EXAMINATION OF THE LEGAL FRAMEWORK FOR COMBATING CYBERCRIMES IN NIGERIA*

Abstract

This article found cybercrime to have emerged as one of the most potent threats to Nigerian contemporary governance, economic stability, national security, and the protection of fundamental rights in this digital age. Nigeria, like many rapidly digitising states, was found to have responded by enacting specialised legislations and established multiple enforcement and regulatory institutions. This article found that these developments notwithstanding, persistent concerns remain regarding the effectiveness, coordination, constitutional compliance, and practical enforcement of the country's cybercrime legal framework. This article therefore examined the legal frameworks for combating cybercrimes in Nigeria, assessing their scope, operational performance, structural challenges, rights implications, and reform prospects. To addressed the missing gap found, the article, inter alia, addressed the following issues: to what extent does the existing Nigerian legal framework effectively address the different forms of cybercrimes in Nigeria? How do the policy gaps and enforcement challenges undermine the fight against cybercrimes in Nigeria? The aim and objectives of the study were achieved by examining the provisions and enforcement framework of Nigeria's Cybercrimes Act 2015 and 1999 constitution. The doctrinal methodology was adopted in this article thus statutes, case law, juristic and non-juristic works contained textbooks, journals, internet, etcetera to achieve the aim and objectives of this article. The article found, inter alia, that Nigeria possesses a substantially developed but operationally constrained cybercrime governance system. The article recommended legal and policy reforms for a comprehensive cybercrime regime in Nigeria among other recommendations.

Keywords: Cybercrimes, Legal Framework, Examination, Nigeria

1. Introduction

The increasing reliance on digital technologies in Nigeria has facilitated new and complex forms of criminal activity within cyberspace, posing serious threats to national security, economic stability, and individual rights. In response, Nigeria has developed a comprehensive legal framework for combating cybercrimes, comprising both national legislation and international legal instruments to which the country is a party. This article examines the legal architecture governing the prevention, investigation, prosecution, and punishment of cybercrimes in Nigeria, comprising relevant domestic statutes and applicable international conventions, which underpin Nigeria's cybercrime control regime.

2. Legal Framework for Combating Cybercrimes in Nigeria: Cybercrimes (Prohibition, Prevention, etc.) Act No. 17 2015

The Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 represents Nigeria's first comprehensive legislation dedicated solely to combating cybercrimes and ensuring cybersecurity. Before its enactment, attempts to address technology-related offenses relied on general provisions in the Criminal Code Act and the Penal Code Act, which were insufficient to deal with the peculiarities of cybercrime.[1] With the growing incidence of online fraud, identity theft, hacking, cyberstalking, and other internet-related offences, coupled with Nigeria's notoriety in global cybercrime rankings, the need for a specific law became imperative. Consequently, the Cybercrimes Act was enacted to provide a legal and institutional framework for the prohibition, prevention, detection, prosecution, and punishment of cybercrimes in Nigeria. The Act also serves to domesticate international obligations arising from Nigeria's participation in global and regional instruments on cybercrime, such as the African Union Convention on

[*] **By Samuel Tolu Olumide ADESINA, LLB, BL, LLM, PhD Candidate**, Bingham University, Karu.
[*] **David Andrew AGBU, LLB, BL, LLM, MILR, PhD**, Professor of Law, Nasarawa State University Keffi, Email: davidmaisongo2@gmail.com; and
[*] **Lawrence Monwo ALABI, LLB, BL, LLM, PhD Candidate**, Nasarawa State University, Keffi.

[1] Y. A. Ibrahim and Others, 'Cybercrime and Cyber Law in Nigeria: An Overview of Challenges and Way Forward' [2023], Proceedings of the International Conference on Computing and Advances in Information Technology (ICCAIT 2023) 21-23 November 2023, Ahmadu Bello University, Zaria, Nigeria

Cybersecurity and Personal Data Protection (Malabo Convention, 2014) and commitments under the Budapest Convention on Cybercrime (though Nigeria is not a signatory, it aligns with many of its principles).[2] The objectives of the Act include to criminalize and punish a wide range of illicit activities committed through computer systems and networks; secure vital systems such as financial institutions, communication networks, power grids, transportation systems, and other national assets that are vulnerable to cyber-attacks; ensure safe use of the cyberspace for economic, social, and governmental activities; establish agencies, obligations, and procedures for effective investigation, enforcement, and prosecution of cybercrimes; and facilitate cross-border collaboration in combating the transnational dimensions of cybercrime, among others.[3]

The Act contains 59 sections divided into eight parts, covering substantive offences, penalties, enforcement procedures, and institutional arrangements. Some of the salient provisions include cybercrime Offences such as unlawful access to computer systems[4], system interference[5], computer-related forgery and fraud[6], cyberstalking and cyberbullying[7], cybersquatting[8], child pornography and sexual exploitation[9], and electronic signature and record validity[10], among others. It is interesting to note that the Act provides protection of Critical National Information Infrastructure (CNII). Consequently, the Act empowers the President, on the recommendation of the National Security Adviser, to designate certain systems as CNII[11]. Attacks on CNII attract severe penalties, including imprisonment up to 10 years and heavy fines.

Beyond the catalogue of cybercrime offenses, the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 contains several other provisions that are crucial to understanding Nigeria's approach to cybersecurity governance. These provisions are largely institutional, regulatory, and procedural in nature, and they provide the framework for enforcement, cooperation, and safeguarding critical systems that underpin the Nigerian economy and national security.

A central feature of the Act is the protection of Critical National Information Infrastructure (CNII).[12] The law recognizes that certain computer systems and networks are so essential to the functioning of the state and the economy that their disruption would have catastrophic consequences. To this end, the Act empowers the President of Nigeria, upon the recommendation of the National Security Adviser, to designate particular systems or networks as critical infrastructure.[13] Such systems may include those related to banking and financial services, energy, telecommunications, defense, transport, and public administration. Once designated, these infrastructures enjoy heightened legal protection, and any act of interference with them attracts severe penalties. This provision reflects the recognition that modern economies and national security are increasingly dependent on the resilience and security of digital systems.

Another important set of provisions in the Act concerns the obligations placed on service providers, financial institutions, and other stakeholders whose platforms are frequently exploited for cybercrimes. Telecommunications companies, internet service providers, and banks are required to retain traffic data for a specified period[14], generally two years, to ensure that information necessary for investigations is

[2] A. O. Salau, 'Cybersecurity, state surveillance and the right to online privacy in Nigeria: A call for synergy of law and policy' [2024] 1, *African Journal on Privacy & Data Protection* 152-175

[3] Section 1

[4] Section 6, which criminalises hacking and unauthorized access.

[5] Section 5 which prohibits interference with data or computer systems, including denial of service attacks

[6] Sections 13 and 14, addressing identity theft, phishing, and manipulation of digital data for fraudulent purposes.

[7] Section 24, criminalizing online harassment, threats, and false information intended to cause harm

[8] Section 25, which criminalizes the registration of domain names with the intent to extort or deceive legitimate owners.

[9] Sections 23 & 32, prohibiting the production, distribution, and possession of child pornography online.

[10] Section 17, which gives legal recognition to electronic signatures and records in commercial transactions.

[11] Section 3

[12] Section 5

[13] Section 3

[14] Section 38 (2)

not lost. These entities are also under a legal duty to cooperate with law enforcement authorities when called upon to provide subscriber information, transaction records, or other relevant data. The Act obliges financial institutions to monitor and promptly report suspicious electronic transactions that may be linked to cybercrime, money laundering, or terrorist financing.[15] By imposing these obligations, the Act seeks to harness the capacities of private sector actors in the prevention, detection, and investigation of cybercrimes, recognizing that government institutions alone cannot combat such crimes effectively.

The institutional framework established under the Act is also worthy of note. One of the key bodies created is the Cybercrime Advisory Council.[16] This is a multi-stakeholder organ made up of representatives from government, the private sector, civil society, and the security community. The Council has the responsibility of advising the government on policies, strategies, and regulations relating to cybercrime and cybersecurity. It provides a platform for coordination across diverse stakeholders whose collaboration is essential in addressing the multidimensional nature of cyber threats. In addition to this, the Act provides for the establishment and operation of the National Computer Emergency Response Team (CERT)[17], which is charged with the responsibility of monitoring, detecting, and responding to cybersecurity incidents nationwide. The CERT plays a frontline role in the technical management of cyber threats, while the Advisory Council ensures coherence in policy and strategic direction.

The Act also extends significant powers to law enforcement agencies in order to strengthen the investigative process. Security agencies such as the police, the Economic and Financial Crimes Commission (EFCC), and other designated authorities are granted the authority to arrest suspects, search premises, seize equipment, and conduct forensic analysis where cybercrime is suspected.[18] Importantly, the Act sets out clear procedures for the preservation and admissibility of electronic evidence.[19] Given that cybercrimes are often perpetrated across borders and leave digital rather than physical trails, the admissibility of electronic evidence in judicial proceedings is a cornerstone of effective prosecution. The Act accordingly recognizes the legal validity of electronic signatures and records[20], thereby modernizing Nigerian law to reflect the realities of a digital economy and ensuring that electronic transactions can be relied upon in both commercial dealings and court proceedings. Jurisdictional provisions in the Act[21] also underscore the recognition of the borderless nature of cybercrime. The law applies not only within Nigeria but also to offences committed outside the country where Nigerian citizens, critical infrastructure, or national interests are affected. This extraterritorial jurisdiction ensures that offenders cannot escape liability merely by operating from beyond Nigerian territory. It also facilitates international cooperation, as the Act provides a legal basis for Nigeria to collaborate with foreign states, international organizations, and law enforcement networks in the investigation and prosecution of cross-border cybercrimes.

A further dimension of the Act relates to the financing of cybersecurity initiatives. The Act establishes the National Cybersecurity Fund[22], which is domiciled with the Central Bank of Nigeria. The Fund is financed through a levy imposed on designated electronic transactions carried out by businesses and financial institutions in the country. The resources are to be used for the implementation of cybersecurity programs, capacity building, public awareness campaigns, and the strengthening of institutional responses to cybercrime.[23] Although this provision has sometimes been criticized for imposing

[15] Sections 21 and 37
[16] Section 42
[17] Section 41
[18] Section 45
[19] Sections 45 and 55
[20] N. C. Uzoka and others, 'Cybercrime and Digital Transactions Law in Nigeria towards Attainment of Sustainable Development Goals' [2025] 16 (2), *Beijing Law Review*, 1037-1049
[21] Section 50
[22] Section 44
[23]U Udoma and B Osagie, 'An Overview of the Application of the National Cybersecurity Levy' < https://uubo.org/wp-content/uploads/2024/05/Article-on-the-cyber-security-levy.pdf> Accessed 28 June 2025

additional financial burdens on businesses, it reflects the understanding that sustainable funding is indispensable for the fight against cybercrime.

The 2024 amendment to the Act reinforced many of these non-offense provisions. The reforms clarified the oversight role of the Office of the National Security Adviser, particularly in the designation and protection of critical national information infrastructure, while also enhancing the responsibilities of financial institutions and service providers in data retention and reporting.[24] They also introduced closer alignment between the Act and the Nigeria Data Protection Act of 2023, especially in the handling of personal data during investigations. Furthermore, the amendments strengthened the mechanisms for international cooperation by providing more explicit procedures for mutual legal assistance and cross-border information sharing, thereby aligning Nigeria's framework with international best practices.

From the above, it is clear that the key provisions of the Cybercrimes Act that transcend the mere criminalisation of offences form the backbone of Nigeria's legal architecture for cybersecurity. They underscore the law's preventive, regulatory, and institutional focus, which complements its punitive elements. By safeguarding critical information infrastructure, obligating service providers and financial institutions to support law enforcement, validating electronic evidence and signatures, establishing strategic and technical institutions, extending jurisdiction across borders, and creating a funding framework, the Act lays the foundation for a holistic national response to the cybercrime menace.

3. Significance of the Act in Combating Cybercrime in Nigeria

The enactment of the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, as amended, represents a watershed moment in Nigeria's legislative response to the challenges posed by the digital age. Prior to its passage, Nigeria relied on outdated criminal statutes, the Criminal Code Act and the Penal Code Act, to prosecute offenses committed in cyberspace. These laws were drafted at a time when computers, the internet, and digital transactions were non-existent in Nigeria, and therefore lacked the conceptual and practical tools to address the complex realities of cybercrime.[25] Against this background, the Cybercrimes Act stands out as the first dedicated, comprehensive, and systematic legal framework to address cyber threats in the country. Its significance can be appreciated across several dimensions:

First, the Act plays a critical role in criminalising a wide spectrum of technology-driven offenses that were previously either unregulated or insufficiently addressed by general criminal law. By expressly defining and prohibiting acts such as cyberstalking, cybersquatting, identity theft, child pornography, and attacks on critical information infrastructure, the law provides legal clarity on behaviors that constitute cybercrimes. This has not only filled the legislative vacuum but has also harmonized Nigeria's approach with global best practices. In doing so, the Act ensures that prosecutors, judges, and law enforcement agencies have a clear statutory basis to charge and punish offenders.

The Act is also significant in terms of protecting critical national information infrastructure (CNII). In a global environment where cyber-attacks can cripple financial systems, disrupt energy supply, or compromise national defense, safeguarding these infrastructures has become a top national security priority.[26] By empowering the President to designate vital systems as critical infrastructure and attaching stringent penalties to interference with them, the Act elevates cybersecurity to a matter of state security and economic survival. This protection is indispensable in an economy that increasingly relies on digital platforms for banking, communication, governance, and commerce.

Equally important is the Act's role in strengthening institutional and regulatory mechanisms. The establishment of the CERT under the Act has institutionalized multi-stakeholder collaboration and

[24] Sections 3(1), 41(1), 44(6), and 56(1)

[25] L Tsado, A Raufu, E Ben-Edet and D Krakrafaa-Bestman, 'Combatting the Threat of Cybercrime in Nigeria: Examining Current Laws and Policies' [2023] 5(4), *Journal of Applied and Theoretical Social Sciences,* 413-430.

[26] A. O. Ayub and L Akor, 'Trends, Patterns and Consequences of Cybercrime in Nigeria' [2022] 5(1), *Gusau International Journal of Management and Social Sciences,* 241-262

technical coordination in the fight against cybercrime.[27] The Advisory Council provides a platform where government agencies, private sector stakeholders, and civil society can formulate policies, strategies, and guidelines for addressing cyber threats, while the CERT plays a frontline role in detecting, managing, and responding to cyber incidents. Together, these institutions foster an integrated and coordinated approach, reducing the fragmentation that often undermines law enforcement responses.

Another dimension of the Act's significance lies in its recognition of electronic records and signatures as valid in law. This provision has had profound implications for Nigeria's digital economy. By giving legal validity to electronic contracts, records, and signatures, the Act has facilitated the growth of e-commerce, online banking, and digital financial services. Businesses and consumers can now engage confidently in online transactions, assured that such transactions will be enforceable in law. This legal certainty has been crucial for promoting financial inclusion, innovation in fintech, and the broader digital economy agenda of the Federal Government.

The Act also represents a step forward in ensuring Nigeria's compliance with international standards and obligations. Cybercrime is transnational in nature, and no country can combat it in isolation. Through provisions on transnational jurisdiction and international cooperation, the Act aligns Nigeria with global efforts such as the African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention). This alignment enhances Nigeria's credibility in the international community and facilitates cooperation with foreign law enforcement agencies, financial intelligence units, and multinational organizations in tackling cross-border cyber threats. In addition, the Act is significant in terms of regulatory obligations on private sector actors.[28] By mandating Internet service providers, telecommunications companies, and financial institutions to retain traffic data, report suspicious transactions, and cooperate with law enforcement, the Act recognizes that the private sector is an indispensable partner in cybersecurity. This obligation expands the reach of law enforcement, ensuring that critical evidence and intelligence are not lost and that potential cybercrimes can be detected early. It also reflects the shared responsibility model of cybersecurity, where both state and non-state actors contribute to securing cyberspace.

From an economic perspective, the Act has played an important role in mitigating financial losses arising from cybercrime. Nigeria loses billions of naira annually to cyber fraud, with the banking sector being the most targeted. By establishing reporting requirements, prescribing penalties, and strengthening enforcement mechanisms, the Act contributes to restoring trust in the financial system, protecting consumers, and encouraging investment in Nigeria's digital economy. Its establishment of the National Cybersecurity Fund, financed through levies on designated electronic transactions, also ensures sustainable financing for cybersecurity initiatives, capacity building, and awareness campaigns.

The Act is equally significant from a human rights perspective, albeit with complexities. On the one hand, it protects citizens from harms such as online harassment, identity theft, and exploitation, thereby upholding the right to security, privacy, and dignity in cyberspace. On the other hand, the broad and sometimes vague provisions, particularly Section 24 on cyberstalking, have been criticised[29] for enabling misuse against journalists and activists. The 2024 amendment sought to address these concerns by narrowing the provision to clearly cover intentional harassment and threats while safeguarding legitimate freedom of expression. This adjustment underscores the evolving nature of the law and its capacity to balance security with human rights in a democratic society.

---

[27] E. Anwana, B. Ogundele, M. Awodiran and others, 'The Prosecution of Cybercrimes in Nigeria: Challenges and Prospects' *Proceedings of the 2023 International Conference on Cyber Management and Engineering* (CyMaEn), 178-182

[28]Y. Makeri, "Cyber Security Issues in Nigeria and Challenges', [2017] 7(4), *International Journal of Advanced Research in Computer Science and Software Engineering*, 319

[29] P D Ederagobor, 'Digital Speech on Trial: Section 24 of Nigeria's Cybercrime Act and its Impact on Civil Liberties' < file:///Users/samoguche-yiaga/Downloads/ssrn-5315568.pdf> Accessed 02 Jan. 2026

Beyond its legal significance, the Act also carries symbolic and cultural weight. Nigeria has often been associated globally with cyber fraud, particularly the notorious 'Yahoo Yahoo' phenomenon. By enacting a strong legal framework, the government sends a clear message both domestically and internationally that it takes cybersecurity seriously. This has the potential to reshape perceptions of Nigeria, attract foreign investment, and reassure international partners that the country is committed to securing its digital environment. It also contributes to domestic value reorientation, particularly among young people, by demonstrating that cybercrime is not a harmless hustle but a serious crime with grave consequences.

Finally, the Act's significance lies in its adaptive and evolutionary potential. The 2024 amendments, which refined contentious provisions, aligned the law with the Nigeria Data Protection Act, and introduced stronger measures against ransomware, illustrate that the framework is not static but responsive to emerging threats. This adaptability is critical in a domain where technology evolves rapidly, and new forms of cybercrime constantly emerge. It positions Nigeria to remain legally prepared in the face of future challenges in cyberspace.

The Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (as amended), is a cornerstone of Nigeria's legal and policy response to the digital age. Its significance spans criminal law, national security, institutional development, economic growth, human rights protection, international cooperation, and cultural perception. While its implementation has not been without challenges, the Act provides the essential legal foundation upon which Nigeria can build a safer, more secure, and rights-respecting cyberspace that supports national development.

4. Conclusion and Recommendations

This article has undertaken a comprehensive examination of the legal and institutional frameworks for combating cybercrimes in Nigeria, situating cybercrime governance within the intersecting domains of criminal justice, national security, digital regulation, and constitutional law. Through a critical of the provisions of the constitution and cybercrime Act, the study demonstrates that Nigeria possesses a substantially developed yet operationally constrained cybercrime governance architecture, characterised by both foundational adequacy and persistent structural limitations. The central argument advanced throughout the article is that the effectiveness of cybercrime control in Nigeria depends not merely on the existence of specialised legislation or enforcement institutions, but on the coherence, coordination, technical capacity, and constitutional legitimacy of the broader governance system within which cybercrime regulation operates.

The article establishes that Nigeria's statutory framework, anchored primarily in the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 and complemented by legislation governing evidence, financial crime, telecommunications, and data protection, provides a comprehensive legal basis for criminalisation, investigation, and prosecution of cyber-enabled offences. This doctrinal foundation reflects a significant legislative response to the realities of digital criminality and positions Nigeria within the evolving global architecture of cybercrime regulation. Nevertheless, the article demonstrates that legal comprehensiveness does not automatically translate into enforcement effectiveness. Jurisdictional ambiguities, evidentiary complexities, and partial misalignment with rapidly developing international cyber norms continue to shape the practical limits of statutory enforcement.

Finally, this article affirms that Nigeria stands at a critical transitional moment in the evolution of its cybercrime governance regime. The foundational elements of effective control are already present within the legal and institutional framework, yet their transformative potential depends on sustained commitment to legal refinement, institutional coordination, technical capacity development, and constitutional accountability. The future trajectory of cybercrime regulation in Nigeria will therefore be determined not solely by legislative enactment, but by the quality of governance, adaptability to technological change, and fidelity to rule-of-law principles. The study reiterates that combating cybercrime in the twenty-first century is not merely a matter of suppressing digital offences; it is fundamentally about shaping the legal and institutional architecture of the digital society itself. Nigeria's ongoing efforts to strengthen cybercrime governance thus carry implications that extend

beyond criminal justice into the broader project of democratic governance, technological progress, and sustainable national development. Through its doctrinal clarification, institutional analysis, and reform-oriented insight, this article contributes to that evolving project and provides a foundation for future scholarship, policy innovation, and rights-centred digital governance in Nigeria and comparable jurisdiction

Arising directly from the above analysis of the legal framework for combating cybercrimes in Nigeria, the article recommended a set of interconnected legal, institutional, procedural, and policy reforms is necessary to enhance the effectiveness, legitimacy, and constitutional compliance of Nigeria's cybercrime governance framework. The following measures are necessary: clarification and harmonisation of the legal framework; strengthening institutional coordination and governance architecture; expansion of technical capacity and digital forensic infrastructure; enhancing judicial specialisation and procedural efficiency; integrating constitutional safeguards and rights-based enforcement; and promoting preventive governance and multi-stakeholder collaboration