

CYBERSECURITY GOVERNANCE AND THE PROTECTION OF CRITICAL DATA INFRASTRUCTURE IN NIGERIA: A POLICY ANALYSIS OF INSTITUTIONAL CAPACITY AND REGIONAL HARMONIZATION

M Umar ¹, Aliyu Tanko ², Mahmud Umar ³

¹ Department of Computer Science, Ibrahim Badamasi Babangida University, Lapai

² Department of Political Science, Ibrahim Badamasi Babangida University, Lapai

³ Department of Political Science, Ibrahim Badamasi Babangida University, Lapai

Correspondence concerning this article should be addressed to UMAR, Maikudi

Email: umaikudi@ibbu.edu.ng, Phone: +2347065491461

DOI: <https://doi.org/10.57233/zjpd.v6i2.13>

Abstract

Nigeria's digital economy has expanded faster than the regulatory apparatus built to secure it. This study examines how Nigeria's legal-institutional architecture for cyber-security coordinates across agencies, aligns with regional and continental instruments, and compares with peer states in West Africa and the wider continent. Institutional isomorphism and policy diffusion theory jointly frame the analysis, explaining why states converge on similar cyber-security structures under coercive, mimetic, and normative pressures, and why implementation nonetheless varies with domestic institutional capacity. The study adopts a qualitative, comparative, desk-based design, applying content analysis to primary legal instruments alongside secondary institutional and scholarly data. Three findings emerge; First, Nigeria's cyber-security architecture is legally dense but organizationally dispersed across at least six institutions, with coordination between them left to informal collaboration rather than binding protocols. Second, domestic instruments draw on globally recognized principles, yet Nigeria has not ratified the African Union's Malabo Convention, and sub-regional harmonization through ECOWAS stays underdeveloped. Third, the Global Cyber-security Index 2024 places Nigeria in Tier 3, combining near-maximum legal scores with persistent weakness in capacity building and cooperation relative to regional leaders such as Mauritius, Rwanda, Kenya, Ghana, and Tanzania. Nigeria's institutional fragmentation, rather than a shortage of legislation, accounts for this gap. The study recommends consolidating institutional coordination, ratifying continental instruments, and prioritizing sustained capacity-building investment over further legislation.

Keywords: Cyber-security governance, Critical information infrastructure, Public policy, Nigeria, Data protection

Introduction

Cyber-security governance determines whether the infrastructure carrying citizens' data functions as an engine of development or as a point of national vulnerability (Calderaro & Craig, 2020). As states digitize public services, finance, and telecommunications, protecting this infrastructure, increasingly classified as critical national information infrastructure,

becomes a governance question. Which institutions hold authority over it, how those institutions coordinate with one another, and how domestic frameworks align with the regional and continental instruments meant to harmonize protection across borders together determine whether legal protection translates into functional protection?

Nigeria illustrates the weight of this governance question. The country hosts Africa's largest mobile subscriber base and one of the continent's fastest-growing digital economies, yet it also records substantial losses to cybercrime (International Telecommunication Union [ITU], 2024). Growth without matching protection is costly. Nigeria's capacity to govern its cyber-security architecture, and specifically to protect the critical infrastructure that carries this data, therefore carries direct economic weight.

Successive administrations have built a layered legal architecture in response. The Cybercrimes Act of 2015, amended in 2024, created the statutory basis for prosecuting cyber-offences (Federal Republic of Nigeria, 2024a). The National Cyber-security Policy and Strategy (NCPS) of 2021 set the coordinating policy framework (Office of the National Security Adviser [ONSA], 2021). The Nigeria Data Protection Act (NDPA) of 2023 established a dedicated data protection authority (Federal Republic of Nigeria, 2023). Most recently, the 2024 Critical National Information Infrastructure (CNII) Order designated thirteen critical sectors and 243 critical services for enhanced protection under ONSA (Federal Republic of Nigeria, 2024b; Technology Times, 2024). Each instrument closes a distinct governance gap. None specifies how the institutions it creates should coordinate with the others.

Continental instruments extend this architecture beyond Nigeria's borders. The African Union's Malabo Convention, in force since June 2023, is the continent's principal attempt to harmonize cyber-security regulation (African Union, 2014; Chatham House, 2025). Nigeria has not ratified the Convention, a position it shares with Algeria and several of the continent's other major economies (Chatham House, 2025). This continental dimension, alongside Nigeria's domestic institutional

architecture, forms the empirical focus of the study.

Statement of Problem

Despite dense legislation, the International Telecommunication Union's Global Cyber-Security Index (GCI) 2024 classified Nigeria in Tier 3 ("Establishing"), behind regional peers such as Ghana, Kenya, Rwanda, and Mauritius, all of which reached Tier 1 (Nairametrics, 2024; Odes, 2024). This gap between legal density and functional capacity is a policy puzzle. Existing scholarship examines Nigerian instruments such as the NDPA, the Cybercrimes Act, and Malabo largely in isolation (Aloamaka, 2025; Ofo, 2026), with little analysis of how Nigeria's institutions coordinate with each other and with the regional frameworks meant to align them. That gap motivates this study.

Research Questions

Three questions guide the analysis:

- (1) What is the current legal-institutional architecture governing cyber-security and critical data infrastructure protection in Nigeria?
- (2) To what extent is Nigeria's domestic cyber-security framework harmonized with continental (African Union) and sub-regional (ECOWAS) instruments?
- (3) How does Nigeria's institutional cyber-security capacity compare with that of selected African peer states, and what institutional factors account for the observed differences?

Objective of the Study

To examine Nigeria's legal-institutional architecture for cyber-security governance, assess the extent to which it is harmonized with continental and sub-regional instruments, and compare Nigeria's institutional capacity with that of selected West African and continental peer states.

Assumption of the Study

The study is guided by the following assumption:

Nigeria's institutional fragmentation, rather than a deficit in legal instruments, accounts for the gap between its legal-measures performance and its lower scores on capacity development and international cooperation in the Global Cyber-Security Index.

Literature Review

Conceptual and Empirical Review

Scholarship on cyber-security governance in developing states has grown alongside digital transformation across the Global South. Calderaro and Craig (2020) find that international cyber-capacity-building initiatives have historically emphasized technical assistance while underestimating the governance and diplomatic dimensions of capacity, producing durable inequalities between norm-shaping and norm-receiving states. Nigeria fits this pattern: legal capacity has developed quickly, while organizational and cooperative capacity, which depend most on sustained institutional investment, lag behind (ITU, 2024).

Nigerian legal scholarship has mostly examined instruments one at a time. Aloamaka (2025) situates the NDPA 2023 against the European Union's General Data Protection Regulation (GDPR) and finds that the Act adopts globally recognized principles even as the independence and enforcement capacity of the new Nigeria Data Protection Commission (NDPC) remain underdeveloped relative to international benchmarks. Ofo (2026) traces Nigerian cyber-security law from early anti-fraud statutes through the Cybercrimes Act and its 2024 amendment, documenting a dense but institutionally dispersed field of agencies spanning the Office of the National Security Adviser (ONSA), the Nigeria Computer Emergency Response Team (ngCERT),

the National Information Technology Development Agency (NITDA), and sector regulators. Related monitoring work documents a 72-hour incident-reporting requirement introduced by the 2024 amendment and the designation of critical infrastructure across thirteen sectors in mid-2024 (Digital Policy Alert, 2025).

At the continental level, the Malabo Convention is Africa's principal attempt at a binding, harmonized cyber-security instrument, but its slow ratification, fewer than a third of the African Union's fifty-five member states by 2025, is attributed in part to newer national and sub-regional frameworks that many states view as better aligned with global standards such as the GDPR (Chatham House, 2025). This pattern matches broader findings that transnational cyber-security governance stays fragmented, with states favouring tailored national instruments over continental harmonization even where the latter would ease cross-border enforcement (Calderaro & Craig, 2020). Across this literature, a gap recurs: studies analyze Nigerian instruments individually or continental instruments apart from national implementation, and rarely connect domestic architecture to the regional frameworks meant to align it. This study addresses that gap through a structured comparative reading of both levels.

Theoretical Framework

The study draws on two complementary theories. Institutional isomorphism and policy diffusion theory: institutional isomorphism, developed by DiMaggio and Powell (1983), holds that organizations within a shared field converge in structure through three mechanisms: coercive isomorphism (external pressure such as treaty obligations), mimetic isomorphism (modeling on perceived successful peers under uncertainty), and normative isomorphism (shared professional norms diffused through training and standard-setting bodies). Applied here, this

framework helps explain why Nigeria's architecture, a national CERT, a data protection authority, and a critical-infrastructure designation regime, mirrors structures found in reference states even where domestic capacity differs substantially.

Policy diffusion theory, as synthesized by Berry and Berry (2018), explains how specific instruments spread across jurisdictions: vertical diffusion from supranational bodies to national governments, and horizontal diffusion among peers through learning and emulation. In Nigeria's case, vertical pressure flows from African Union and ECOWAS instruments, while horizontal pressure flows from comparator states such as Ghana, Kenya, and Rwanda, whose stronger GCI standings make them plausible reference points (ITU, 2024). Together, these frameworks generate the study's guiding proposition: Nigeria's architecture reflects genuine isomorphic and diffusion pressure at the level of legal-instrument adoption, but implementation and coordination capacity, which diffuses less readily than legal text, stay constrained by domestic institutional factors. Section 5 tests this proposition against the documentary evidence.

Methodology

Research Design

This study uses a qualitative design, deploying comparative, content analysis, and desk-based policy analysis approaches suited to a systematic assessment of legal-institutional architecture within a compressed timeframe. The design combines structured qualitative content analysis of primary legal and policy texts with comparative policy analysis that situates Nigeria's institutional performance against regional peers using secondary indicator data. Together, these components answer the descriptive question on institutional architecture (RQ1) and the comparative questions on harmonization

and peer performance (RQ2, RQ3) without requiring primary data collection.

Data Sources and Selection Criteria

Data collection drew on three categories of sources. The first category comprised primary legal and policy instruments, collected from official Nigerian and international portals: the NCPS 2021 (ONSA, 2021), the NDPA 2023 (Federal Republic of Nigeria, 2023), the Cybercrimes Act 2015 and its 2024 amendment (Federal Republic of Nigeria, 2024a), the CNII Order 2024 (Federal Republic of Nigeria, 2024b), and the Malabo Convention (African Union, 2014). The second category consisted of institutional indicator data, principally the ITU's GCI 2024, which benchmarks 194 countries across five pillars: legal, technical, organizational, capacity development, and cooperation (ITU, 2024). The third category comprised secondary scholarly sources: professional legal scholarship analyzing these instruments (Aloamaka, 2025; Calderaro & Craig, 2020; Ofo, 2026). Sources qualified for inclusion if issued between 2014 and 2026, if they addressed cybersecurity governance, data protection, or critical-infrastructure protection in Nigeria, West Africa, or the African Union framework directly, and if they were retrievable from an official portal, an international organization, a peer-reviewed legal journal, or a reputable policy-monitoring body. Sources lacking identifiable attribution, or addressing purely technical rather than governance questions, were excluded.

Analytical Approach

Primary texts were coded for the institution each creates or empowers, the coordination mechanisms it states with other agencies, and its relationship to continental or sub-regional instruments, supporting RQ1 and RQ2. For RQ3, a comparative analysis matched Nigeria's GCI 2024 tier and pillar scores against

four reference states, Ghana, Kenya, Rwanda, and Mauritius, chosen as the region's highest performers and therefore plausible mimetic reference points under institutional theory (DiMaggio & Powell, 1983). The resulting themes are organized by research question in the findings, with two summary tables.

Limitations

As a desk-based study, this analysis lacks primary interview data from Nigerian practitioners that would test documented mandates against lived coordination practice, and it is bound by the currency of the GCI 2024 assessment cycle.

Findings

RQ1: Institutional Architecture and Coordination

Nigeria's cyber-security architecture is legally dense but organizationally dispersed across at least six institutions, each created under a separate instrument and reporting through a different line of authority, summarized in Table 1. ONSA occupies the apex coordinating role under the NCPS 2021 and the 2024 CNII Order, which designated thirteen critical sectors, fifty-two sub-sectors, 243 critical services, and fifty-two regulatory agencies for enhanced protection (Technology Times, 2024). Beneath ONSA, the national CERT (ngCERT) coordinates incident response, while sector-specific CERTs, NITDA's CERRT, the NCC-CSIRT for telecommunications, and the Central Bank of Nigeria's (CBN) Security Operations Centre for finance, operate their own advisory and reporting functions.

Table 1 *Nigeria's Cyber-security Institutional Architecture*

Institution	Statutory Basis	Core Mandate
Office of the National Security Adviser (ONSA)	National Cyber-security Policy and Strategy, 2021	National coordination of cyber-security policy; oversight of CNII protection
Nigeria Computer Emergency Response Team (ngCERT)	Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015/2024	National incident response, threat advisories, coordination of sectorial CERTs
National Information Technology Development Agency (NITDA)	NITDA Act, 2007	IT governance and standards; hosts the NITDA Computer Emergency Readiness and Response Team (CERRT)
Nigerian Communications Commission (NCC) / NCC-CSIRT	Nigerian Communications Act, 2003	Sectorial incident response for telecommunications infrastructure and operators
Nigeria Data Protection Commission (NDPC)	Nigeria Data Protection Act, 2023	Data protection supervision, registration of data controllers/processors, enforcement
CBN Security Operations Centre (SOC)	CBN Risk-Based Cyber-security Framework	Sectorial oversight of cyber-security in banking and payments infrastructure

This structure exhibits the coercive and mimetic isomorphism institutional theory predicts: a national CERT and sectorial

CSIRTs mirror globally recognized models, and the NDPA 2023 follows the GDPR's structural template, including an

independent supervisory authority with enforcement powers (Aloamaka, 2025). Coordination mechanisms between ONSA, NITDA, the NCC, and the NDPC, however, are described only in general terms, information-sharing and collaboration, rather than as binding protocols. Ofo (2026) reaches a parallel conclusion: Nigerian cyber-security law has developed incrementally rather than through a single consolidating framework.

RQ2: Regional and Continental Harmonization

Nigeria's domestic framework aligns only partially with continental instruments. The NCPS 2021 and NDPA 2023 draw on internationally recognized principles, yet Nigeria has not ratified the Malabo Convention, a position it shares with Algeria and other major African economies (Chatham House, 2025). Less than a third of the African Union's fifty-five member states had ratified the Convention by 2025, despite its June 2023 entry into force (African Union, 2014; Chatham House, 2025). ECOWAS-level coordination stays underdeveloped, and the reviewed documents identify no

binding sub-regional incident-sharing mechanism comparable to the European Union's Network and Information Security framework. Many African states now regard their national frameworks as more current than the decade-old Malabo text, which reduces the incentive to ratify (Chatham House, 2025). Under policy diffusion theory, horizontal diffusion from peer states has substituted for, rather than reinforced, vertical diffusion from the continental instrument.

RQ3: Comparative Institutional Capacity

The GCI 2024 gives a structured basis for comparing Nigeria's capacity with regional peers. Nigeria was classified Tier 3 ("Establishing"), scoring highest in legal measures, 19.52 of 20 points, but lower in capacity development and international cooperation (Nairametrics, 2024). Mauritius, Egypt, Ghana, Tanzania, Kenya, Rwanda, and Morocco reached Tier 1, reflecting stronger organizational and cooperative-pillar performance rather than legal measures alone (Odes, 2024). Table 2 summarizes this comparison.

Table 2 *Global Cyber-security Index 2024: Nigeria and Selected African Peer States*

Country	GCI 2024 Tier	Notable Standing
Mauritius, Egypt	Tier 1 (Role-modeling)	Perfect scores; strong performance across all five GCI pillars
Ghana, Tanzania, Kenya, Rwanda, Morocco	Tier 1 (Role-modeling)	Advanced institutional and organizational cyber-security commitments
Zambia, Benin, Togo, South Africa	Tier 2 (Advancing)	Solid frameworks with identifiable gaps in select pillars
Nigeria	Tier 3 (Establishing)	Strongest pillar: legal measures (19.52/20); weakest: capacity building and international cooperation

This comparison suggests Nigeria's weakness is not principally legislative but an implementation and cooperation gap, dimensions institutional theory identifies as least amenable to simple mimetic adoption because they depend on sustained funding, training pipelines, and functioning liaison relationships rather than statutory passage (DiMaggio & Powell, 1983; Calderaro & Craig, 2020).

Contribution of the Study

The study contributes to public policy scholarship on digital governance in developing states by assessing institutional coordination rather than reviewing a single instrument. For policymakers, it identifies where Nigeria's framework is strong (legal measures) and where it lags (capacity building, cooperation). For the wider region, it speaks to the challenge of aligning national regimes with continental instruments at a moment when Malabo has only recently entered into force and most member states have yet to ratify it (Chatham House, 2025).

Discussion and Recommendations

Discussion

The findings support the study's guiding proposition. Nigeria's adoption of a national CERT, a GDPR-modeled data protection authority, and a critical-infrastructure designation regime shows clear coercive and mimetic isomorphism, with structures adopted in forms that track global and regional reference models (DiMaggio & Powell, 1983). Legal-instrument diffusion has proceeded relatively smoothly, matching Berry and Berry's (2018) account of vertical and horizontal diffusion, whether through Malabo, GDPR-style global norms, or the performance of peer states such as Rwanda and Kenya. Persistent institutional fragmentation complicates this picture: CERT mandates overlap, ONSA's coordinating role is not always implemented through binding protocols,

and Nigeria has not ratified Malabo despite broad substantive alignment with it. These gaps indicate that the organizational and cooperative capacities institutional theory associates with normative isomorphism have diffused more slowly than legal text. Normative isomorphism depends on professionalization: shared training, staff exchange, and participation in international communities of practice (DiMaggio & Powell, 1983). Nigeria's comparatively low GCI capacity-building and cooperation scores fit this pattern, suggesting normative diffusion is currently the weakest channel of convergence (ITU, 2024). This reframes the policy problem. The framework itself, including the NDPA 2023 and the amended Cybercrimes Act, already tracks international standards (Aloamaka, 2025; Ofo, 2026). What Nigeria lacks is not legislation but implementation and coordination, rooted in fragmented authority across ONSA, NITDA, the NCC, and the NDPC.

Recommendations

Four recommendations follow, tailored to institutional capacity constraints typical of developing-country governance.

First, consolidate inter-agency coordination. The National Cyber-Security Coordination Centre envisaged under the NCPS 2021 should be put into effect through a binding memorandum of understanding among ONSA, NITDA, the NCC, the NDPC, and sectoral CERTs that specifies reporting lines and escalation procedures rather than general collaborative language.

Second, advance ratification of the Malabo Convention. Because domestic instruments already align substantially with its requirements, ratification would be a low-cost step that strengthens cross-border cooperation and regional leadership.

Third, prioritize capacity-building investment over further legislation. Given

Nigeria's strong legal-measures score, investment should target the GCI's weaker pillars through sustained funding for ngCERT and sectoral CERT staffing, training partnerships, and regional exercises.

Fourth, strengthen ECOWAS-level cooperation. As the sub-region's largest economy, Nigeria is well placed to champion a binding incident-sharing mechanism modeled on the European Union's Network and Information Security framework, reducing reliance on the slower continental instrument alone.

Conclusion

This study examined how Nigeria's cyber-security architecture coordinates internally, aligns with continental instruments, and compares with regional peers. Anchored in institutional and policy diffusion theory, the analysis finds Nigeria has absorbed the legal and structural templates of global cyber-security governance without matching the coordination and capacity-building depth of higher-performing peers such as Rwanda, Kenya, and Mauritius. The gap is best understood as an implementation and normative-diffusion shortfall rather than a legislative one, which points policymakers toward institutional consolidation and capacity investment as the priority for Nigeria's next governance phase. Future research using primary interviews with agency officials, alongside comparable analysis of additional ECOWAS states, would extend and test the account offered here.

References

African Union. (2014). *African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)*. Adopted 27 June 2014; entered into force 8 June 2023.
[https://au.int/en/treaties/african-](https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection)

[union-convention-cyber-security-and-personal-data-protection](https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection)

Aloamaka, P. C. (2025). A critical analysis of the Nigeria Data Protection Act 2023: Elevating standards to global norms. *UCC Law Journal*, 4(2), 242–263.

<https://journal.ucc.edu.gh/index.php/ucclj/article/view/1724>

Berry, F. S., & Berry, W. D. (2018). Innovation and diffusion models in policy research. In C. M. Weible & P. A. Sabatier (Eds.), *Theories of the policy process* (4th ed., pp. 253–297). Routledge.

<https://doi.org/10.4324/9780429494284-8>

Calderaro, A., & Craig, A. J. S. (2020). Transnational governance of cyber-security: Policy challenges and global inequalities in cyber capacity building. *Third World Quarterly*, 41(6), 917–938.
<https://doi.org/10.1080/01436597.2020.1729729>

Chatham House. (2025, October). *The AU can help African countries adopt the UN cybercrime convention. But the challenges are significant*.
<https://www.chathamhouse.org/2025/10/au-can-help-african-countries-adopt-un-cybercrime-convention-challenges-are-significant>

Digital Policy Alert. (2025). *DPA digital digest: Nigeria* [2025 edition].
<https://digitalpolicyalert.org/digest/dpa-digital-digest-nigeria>

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 48(2), 147–160.

<https://doi.org/10.2307/2095101>

- Federal Republic of Nigeria. (2023). *Nigeria Data Protection Act, 2023*.
- Federal Republic of Nigeria. (2024a). *Cybercrimes (Prohibition, Prevention, Etc.) (Amendment) Act, 2024*.
- Federal Republic of Nigeria. (2024b). *Designation and Protection of Critical National Information Infrastructure Order, 2024*.
- International Telecommunication Union. (2024). *Global Cyber-security Index 2024*. <https://www.itu.int/hub/publication/d-hdb-gci-01-2024/>
- Nairametrics. (2024, September 13). *ITU lists Nigeria among tier-3 countries in Global Cyber-security Index 2024*. <https://nairametrics.com/2024/09/13/itu-lists-nigeria-among-tier-3-countries-in-global-cybersecurity-index-2024/>
- Odes, D. (2024, October 18). *Cyber-security in Africa: Rankings and insights from the 2024 Global Index*. Web Security Lab. <https://websecuritylab.org/cybersecurity-in-africa-rankings-and-insights-from-the-2024-global-index/>
- Office of the National Security Adviser. (2021). *National Cyber-security Policy and Strategy 2021*. Federal Government of Nigeria.
- Ofo, N. (2026, April 14). *Introduction to cyber-security law in Nigeria [SSRN working paper]*. <https://ssrn.com/abstract=6701238>
- Technology Times. (2024, August 26). *Critical National Information Infrastructure: Tinubu orders NSA to secure 13 key sectors*. <https://technologytimes.ng/critical-national-information-infrastructure/>