration at the regional level (ECOWAS, 2025). With a collective security prism, analysts can see how regional networked system and data infrastructure inter-dependence builds perceptions of threats and how states are sucked into cooperative (or even competitive) relationships of digital sovereignty.

Therefore, by basing the analysis on the theory of securitization and concept of collective security, one may infer the way in which states and regional organizations are defining cybersecurity not as a technical field, but as an essential aspect of national and regional survival, sovereignty and stability. Cyber-threats are approximated as existential incentive mobilisation, regulatory transformation and institutional innovation; and regional institutions are utilized in order to overcome the transnationality of cyber-risks and in the encouragement of digital sovereignty with the help of collective governance. These theoretical prisms point to the potential and the challenge of applying cybersecurity (as national security), regional security complex dynamics, and digital sovereignty to a consistent policy framework that responds to the challenges of the 21 st century in the context of African reality.

Cyber Threat Landscape in Nigeria

The cyber threat environment in Nigeria is marked by an abundance of financially-driven intrusions especially investment fraud, business email compromise (BEC), phishing and ransomware as well as the increasing politically-driven disinformation efforts. In the report of Cyber Security Experts Association of Nigeria (CSEAN) 2023, it is stated that billions of nairas are being lost annually by Nigerian organisations to cyberattacks and the issue is not heavily regulated due to the fact that many players are interested in regulatory compliance, but not in actual security architecture enhancements (Odumesi, 2023). Moreover, the trends indicate that phishing and social-engineering-based fraud continue to be some of the most widespread vectors, particularly in the SMEs and public-sector organisations (CSEAN, 2023). These reports highlight that threat actors are taking advantage of poor email hygiene, inadequate use of multi-factor authentication and older systems in both public and private networks, and large scale ransomware attacks are disproportionately affecting healthcare, financial services and critical-service providers and increasing operation disruption and recovery expenses (Odumesi, 2023).

The main characteristic of the cyber-crime ecosystem in Nigeria is the organised locally-based communities popularly known as the Yahoo Boys whose operations extend to advance-fee fraud and more sophisticated. The social and organisational forms of these organizations are described with references to the apprenticeship models and specialised divisions (e.g., social-engineering teams, money-movement specialists) (Orji, 2023). Although most of the operations continue to be transnational in influence (victims are usually abroad), domestic weaknesses like lack of investment in cyber policing, lack of digital forensic capacity, and absence of inter-agency coordination provide enabling conditions that not only protect but also expand these criminal networks (Saidu, Suleiman & Akpan, 2021). These two factors of high demand, low domestic defence and international opportunity make Nigeria a good area to fight over by malicious actors.

The economic and reputational impact of cybercrime on Nigerian economy and institutions is not trivial: empirical evidence suggests that cyber-incidents lead to direct financial losses, loss of investor confidence and increase in the costs of operations to enterprises that need to harden systems and insure them against attacks (Saidu et al., 2021). Macro-level effects of these dynamics are loss of digital trust that limits potential GDP contributions of a digital economy that is otherwise booming; institutional-level, the lack of threat-intelligence sharing and more protracted incident-response increases recovery and recovery costs of organisations under

attack (Odumesi, 2023). A combination of these causes a scenario where organised fraud syndicates and external malicious actors have asymmetric advantages over defenders of both the public and the private sector.

Nigeria's National Cybersecurity Architecture

The National Cybersecurity Policy and Strategy (NCPS) 2021 forms the basis of the national cybersecurity architecture in Nigeria and is aimed at establishing a secure and resilient cyberspace by enhancing governance, safeguarding critical information systems, and developing a coordinated institutional capacity (NCP Report, 2021). The policy states that; "Nigeria will develop and sustain a general governance framework on cybersecurity, define the roles and responsibilities between government agencies and formulate a consistent strategic framework. The document identifies partnerships with the industry and the multi-stakeholder approach, as well as global collaboration, as the key building blocks of national cyber defence (NCP Report, 2021; Diplo Report, 2022)". Essentially, the NCPS 2021 is an effort to institutionalize the changing nature of Nigeria towards the concept of securing cyberspace by providing a framework of how institutions should be coordinated, manage risks, and reduce threats under the umbrella of a single policy.

Table 1.1 Ranking of focus countries in the Global Cybersecurity Index and National Cybersecurity Index.

Country	Global Cybersecurity Index (2020) Score (rank)	National Cyber Security Index (October 2022) Score (rank)
Côte d'Ivoire	67.82 (75)	31.17 (97)
Ghana	86.69 (43)	31.17 (98)
Kenya	81.7 (51)	41.56 (80)
Namibia	11.47 (155)	15.58 (131)
Nigeria	84.76 (47)	54.55 (61)
Rwanda	79.95 (57)	33.77 (92)
Senegal	35.85 (100)	19.48 (121)
South Africa	78.46 (59)	36.36 (89)

Source: Diplo Report, 2021

The table is the comparison of the African countries of interest in terms of cybersecurity performance according to the Global Cybersecurity Index (GCI) 2020 and the National Cyber Security Index (NCSI) 2022. In GPI scores, Ghana (86.69, rank 43) and Nigeria (84.76, rank 47) are the leaders as they have more effective institutional structures and preparedness. Nevertheless, Nigeria is still the top ranked on the NCSI (54.55, rank 61), with better real-time capacity. Namibia (11.47, position 155) and Senegal (35.85, position 100) are not doing well in both indicators, indicating poor infrastructure and policies. Altogether, the differences between GCI and NCSI indicate that the implementation of cybersecurity in comparison with the policy development in African states is different.

Under this structure, such important institutions as the Office of the National Security Adviser (ONSA), the National Information Technology Development Agency (NITDA) and the Economic and Financial Crimes Commission (EFCC) have significant and overlapping roles. Under the ONSA, the NCPS 2021 puts the coordination of incident-response, cyber intelligence and national-level threat awareness (Federal Republic of Nigeria, 2021). In the meantime, NITDA will be involved with the promotion of the digital economy infrastructure, establishing standards regarding the ICT security and aiding with the capacity-building (NIGERIAN Journals Online, 2024). Although the EFCC is more of an anti-fraud and financial-crime agency, it has also become more active in prosecuting cyber-crime offences and contributing to enforcement of the wider cybersecurity agenda (Adisa, 2023; Awhefeada and Ogechi, 2020). Regardless of the delineation of roles, studies have indicated that multi agencies contributions have led to the development of jurisdiction

overlaps, coordination challenges and uneven adoption of policy across sectors (Rasaq, 2025; Idowu and Madaki, 2021).

I argue that the architecture however has serious capacity gaps and implementation issues. Research shows that despite the formal frameworks and strategies, practitioners and stakeholder awareness is low: less than a quarter of surveyed professionals stated that they were very familiar with national cybersecurity strategies, which shows that there are severe gaps in dissemination and training (Rasaq, 2025). Other literature identifies human-resource deficits (skills, expertise), insufficient funding, ineffective infrastructure and poor enforcement systems as the primary barriers (Carver, 2024; UNESCO, 2025). As an illustration, in investigations into cyber-crime control in Nigeria, researchers note that the lack of institutional capacity, inadequately equipped law-enforcement bodies and ineffective legal frameworks are a great impediment to the effective response to cyber threats (Idowu & Madaki, 2021; Awhefeada and Ogechi, 2020). Moreover, a significant portion of organizations in the private sector have been limited in their ability to embrace the best practices of cybersecurity amid the increased threat (Abdulmalik, 2025).

Collectively, the NCPS 2021 and institutional framework are indicators of awareness on the strategic significance of cybersecurity in Nigeria, and a positive move towards a consistent national cyber-defence stance. However, the performance of this architecture is still hindered by the lack of coherent coordination, redundancy of institutional mandate and lack of pervasiveness in capacity. The system must also be backed by long-term investment in awareness, training, sector-wide coordination and enforcement capacity to realise its potential as highlighted by recent studies on the governance of cybersecurity in Nigeria (Carver, 2024; Rasaq, 2025).

Regional Cooperation and Collective Cybersecurity Efforts in West Africa

The West African countries have now realized that within the transnational international system, cyber threats are more likely to cross national borders and require regional efforts and unified actions. In 2011, the Economic Community of West African States (ECOWAS) made a timely move by adopting the Directive C/DIR.1/08/11 on Fighting Cybercrime obligating the member states to criminalise certain online offences as well as establishing structures on legal cooperation and technological co-operation (ECOWAS, 2011). On the continental level, the Convention on Cyber Security and Personal Data Protection otherwise referred to as the Malabo Convention was created by the African Union (AU) in 2014. This treaty has a detailed legal framework that interconnects cybercrime prevention, data protection, and e-commerce regulation in the unified governing framework (African Union, 2014). Adewopo et al. (2025) note that both tools show how Africa tries to institutionalize the governance of cybersecurity by legal harmonization and multilateral interaction, which are needed to have an impact on curbing the digital vulnerabilities in a region where internet use is rapidly increasing yet the institutions are poorly positioned to support these regulations.

These legal structures have been supplemented by the operational networks. An example is that the West and Central African Research and Education Network (WACREN) has integrated cybersecurity awareness and incident-response training in its research and academic curricula, which enhances digital resilience in universities and research centers who host many critical infrastructures (Adewopo et al., 2025). Equally, AFRIPOL or African Police Cooperation Organization enables member-state law enforcement agencies to coordinate performances in the attempt to stop transnational crimes, including cyber-enabled crimes (Ijaiya, 2024). These efforts are further translated into national and subregional Computer Emergency Response Teams (CERT) that act as technical nodes in the detection and response of cyber incidents. As Mohamed and Kamau (2023) note, such CERTs, even in their new form, are very crucial in regional threat intelligence sharing and early-warning systems that would allow a quicker response to inter-country cyber-attacks.

Nevertheless, such structures notwithstanding, the efficiency of regional cybersecurity collaboration is still limited by the issues of coordination and capacity. Research has indicated the presence of long-standing policy gap, maladaptive home legislation, and institutional implementation fracturedness (Ijaiya, 2024; Adewopo et al., 2025). The 2011 Directive is yet to be domesticated into national law in most ECOWAS states and therefore there is inconsistent application and less legal interoperability (Adewopo et al., 2025). Furthermore, there is usually an issue with the sovereignty sensitivities that hinder the intelligence sharing between the states

that fear letting sensitive information or the vulnerabilities of their operations be revealed (Bouke et al., 2023). This is reinforced by the statistics released by INTERPOL on the regional crime in 2025 that indicated over 30 percent of reported crimes in West and East Africa were cybercrime, and 86 percent of countries cited poor international cooperation and technical capacity as limiting effective implementation (Nairametrics Report, 2025). This is how a divide exists between policy making and real implementation a divide that is enhanced by sparse funding, skewed technological coverage and disparate national interests.

To a more optimistic extent, joint training sessions and building digital forensics capabilities become a ray of light in the cybersecurity situation in West Africa. With the help of the ECOWAS European Union OCWAR-C project, there was the creation of a digital forensic lab in The Gambia to enhance technical investigative capacity and promote cooperation at the regional level (ECOWAS, 2025). Other member states have also launched similar capacity-building programs, where hands-on training, simulation exercises and standard forensic methods are important factors (Adewopo et al., 2025).

These efforts have enhanced the competence of the practitioners and enlarged the admissibility of digital evidence in courts, which is essential in prosecuting cybercriminals. However, despite this, as Mohamed and Kamau (2023) observe, there is the issue of sustainability because of the financial constraints and a shortage of accreditation criteria of digital forensic specialists in the area. Such gains may be short lived unless there is a consistent investment and policy follow up.

The cybersecurity regional architecture in West Africa is ambitious but poorly implemented. ECOWAS Directive and the AU Malabo Convention have established a critical legal and normative basis of cooperation, whereas the operational platforms in the form of WACREN, AFRIPOL and national CERTs have enabled slow but steady capacity building and coordination. Nevertheless, as Adewopo et al. (2025) and Bouke et al. (2023) note, the lack of coordination, the sensitivity of sovereignty, and the lack of resources still hinder the comprehensive implementation of collective cyber defense. The experience of West Africa proves that legal and institutional advancement is visible, but cyber threats are changing more rapidly than the policy changes. As a result, the process of building resilient regional cybersecurity posture requires continuous cooperation, legal harmonization, and the further enhancement of trust between states in terms of sharing intelligence and resources.

Empirical Assessment: Challenges and Opportunities for Nigeria in Regional Cooperation

The economic and population density of Nigeria in West Africa still characterizes its primary position and the obstacles it experiences in collaborating with others regionally. Nigeria is the largest economy and most populous country in the region and thus has a great influence in Economic Community of West African States (ECOWAS) but this dominance has its restrictions to integration in the region. Indicatively, researchers find that institutional poorly endowed giant economies are likely to generate intra-regional trade performance that is less than the expectations in the existence of structural imbalances (Gammadigbe, 2021). The hegemony of the ECOWAS by Nigeria has been examined, and the authors observe that the hegemony faces domestic governance, economic inequalities and policy inconsistencies as major challenges to its ability to spearhead integration in an effective way (Moses, 2024). These institutional and structural characteristics imply that the market size of Nigeria presents a regional opportunity to develop its value-chain, but its poor diversification of the economy and poor infrastructure limits its capacity to enable sustainable intra-ECOWAS trade flows.

Another level of difficulty in the regional engagements in Nigeria is institutional preparedness and allotment of resources. Empirical studies of West Africa demonstrate that the quality of institutions is a major predictor of intra-regional trade: the stronger the institutions, the more they trade with their neighbours and the weaker the institutions, the weaker the services such as the poor quality of public services, border procedures and corruption which deter trade integration (Gammadigbe, 2021). With regards to the example of Nigeria, the results of the hegemonic role analysis suggest a lower ability of this country to operationalize regional agreements due to its internal institutional restrictions such as bureaucratic fragmentation, lack of inter-agency coordination and under-resourced regional implementation (Moses, 2024; Ameh et al, 2025). Moreover, the skewed distribution of resources to the regional infrastructure and multilateral programmes dilute leadership of

common good by Nigeria hence inhibiting the multiplier impact of its economic dimension to the larger region.

Policy convergence in ECOWAS is still the foundation of joint development, whereas the domestic policy situation in Nigeria tends to be dissimilar to regional standards. The study of the Nigerian foreign policy in West Africa has been focused on two aspects of its participation in the security and regional politics yet less in the economic and institutional aspects of integration (Ogele, 2025). In a broader sense, the literature on regional integration in West Africa highlights institutional harmonisation, convergence of trade policies and regulatory convergence as the major prerequisites of increased cooperation but none are perfect throughout the sub-region (Aryeetey, 2001; Gammadigbe, 2021). In the case of Nigeria, the realignment of such areas as customs regulation, facilitation of digital trade and regulation of sectoral infrastructure is a quantifiable chance to develop further integration on the condition of domestic reforms. Finally, the perspective of regional cooperation in Nigeria is a two-sided situation: the size and power of the nation make it irreplaceable to the success of ECOWAS, but internal governance, inconsistency of institutions, and policy remain as the obstacles to its success.

CONCLUSION

This study has revealed that the cybersecurity situation of Nigeria is closely connected to the general national security and stability issues in the region. As the economic and the governance systems of the country are becoming more digitized, the complexity of the cyber threats of organized criminal networks to politically motivated disinformation is multidimensional challenges to the sovereignty, critical infrastructure, and trust of the population. The National Cybersecurity Policy and Strategy (NCPS, 2021) has a well-organized plan of action, which is to be followed upon the response, but the lack of institutional cohesion, lack of capacity, and poor enforcement mechanisms remain the obstacles to its efficiency. The research discovered that the vulnerabilities of cybersecurity in Nigeria are not unique and singular but a subset of a wider regional security complex in West Africa whereby cyber risks are transnational.

Applying the securitization theory, the study revealed that the policy recognition but not yet adequate operational coordination of cyber threats in Nigeria has been made possible through the reframing of cyber threats as existential national security problems. In the meantime, collective security model highlights the need of regional synergy within the ECOWAS and the AU systems like Malabo Convention. Yet, the difference between policy formulation and effective application is still significant, with the lack of effective intelligence-sharing regimes, sovereignty-related sensitivities, and the absence of institutional capacity expanding the range of cyber vulnerability in the region. Therefore, Nigeria has the highest indicators of regional digital readiness, but it continues to have difficulties transforming this leadership into regionally integrated cybersecurity governance.

Policy Recommendations

I recommend that Nigeria needs to focus on institutional coherence, capacity-building, and multilateral trust-building in order to be able to reinforce its national and regional cybersecurity posture. To begin with, achieving a balance between overlapping institutional mandates between the Office of the National Security Adviser (ONSA), NITDA, and EFCC would facilitate operational efficiency and responsibility clarity. Second, the long-term human-resource capacity building in specialized training, cybersecurity training, and technical cooperation will help fill gaps in existing skills as suggested by Carver (2024) and UNESCO (2025).

Third, Nigeria needs to more thoroughly integrate its Computer Emergency Response Team (CERT) with ECOWAS and AFRIPOL models to improve coordination of cross-border threat intelligence and incident response. Furthermore, Nigeria should lead coordination of legislation harmonization between the states in the ECOWAS region so that the 2011 Cybercrime Directive and the Malabo Convention can be domesticated and legal interoperability can be achieved in prosecution and sharing of evidence. Enhanced public-private collaboration would also capitalize on local innovation and commercial infrastructure in safeguarding critical infrastructure, as well as, integrating cybersecurity into digital transformation and sustainable development agendas would help to create resilience beyond compliance. Lastly, the leadership of Nigeria in the ECOWAS

must be transformed into a form of facilitation that creates trust and technical solidarity between the member states through the common laboratory, simulation drills, and pooling of resources. It is only in the context of these coherent domestic changes and a real regional cooperation that Nigeria can turn its cyber policy frameworks into effective security architecture that can both ensure the national interests and make a valuable contribution to the overall cyber resiliency in West Africa.

REFERENCES

1. Abdulmalik, A. (2025). Bridging the cybersecurity gap in Nigerian SMEs: Awareness and protective measures. IJCSMT, 11(5), 93-101.
2. Adewopo, V. A., Azumah, S. W., Yakubu, M. A., Gyamfi, E. K., Ozer, M., & Elsayed, N. (2025). Comprehensive analytical review of cybercrime and cyber policy in West Africa. Journal of Electrical Systems and Information Technology, 12(1), 20–33.
3. Adisa, O. T. (2023). The impact of cybercrime and cybersecurity on Nigeria's economy. In Adisa, O. T. (Ed.), The impact of cybercrime and cybersecurity on national economies (pp. …). Czech University Press.
4. African Union. (2014). Convention on Cyber Security and Personal Data Protection (Malabo Convention). Addis Ababa: African Union Commission.
5. Ameh, M., Kolawole, J. S., Adesuyi, O. O. (2025). United Nations Security Council Resolutions 2349 and 2391 and Counter Terrorism in the Lake Chad Basin and Sahel Region. American Journal of Operations Management and Information Systems, 10(2), 42-54. https://doi.org/10.11648/j.ajomis.20251002.12
6. Aryeetey, E. (2001). Regional Integration in West Africa. OECD Development Centre Working Papers, No. 170. OECD Publishing. https://doi.org/10.1787/751603543122
7. Atalor, S., & Fakunle, O. S. (2023). Effects of cybercrime on national development: A literature review. Management Analytics and Social Insights. https://doi.org/10.22105/masi.v2i2.68 masi.reapress.com
8. AU. (2014). African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention). Retrieved from AU documents.
9. Awhefeada, U. V. & Ogechi, B. (2020). Appraising the laws governing the control of cybercrime in Nigeria. Journal of Law and Criminal Justice, 8(1), 30-49.
10. Bouke, M. A., Abdullah, A., Alshatebi, S. H., El Atigh, H., & Cengiz, K. (2023). African Union Convention on Cyber Security and Personal Data Protection: Challenges and Future Directions. arXiv.
11. Buzan, B., Wæver, O., & de Wilde, J. (1998). Security: A New Framework of Analysis. Lynne Rienner Publishers.
12. Carver, J. (2024). Capacity-building assistance and strategic competition in cybersecurity: Addressing capacity gaps in emerging economies. SSRN Electronic Journal.
13. Clarke, R. A., & Knake, R. K. (2010). Cyber War: The Next Threat to National Security and What to Do About It. Ecco.
14. Diplo Report. (2022). National cybersecurity and cybercrime policies in Africa: Nigeria's approach. Diplomacy.edu.
15. Economic Community of West African States (ECOWAS). (2011). Directive C/DIR.1/08/11 on Fighting Cyber Crime within ECOWAS. Abuja: ECOWAS Commission.
16. Economic Community of West African States (ECOWAS). (2025). Fight against Cybercrime in West Africa: ECOWAS and the European Union Provide a Digital Laboratory to The Gambia. Abuja: ECOWAS Directorate of Digital Economy.
17. ECOWAS Report . (2025, May 21). ECOWAS convenes high-level briefing on cyber diplomacy to advance regional resilience and digital cooperation. Retrieved from ECOWAS website.
18. Gaidaev, A. (2020). Securitization Theory or a Well Overlooked Old: On the Philosophical and Theoretical Premises and Origins of the Theory. Vestnik RUDN. International Relations.
19. Gammadigbe, V. (2021). Trade Integration in West Africa: Does the Quality of Institutions Matter? Journal of African Trade, 8 (1), 65-81. https://doi.org/10.2991/jat.k.211201.001
20. Idowu, O. O. & Madaki, M. (2021). Cybercrimes and challenges of cyber-security in Nigeria. ResearchGate.

21. Ijaiya, T. (2024). Combatting Cybercrime in West Africa: Assessing the Role of ECOWAS as a Capable Guardian. Governance and Society Review, 3(2), 55–70.
22. Ikuero, F. E. (2022). Preliminary review of cybersecurity coordination in Nigeria. Nigerian Journal of Technology, 41(3), 521-526. Nijotech
23. Jude, O. (2024). Cybersecurity and Nigeria's role in combating transnational digital threats. Irish International Journal of Law, Political Sciences and Administration. https://doi.org/10.5281/zenodo.17296358 aspjournals.org
24. K. Orji. (2023). Understanding the Crime-grid of the Nigerian Yahoo Boys. National Journal of Cyber Security Law. https://doi.org/10.37591/njcsl.v7i2.1651
25. Mohamed, A. Y., & Kamau, S. K. (2023). A Continent-wide Assessment of Cyber Vulnerability Across Africa. arXiv preprint arXiv:2301.03008.
26. Moses, T. S. (2024). The role of Nigeria in the regional integration process in West Africa (1975-2023): Case study of ECOWAS. International Journal of Science & Technology Research Archive, 7 (2), 001-014. https://doi.org/10.53771/ijstra.2024.7.2.0059
27. Nairametrics. (2025, June 27). Cybercrime accounts for more than 30% of all reported crimes in Western and Eastern Africa – INTERPOL. Lagos: Nairametrics Research.
28. NCP Report. (2021). National Cybersecurity Policy and Strategy (NCPS 2021). Nigeria Computer Emergency Response Team (ngCERT).
29. Nye, J. (2010). Cyber Power. Belfer Center for Science and International Affairs, Harvard Kennedy School.
30. Odumesi, J. (2023). National Cyber Threat Forecast 2023. Cyber Security Experts Association of Nigeria. Retrieved from https://csean.org.ng/technical-reports
31. Ogele, E. P. (2025). The Hegemon's Role: Nigeria's Foreign Policy and Its Impact on West African Regional Security and Cooperation. International Journal of Pedagogy of Social Studies, 10 (1), 43-56.
32. Okoru, A. O., & Oluku, O. (2023). Cybercrime, crime security and national development in Nigeria. FUOYE Journal of Criminology and Security Studies. fjcss.fuoye.edu.ng
33. Rasaq, A. O. (2025). Establishing a Nigerian centralized cybersecurity enforcement agency. Cyberspace Studies.
34. Saidu, I. R., Suleiman, T., & Akpan, U. E. (2021). The challenges of security threat in Nigeria cyberspace. FUDMA Journal of Sciences. https://doi.org/10.33003/fjs-2021-0501-554
35. Tella, O. (2022). Cybersecurity and Nigeria's national security: Challenges and policy options. African Security Review, 31(3), 215–233.
36. UNESCO. (2025). Advancing Nigeria's digital transformation: Human-resource capacity gaps in AI, data and cybersecurity. UNESCO.
37. Yusuf, I. B. (2014). Cyber threats and national security in Nigeria: Challenges and options. NDC E-Journal, 13(2), 131-146. ndcjournal.ndc.gov.bd