International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2024: 7.101

An Assessment of Nigeria's Cyber Laws: Effectiveness, Gaps, and International Alignment

Ahmad Muhammad Tahir[1 2]

[1]Department of Forensic Science, Vivekananda Global University Jaipur
[2]Department of Computer Science, Aliko Dangote University of Science and Technology Wudil
Corresponding Author Email: *ahmad.tahir4[at]yahoo.com*

Abstract: ***The digital economy has grown at a fast pace in Nigeria bringing about great social and economic value but also exposing people to cyber threats. This research will assess the suitability of the key cyber laws in Nigeria, namely the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (amended 2024) and the Nigeria Data Protection Act (NDPA) 2023, to the requirements of the modern cyber threats, and how they fit into the global best practices frameworks (EU GDPR/NIS2, US sectoral strategies, the IT Act of India and the cyber regime in South Africa). The research uses a comparative legal-analysis methodology and targeted literature synthesis to conclude that the legislative system in Nigeria is conceptually consistent with global standards but operationally flawed: overlapping institutional mandates, limited forensic and prosecutorial capacity, inadequate mandatory breach-reporting requirements, and incomplete international cooperation mechanisms. The paper proposes prioritized, practical reforms to boost enforcement capacity, clarify agency roles, mandate incident reporting, and operationalize international evidence-sharing. The recommendations are intended to inform policymakers, regulators, and civil society engaged in Nigeria's digital governance reforms.***

Keywords: Cyber law, NDPA, Cybercrimes Act, Nigeria, GDPR, Incident reporting, DFIR, Ransomware, IoT security

1. Introduction

The digital transformation has taken the centre stage in the economic development of Nigeria. Fintech, e-commerce, digital government services, and mobile communications facilitate expansion but also increase attack surfaces used by fraudsters, ransomware operators as well as state and non-state advanced persistent threat (APT) actors. According to the recent national and regional reports, there has been an increasing rate of cyber incidents in the African continent and Nigeria as a country, in particular, which reflects the urgency of the credible legal and operational response [1].

The Cybercrimes Act (2015, amended 2024) and the Nigeria Data Protection Act (NDPA, 2023) represent the key milestones of cyber governance in Nigeria. Nonetheless, the presence of laws on books may not translate to operational deterrence and resilience in incident management. This paper seeks to answer these questions:

Are the cyber laws in Nigeria working effectively in practice?

- In what areas are they weak compared to the current threat vectors (ransomware, IoT, supply-chain attacks, AI-enabled attacks)?
- And to what extent do they conform to the international legal and operational standards?

The paper will then position the cyber laws in Nigeria within the global and regional context, outlining the comparative methodology, providing the findings on gaps and effectiveness, and giving prioritized recommendations.

2. Literature Review

This section synthesises literature on cyber law design, enforcement capacity, and emerging threat dynamics.

2.1 Legal Foundations, Enforcement Capability, and Institutional Design (Nigeria & Africa)

Multiple studies of the cyber governance in Nigeria observe that Nigeria has made significant standardising gains: the Cybercrimes Act categorizes offence types well, and the NDPA prevents personal data misuse more effectively, although implementation problems remain. Nwocha et al. and related commentaries catalogue the extensive coverage of the Act but emphasize open-ended enforcement prescriptions (the Act tasks relevant enforcement agencies without clear allocation) and lack of resources that hamper the effectiveness of prosecution [2].

The establishment of Nigeria Data Protection Commission (NDPC) by the NDPA is a significant institutional improvement to the previous NDPR; but numerous policy reviews have warned that the establishment of an institution is merely the start, autonomy, financial clarification, and procedures (e.g. deadlines to respond to data-subject requests) are needed before its enforcement can become efficient.

Common themes have been noted in scholarship and reports across Africa: shortages in skills, low reporting rates, poor forensic capacity, and deficiencies in coordination. The case of South Africa abundantly illustrates the same trends: the effective drafting of the legislative acts is sometimes disabled by a lack of operational capacity and sluggish international collaborations for evidence sharing [1].

2.2 International Standards and Operational Obligations

International frameworks can offer both substantive and procedural models. The GDPR enshrines strong data-subject rights (e.g., erasure, portability), and explicit timeframes (72-hour notification to the supervisor in case of a breach) and the NIS2 directive reinforces mandatory reporting of incidents and supply chains risk management obligations for essential/important entities. These tools are a mix of law and

supervisory enforcement that form quantifiable compliance vectors of regulated entities (DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022on Measures for a High Common Level of Cybersecurity across the Union, Amending Regulation (EU)No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive), 2022; Notification of a Personal Data Breach to the Supervisory Authority, 2018).

The most important multilateral tool towards cooperating on cybercrime is the Budapest Convention on Cybercrime (Council of Europe), which standardises offences and mutual assistance practice; it has been used as a model by many jurisdictions for mutual legal assistance and procedural powers [5]. The Malabo Convention of the African Union is aimed at providing a pan-African legal floor but is not being widely ratified and implemented at the continent-wide level, making bilateral and multilateral operational arrangements (e.g. MLATs, 24/7 contact points) practical necessities [6], [7].

The cybersecurity practice in the United States is sectoral: well-developed incident-response ecosystems, NIST guidelines for risk management, and a combination of sectoral statutory requirements (e.g., financial, healthcare). The CLOUD Act offers an expedient process of cross-border access to data under certain conditions, demonstrating that legal interoperability of evidence access is as significant as the presence of domestic offences [8], [9].

2.3 Emerging Threats: Ransomware, IoT, AI, and Supply-Chain Attacks

Modern threat assessments highlights ransomware, supply-chain breaches, and more frequently, the role of AI in automating and scaling attacks. ENISA Threat Landscape 2024 refers to ransomware and availability-cantered attacks as the leading issues; the world reporting confirms the idea that ransomware is a very lucrative and adaptable threat. Academic literature on ransomware detection and response also highlights the need for rapid notification and disruption of criminal infrastructure as efficient mitigations [10], [11].

The research literature is beginning to describe the use of AI to orchestrate attacks, experimental studies have shown how large language models can be utilized to automate reconnaissance and the creation of social-engineering content, a tool that could reduce the price of targeting more advanced attacks unless legal, technical, and defensive methods evolve. Concurrently, some high-profile academic claims about the current involvement of AI in ransomware have been refuted and partially retracted, indicating that policy response need to be judicious and supported by evidence [12], [13].

2.4 Comparative Assessments

Comparative studies can offer valuable counterarguments to the reform agenda of Nigeria due to their depiction of the interplay of legal structure, institutional financing, and operation of practice to provide (fail provide) cyber resilience.

In India the IT Act (2000) and other subsequent regulations established the first legal framework to deploy digital commerce and fundamental cybercrimes, yet scholarly criticism highlights limit in its scope and enforcement: the Act was not written with the current threats of IoT, supply-chain, and AI-based in mind, and enforcement remains biased across states and industries [14]. The Indian experience emphasizes that while having foundational statutes is necessary, it must be complemented with regulatory tools, specific supervisory capacity, and swift incident reporting regimes to effectively handle the rapidly evolving threats. This resembles the issues of modernisation and enforcement in Nigeria.

The Cybercrimes Act (2020) and the Protection of Personal Information Act (POPIA) of South Africa have comparators at the regional level: both have extensive definitions of offences and data-protection standards. Nonetheless, South African scholarship and policy reviews identify these same practical barriers experienced in Nigeria: under-resourced forensic laboratories, underreporting, gap in prosecution capacity and slow international collaboration in evidence sharing [15], [16]. The case of South Africa thus indicates that the level of sophistication in legislation should be accompanied by the investment in DFIR, the level of public awareness, and simplified cross-border procedures to give some tangible improvements.

The US model is informative as it integrates a fundamentally sectoral regulatory framework with robust capability of incident response in the private sector with a well-coordinated system of public-private collaboration (e.g., CERTs, ISACs) instead of an overall federal statute regulating cybercrime. The effectiveness of enforcement in the US is due to strong technical assets of the private sector, well-developed incident response ecosystem, and practical frameworks like the NIST Cybersecurity Framework that would ensure consistency in operations in various industries. The US practice highlights the fact that the design of statutes should be supplemented by strong public-private collaboration, widely accepted standards, and practical cross-border evidence regulation (e.g., arrangements of CLOUD Act) to facilitate prompt investigation. In the case of Nigeria, it implies that parallel investments in the threat sharing between the public and the private sector and the practical standards can achieve disproportionate gains prior to attaining regulatory sophistication [9], [17], [18], [19].

The EU presents a complementary model, with its hard-law instruments like the GDPR and NIS2, that integrate robust individual rights, clear breach-notification periods, and substantive cyber-risk-management requirements on essential and significant entities. EU focuses on centralized supervisory powers (national data protection authorities) with defined enforcement mechanisms (administrative fines, compulsory reporting) and emergent products / IoT regulation that deals with supply-chain vulnerabilities. A comparative analysis reveals that EU-style mandatory timelines, certification frameworks, and supervisory enforcement have a significant beneficial impact on compliance incentives and incident response; lessons that Nigeria can emulate by operationalising the NDPC and by adopting compulsory incident-reporting regulations (DIRECTIVE (EU) 2022/2555

OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022on Measures for a High Common Level of Cybersecurity across the Union, Amending Regulation (EU)No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive), 2022; Lella, 2024)

.

All these comparators are depictive of a repetitive theme: the text of law is not enough. India and South Africa demonstrate that good laws can fail to work efficiently unless they have DFIR capacity and effective collaboration; the US can prove the importance of effective response of the private sector and industry standards; and the EU can illustrate the usefulness of binding supervisory regulations, timeframes, and product safety requirements. In the case of Nigeria, the lesson of comparison is obvious: carry on with legal modernisation, but with an instant and specific institutional funding, obligatory operation principles (reporting, certification), and threat-sharing devices between the state and the business to seal the enforcement gap.

Together these comparators illustrate a recurring theme: *legal text alone is insufficient*. India and South Africa demonstrate that well-intentioned statutes can underperform without DFIR capacity and streamlined cooperation; the US shows the value of strong private-sector response and sectoral standards; and the EU demonstrates the benefits of binding supervisory rules, mandatory timelines, and product security obligations. For Nigeria, the comparative lesson is clear: continue legal modernisation, but couple it immediately with targeted institutional funding, mandatory operational rules (reporting, certification), and public–private threat-sharing mechanisms to close the enforcement gap.

3. Methodology

This study adopts a qualitative comparative legal-analysis approach, synthesising statutory texts, policy documents, peer-reviewed literature, governmental and multilateral reports, and targeted case studies. The primary sources include the Cybercrimes Act (as analysed in Nigerian law reviews) and NDPA commentaries from the uploaded corpus (file sources cited throughout). The comparative frame is constructed using authoritative international sources (GDPR, NIS2, Budapest Convention, CLOUD Act, ENISA). The analysis focuses on: (a) statutory design, (b) enforcement and operational readiness, (c) coverage of modern threats, and (d) international cooperation mechanisms.

Limitations: empirical incident-level data for Nigeria is limited due to under-reporting; therefore, the study relies on secondary sources, legal commentary, and comparative benchmarks to infer practical effectiveness.

4. Findings

4.1 Legal coverage and substantive alignment

Cybercrimes Act (2015; amended 2024): The Act codifies a broad set of cyber offences (unauthorised access, data interference, interception, identity theft, offences against critical national information infrastructure), and includes procedural powers for preservation, search and seizure, and cooperation. The 2024 amendments substituted and clarified several sections, but academic critiques emphasise that the Act retains vague references to "relevant enforcement agencies," failing to designate clear institutional responsibility for day-to-day enforcement.

NDPA (2023): The NDPA introduces GDPR-aligned rights (access, erasure, portability), creates the Nigeria Data Protection Commission (NDPC), and formalises cross-border transfer mechanisms (SCC/BCR analogues). This represents a normative leap from the NDPR era. However, evaluative studies caution that NDPA lacks granular procedural timelines (e.g., compulsory response windows for subject access requests) and that NDPC operational funding and independence remain unresolved in practice.

4.2 Enforcement & operational capacity

Across the literature, enforcement capacity is the single largest practical constraint to legal effectiveness. Nigerian analyses point to limited numbers of trained DFIR investigators and specialised prosecutors, under-resourced forensic labs, and judicial unfamiliarity with cyber evidence; all of which impede successful prosecutions and timely remediation. Victim under-reporting compounds this problem. These constraints mirror continent-level trends noted in African studies.

4.3 Modern-threat coverage

While Nigeria's laws criminalise many traditional offences, they do not yet embody the full suite of operational requirements used in more advanced regimes to contend with modern threats:

- **Ransomware & fast-moving incidents:** There are no mandatory national breach-notification timelines or a well-resourced national incident-response certification and playbook comparable to NIS2/GDPR or NIST recommendations that would expedite containment and evidence preservation. Mandatory reporting and quick preservation are critical in ransomware response [4], [20].
- **IoT and product security:** The NDPA and Cybercrimes Act do not address product security obligations or certification regimes for IoT devices (unlike EU moves on product cybersecurity). These omissions create supply-chain exposure [20].
- **AI-enabled threats:** Nigeria currently lacks a national AI security framework to anticipate or regulate AI-driven threat vectors (e.g., automated social engineering). The literature suggests measured, evidence-based policy development is required given mixed claims about AI's current role in cybercrime [12], [13].

4.4 International cooperation

Nigeria's statutory architecture contemplates mutual assistance, but operational mechanisms (24/7 contact points, streamlined MLAT procedures or executive agreements like CLOUD Act equivalents) are not yet fully operationalised. This is problematic because much cybercrime and evidence (logs, backups, cloud data) exist across borders. Comparative practice shows that operational cooperation regimes materially affect investigation speed and success [5], [9].

5. Discussion: Strengths and Weaknesses in Context

5.1 Strengths

- **Comprehensive statutory offence coverage.** Nigeria's Cybercrimes Act contains a wide catalogue of offences and procedural tools that, in principle, enable prosecution [2].
- **Modernised data-protection statute.** The NDPA aligns Nigeria with international data-protection norms and creates an independent supervisory body (NDPC), addressing a long-standing shortcoming [21].
- **Policy momentum.** Ongoing policy discussion and amendments indicate political will to improve digital governance [2].

5.2 Weaknesses

- **Implementation and capacity shortfall.** Without accredited DFIR labs, trained prosecutors, and judicial familiarity, offences remain hard to litigate successfully. Victim under-reporting and resource constraints magnify this weakness [2].
- **Institutional fragmentation.** Vague agency roles and overlapping mandates reduce accountability and slow response times; a central coordinating secretariat or directive is missing [2].
- **Absence of operationally prescriptive rules for modern threats.** Mandatory incident-reporting timelines, IoT/product security standards, and formalised threat-sharing mechanisms are absent or underdeveloped relative to EU NIS2/GDPR and other benchmarks [4], [20].
- **International cooperation is not yet operationalised.** Speed of evidence access, and cross-border preservation is limited by slow MLATs and lack of robust 24/7 contact points [5], [9].

6. Recommendations

The recommendations are grouped by priority and timeframe, integrating comparative best practices.

6.1 High priority (0–12 months)

1) **Clarify enforcement roles via an executive directive**: a Presidential Cyber Governance Directive should explicitly assign lead responsibilities among NITDA, NCC, ONSA, Police cyber units, EFCC, and NDPC, and create an empowered coordination secretariat to manage incident response and MLAT routing. This reduces duplication and accelerates decision-making [2].
2) **Operationalise and fund the NDPC**: provide ring-fenced budgets, staffing plans, enforceable timelines for subject requests (e.g., 30 days), and a published enforcement guideline manual. This will transform statutory powers into practical enforcement [21].
3) **Mandate incident-reporting for critical sectors**: adopt regulations requiring reporting within defined windows (e.g., 72-hour supervisory notification following GDPR practice) for critical infrastructure, finance, telecoms, and government services. This will improve rapid containment and evidence preservation [4], [20].
4) **Create a 24/7 national contact point**: establish a functional contact point for cross-border preservation requests and rapid liaison with foreign counterparts (align with Budapest Convention practice) [5].

6.2 Medium term (12–24 months)

1) **Build specialist DFIR & prosecution capacity**: fund accredited digital-forensics labs, train prosecutors and judges in cyber evidence, and institute certification for DFIR practitioners (public–private capacity building recommended) [2].
2) **Introduce IoT/product security minimums**: adopt baseline cybersecurity requirements for connected devices and certification/labeling regimes for imports and domestic production (mirror EU product cybersecurity approaches) [20].
3) **Establish a National Cyber Threat Exchange (NCTX)**: formalise threat intelligence sharing between government, critical industry, and CERTs, modelled on ISAC/ISAO approaches [8].

6.3 Long term (24–36+ months)

1) **Develop an AI safety & cybersecurity framework**: anticipate AI-enabled threat vectors and require risk assessments for high-impact AI systems; adopt measured rules grounded in empirical threat assessments [12], [13].
2) **Pursue regional and international instrument operationalisation**: accelerate ratification and practical implementation of continental instruments (Malabo) and deepen cooperation with Budapest Convention parties and other partners, using bilateral MLAT improvements where expedient [5], [6], [7].

6.4 Implementation considerations & monitoring

- **Funding & governance:** Reforms require a multi-year, multi-agency funding plan with measurable milestones. Consider a dedicated national cybersecurity fund or ring-fenced budget lines.
- **Stakeholder engagement**: include telecoms, banks, fintechs, cloud providers, and civil society.
- **KPIs:** number of incidents reported, average time from report to containment, prosecution conviction rates, NDPC enforcement actions, and number of DFIR-certified labs.

7. Conclusion

Nigeria has enacted modern legal instruments for cybercrime and data protection. However, to convert normative progress into operational resilience requires targeted reforms in institutional clarity, forensic and prosecutorial capacity, incident reporting, product security, and international cooperation. Implementing the prioritized reforms in this paper will close critical gaps, enabling Nigeria to better prevent, detect, and respond to modern cyber threats while aligning more closely with international norms.

References

[1] S. Henrico and S. Els, "Cyber Attacks in South Africa: Geopolitical and legal implications," *African Security Review*, 2025, doi: 10.1080/10246029.2025.2489352.
[2] Matthew E. NWOCHA, Chioma Vivian ITESHI, and Paul Mgbada AWADA, "AN OVERVIEW OF THE NIGERIAN CYBERCRIME ACT 2015 (AS AMENDED)," 2025.
[3] Official Journal of the European Union, *DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*. THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, 2022.
[4] *Notification of a personal data breach to the supervisory authority*. 2018.
[5] Council of Europe, *Convention on Cybercrime*. 2001.
[6] African Union, *African Union Convention on Cyber Security and personal data protection*. 2014.
[7] A. Gakiria and T. M. Gitonga, "What is the Malabo convention?" Accessed: Nov. 29, 2025. [Online]. Available: https://www.diplomacy.edu/blog/what-is-the-malabo-convention/?utm_source=chatgpt.com
[8] National Institute of Standards and Technology, "The NIST Cybersecurity Framework (CSF) 2.0," Feb. 2024. doi: 10.6028/NIST.CSWP.29.
[9] Stephen P. Mulligan, "Cross-Border Data Sharing Under the CLOUD Act," *Congressional Research Service*, Apr. 2018, [Online]. Available: https://crsreports.congress.gov
[10] I. Lella, "ENISA THREAT LANDSCAPE 2024," Sep. 2024. doi: 10.2824/0710888.
[11] E. Kritika, "A comprehensive literature review on ransomware detection using deep learning," *Cyber Security and Applications*, vol. 3, Dec. 2025, doi: 10.1016/j.csa.2024.100078.
[12] Efosa Udinmwen, "Well, that is awkward - MIT Sloan forced to withdraw 'absolutely ridiculous' paper claiming AI played 'significant role' in most ransomware attacks," Nov. 2025. Accessed: Nov. 29, 2025. [Online]. Available: https://www.tomshardware.com/tech-industry/cyber-security/ai-powered-promptlocker-ransomware-is-just-an-nyu-research-project-the-code-worked-as-a-typical-ransomware-selecting-targets-exfiltrating-selected-data-and-encrypting-volumes?utm_source=chatgpt.com
[13] Nathaniel Mott, "AI-powered PromptLocker ransomware is just an NYU research project — the code worked as a typical ransomware, selecting targets, exfiltrating selected data and encrypting volumes." Accessed: Nov. 29, 2025. [Online]. Available: https://www.tomshardware.com/tech-industry/cyber-security/ai-powered-promptlocker-ransomware-is-just-an-nyu-research-project-the-code-worked-as-a-typical-ransomware-selecting-targets-exfiltrating-selected-data-and-encrypting-volumes?utm_source=chatgpt.com
[14] A. M. Tahir, "The Efficacy of the Information Technology Act, 2000, in Addressing Emerging Cyber Threats in India," *International Journal of Science and Research (IJSR)*, vol. 14, no. 11, pp. 1692–1694, Nov. 2025, doi: 10.21275/SR251124195921.
[15] S. Mabunda and R. Akindele, "ON LEGISLATING CYBERCRIME: NIGERIAN, SOUTH AFRICAN, AND UNITED KINGDOM PERSPECTIVES," 2024. [Online]. Available: https://scholarworks.lib.csusb.edu/ciima
[16] M. Watney, "Exploring South Africa's Cybersecurity Legal Framework Regulating Information Confidentiality, Integrity, and Availability." [Online]. Available: https://www.popiact-compliance.co.za/images/Documents/POPIA_Regulations_-_Dec_2018.pdff
[17] "NIST Cloud Computing Standards Roadmap," Gaithersburg, MD, Jul. 2013. doi: 10.6028/NIST.SP.500-291r2.
[18] "Framework for Improving Critical Infrastructure Cybersecurity," Gaithersburg, MD, Apr. 2018. doi: 10.6028/NIST.CSWP.04162018.
[19] S. Atkins and C. Lawson, "Cooperation amidst competition: cybersecurity partnership in the US financial services sector," *J Cybersecur*, vol. 7, no. 1, 2021, doi: 10.1093/cybsec/tyab024.
[20] European Union, *NIS2 Directive: securing network and information systems*. 2022. [Online]. Available: https://www.enisa.europa.eu/topics/eu-cyber-crisis-and-incident-management/csirts-network
[21] S. Nma Modilim, I. Bolarinwa, M. Tolani Omidiora, and O. Tawo, "Reforming Data Governance in Nigeria: A Critical Analysis of the Nigeria Data Protection Act, Regulatory Enforcement, and Global Alignment," *International Journal of Law Management & Humanities*, vol. 7, no. 6, 2024, doi: 10.10000/IJLMH.119827.