TechForGood Initiative
https//tfg-initiative.com

e-RIGHTS
Enhancing Digital Rights in Nigeria

AVOCATS SANS FRONTIÈRES FRANCE

Policy Brief

Reforming Cybersecurity Regulation in Nigeria

July 2025

Iheanyi Nwankwo, PhD
Angela Uwandu Uzoma - Iwuchukwu

Executive Summary

Society's dependence on information and communication technologies makes strong cybersecurity measures indispensable. Governments globally are enacting various regulations, including cybercrime laws, cybersecurity laws, data protection laws, cyber safety laws, and cyber warfare laws to counter the rising tide of digital threats.

Despite instituting several regulatory measures, Nigeria's cybersecurity landscape is plagued by some challenges: an outdated and inadequate Cybercrime Act as well as its perceive misuse by law enforcement authorities, lack of a comprehensive (horizontal) cybersecurity law, a reactive rather than proactive legislative approach, fragmented and complex coordination framework, weak institutional capacity and shortage of cyber-skilled professionals, and low public cybersecurity awareness.

To address these challenges, this policy brief recommends a comprehensive reform of Nigeria's cybersecurity framework. Key recommendations include:

- Conducting an in-depth study to inform the amendment of the Cybercrime Act to address modern threats like deepfakes and ransomware.
- Enacting a comprehensive (horizontal) Cybersecurity Act to standardise obligations across all critical sectors.
- Include period review mechanisms in future cybersecurity legislation to ensure the laws keep up to date.
- Address issues of cybercrime victim support.
- Prioritise stakeholder engagement and greater transparency in legislative processes.
- Establishing a new, centralised national authority for cybersecurity to streamline enforcement and coordination, taking this responsibility from the ONSA.
- Domesticating the Budapest Convention on Cybercrime to enhance international cooperation.
- Establish a national cyber defence framework leveraging citizen expertise.
- Intensifying national skill-building initiatives and public awareness campaigns to foster a culture of cyber hygiene.

These reforms are crucial for strengthening Nigeria's national security, economic stability, and public trust in the digital age.

About the Authors

Dr. Iheanyi Nwankwo, PhD is a legal practitioners and the founder of Tech For Good Initiative. His expertise are on Information Technology and Intellectual Property Law, the legal aspects of Data Protection and Cybersecurity.

He can be reached at.
nwankwo@tfg-initiative.com

Angela Uwandu Uzoma-Iwuchukwu is the Country Director of Avocats Sans Frontières France in Nigeria and is the Project Manager of the European Union and UNESCO funded eRIGHTS project on enhancing digital rights in Nigeria. She is an expert in international law and human rights law, including digital rights.

She can be reached at:
office.nigeria@avocatssansfrontieres-france.org

Introduction

Modern society heavily relies on information and communication technologies (ICTs), the systems they encompass, and the critical infrastructures they support. Protecting these requires a comprehensive approach, utilising a vast array of tools. These tools include frameworks and methodologies that cover technical, organisational, and regulatory aspects. Governments worldwide have supported these initiatives through various regulatory measures, from those mandating foundational security design principles and best practices to industry certifications that validate cybersecurity expertise and products. All these efforts are aimed at stemming the tide of cyber threats.

Over the years, a multitude of cybersecurity-focused laws have emerged, both nationally and internationally. These laws serve to protect not only digital assets but also the individuals who interact within cyberspace. While not always explicitly labelled "cybersecurity laws," there is a broad consensus that the regulatory response to cyber threats encompasses various types of legislation, including general laws, sector-specific laws, and criminal law.

Although it is challenging to append strict classifications to these laws, a working demarcation could place them within the rubrics of:

1. Cybercrime laws: These laws prohibit and punish specific actions committed using computers or the internet, or against information systems, such as the unlawful interception of data over a public network, online fraud or scams, cyberbullying, ransomware attacks, among others. They define offences and outline procedures for investigating and prosecuting perpetrators. These laws are complemented by rules of evidence for digital materials and specific law enforcement powers.

2. Cybersecurity laws: These regulations are designed to protect cyber assets (encompassing both public and private infrastructure) from breaches of their confidentiality, integrity, and availability. They impose requirements on those who handle these informational assets to implement specific proactive and reactive measures aimed at protecting the system. At the core of these laws is the need to ensure the resilience and integrity of digital systems. Examples of such requirements include ex-ante risk management measures, data breach notifications, and incident response protocols.

3. Data protection and privacy laws: These laws regulate how personal data is processed, and aim to provide individual data subjects with specific controls and rights against those who process their data. Data security is an integral part of these laws, requiring data controllers and processors to implement appropriate technical and organisational measures to protect personal data under their care.

4. Cyber safety laws: As people of all ages and knowledge levels, including vulnerable population like children use cyber assets for their daily activities, it has become necessary for the law to focus on protecting these individuals. Cyber safety laws are becoming an extension of these other laws focused with the safe usage of the digital space, designed with vulnerable groups and consumers, or general users in mind. Example include children online safety and age verification law (see the UK Online Safety Act 2023) and cyber awareness frameworks.

5. Cyber warfare laws: These reflect the military and offensive aspects of cyber defence. They govern the use of cyber capabilities in military and state-sponsored operations, particularly during times of conflict or tension between nations (see the Japanese Active Cyberdefence Law, 2025).

In practice, these laws overlap. It is common to see a cybersecurity law include cyber safety aspects, prohibitory provisions or criminal sanctions.

Apart from this loose categorisation, it is pertinent to note that various areas of human interaction now incorporate a digital element. This has led to laws regulating these interactions, including sector-specific laws, incorporating specific provisions addressing cybersecurity. For instance, intellectual property (IP) law, while primarily focused on the rights of intellectual creators, now includes aspects that prohibit the circumvention of technical protective measures designed to protect IP rights. Similarly, consumer protection laws currently address cybersecurity. In the EU, for example, a recent amendment to the product liability regulation includes cybersecurity as a factor in assessing product safety (see Directive (EU) 2024/2853, Art. 7(2)(f)).

In summary, given the pervasive integration of digital technology into every facet of modern life, cybersecurity cannot be confined to a standalone legal instrument. Instead, its principles and concerns are becoming embedded across a broad spectrum of laws governing human activity, ranging from human rights, healthcare and finance to education, defence, and consumer protection. Consequently, any comprehensive approach to cybersecurity regulation must recognise this trend.

The Problem Statement

Nigeria, like other nations, has been plagued by cyber threats and has over the years instituted several measures to regulate these threats. These regulatory efforts encompass legislation, self-regulation, national policy and strategy, judicial intervention, enforcement actions, and international cooperation, among others.

However, despite progress at various levels, the overall impact remains limited, as reflected in Nigeria's ranking on the global cybersecurity index and the public's perception of the country's cybercrime rate. One such index, published by Oxford University researchers, ranks Nigeria 5th in a global report on sources of cybercrime activities, coming behind Russia, Ukraine, China, and the United States, which occupied the first, second, third, and fourth positions, respectively (See Miranda Bruce, et al, 2024). This position is uncomfortable, given that Nigeria is not as technologically advanced as the other countries on the list.

Such a posture calls for a reevaluation of Nigeria's cyber regulatory landscape and technological capabilities to fortify any loose ends. Several weaknesses in the regulatory front highlight this problem:

1. An Outdated Cybercrime Act

The Cybercrime (Prohibition, Prevention, etc.) Act of 2015 was enacted at a time when crimes committed via computer systems were nascent. The Act was amended in February 2024 to address some issues, including compliance with the ECOWAS Court's decision, which found that Section 24 of the Cybercrime Act violated the African Charter on Human and Peoples' Rights. However, this amendment was not substantial enough to address the law's shortcomings, especially in light of Nigeria's evolving cyber threats and the increasing scale and sophistication of these threats.

The offences addressed by the Act were common at the time of its enactment, but new cybercrimes have since emerged, and old ones continue to evolve. This was not fully addressed in the amendment. While some provisions of the Act could be extended to cover new methods of cybercrime, it is doubtful whether the Act is flexible and adaptive enough to address emerging threats like revenge porn, pig butchering, disinformation, deepfakes, and ransomware. Clarity in the definition of offences is crucial in criminal law, and ambiguities that arise from stretching existing definitions to cover new crimes could impede justice.

Additionally, the penalties outlined in the Cybercrimes Act are not sufficiently dissuasive to prevent these crimes in some cases. Many fines are far lower than the potential damage caused to information systems and individuals by cybercrime (e.g, section 12(3)).

Moreover, the Act lacks adequate provisions for victim support in terms of psychological assistance for those affected by cyberstalking or online harassment.

Finally, although Nigeria acceded to the Council of Europe Convention on Cybercrime in July 2022, the Convention will not have local effect until it is domesticated in accordance with Section 12 of the Nigerian Constitution.

2. The Perceived Misuse of the Cybercrime Act to Target Human Rights Defenders and Journalists

In recent years, numerous reports indicate that certain provisions of Nigeria's Cybercrime Act have been unjustly applied to target activists and violate human rights. While a decision by the ECOWAS Court may have spurred the recent amendment of Section 24 of the Act, this amendment only addressed a subsection of the provision. Other subsections, such as Section 24(2), remain untouched.

Section 24(2) addresses criminal liability for threatening, harassing, or extortion-related communications via computer systems or networks. However, the terms used in this provision—such as "bully," "harass," "threat," "reputation," and "fear of violence"—lack clear definitions. This ambiguity leaves their interpretation open to the subjective judgment of law enforcement and prosecutors. Consequently, critics, including in an opinion editorial by the U.S. Mission in Nigeria, rightly argue that this provision is vague, overbroad, and susceptible to abuse
(See Opinion editorial by the U.S Mission in Nigeria).

Indeed, this provision has been used to arrest bloggers, journalists, and social media users for merely criticising individuals, not necessarily for making threats or engaging in extortion. This practice lends significant credence to arguments about the misuse of the law.

3. Lack of a Comprehensive (Horizontal) Cybersecurity Law

While the Cybercrime (Prohibition, Prevention, etc.) Act, 2015 was a significant legislative step aimed at addressing cyber threats and promoting cybersecurity in Nigeria, it falls short of providing a comprehensive legal framework for a holistic national cybersecurity governance.

The Problem Statement

One of its stated objectives is to enhance cybersecurity across the country; however, since its enactment, there has been no follow-up legislation of general application—what is often referred to as a horizontal cybersecurity law—to systematically operationalise this goal.

Instead, Nigeria has relied solely on a fragmented approach, where certain industries such as finance and telecommunications have developed sector-specific cybersecurity regulations. While these are important areas, the majority of critical sectors—including healthcare, education, manufacturing, and transport—lack clear, enforceable cybersecurity regulation.

This regulatory gap creates inconsistencies in cyber risk management and leaves significant vulnerabilities across the national digital infrastructure. Effectively, the absence of a harmonised cybersecurity legal framework weakens the overall supply chain and undermines the resilience of Nigeria's cyberspace.

4. Reactionary Legislative Intervention

Compounding the issue is Nigeria's predominantly reactive legislative approach to cybersecurity. Legal and policy interventions are often spurred by incidents, such as financial fraud, data breaches, or international scrutiny, rather than being grounded in foresight or proactive risk assessment. The Cybercrime Act of 2015 itself was a response to mounting pressure to curb the rising tide of cyber fraud and repair Nigeria's global image. However, nearly a decade later, legislative innovation in cybersecurity has stagnated, even as the threat landscape has dramatically evolved.

Further complicating matters are legislative proposals that misinterpret cybersecurity needs by focusing disproportionately on content control, surveillance, or social media regulation, rather than on technical safeguards, critical infrastructure protection, and capacity building. Such conflations not only divert attention from genuine cybersecurity priorities but also risk infringing on civil liberties without enhancing national cyber resilience.

5. Unclear Supervisory Coordination and Weak Enforcement

Several agencies play different roles in enforcing cybersecurity in Nigeria, including the Office of the National Security Advisor (ONSA), the Attorney General of the Federation, law enforcement agencies (police, EFCC, Independent Corrupt Practices Commission, etc.), the Nigerian Computer Emergency Response Team (ngCERT), NITDA, Cybercrime Advisory Council, Nigerian Data Protection Commission (NDPC), NCC, CBN, etc.
In the hierarchy, ONSA is responsible for cybersecurity co-ordination efforts in Nigeria, but it is unclear how the downstream coordination of the other agencies is done. There is limited evidence of ONSA's technical, legal and organisational capabilities to respond to cybersecurity challenges across all levels of cyber governance in Nigeria. This presents significant enforcement challenges.

ONSA seems overwhelmed by its responsibilities of coordinating both traditional and cyber-related national security issues, especially, given the complexities of contemporary cyberthreats. These enforcement gaps create an environment where cyberattacks are often concealed and organisations are hesitant to report breaches, resulting in weakened data breach notification systems through denial and counter-accusations.

6. Weak Institutional Capacity and Critical Skills Gap

Nigeria's cybersecurity landscape is significantly undermined by institutional fragility and a pronounced shortage of skilled professionals. Regulatory bodies appear to lack the operational capacity, strategic coherence, and technical depth required to address the rapidly evolving nature of modern cyber threats. This is compounded by persistent resource constraints that stifle the development and implementation of a resilient cybersecurity framework. Many sectors, particularly government institutions and small-to-medium-sized enterprises (SMEs), are unable to allocate adequate budgets toward cybersecurity infrastructure. This includes not only advanced threat detection and response tools but also the continuous professional development necessary to keep pace with global cybersecurity standards.

The skills gap, in particular, remains a formidable barrier: there is a dearth of qualified personnel capable of designing, managing, and sustaining secure digital environments. Without targeted investment in both institutional reform and capacity-building initiatives, Nigeria remains vulnerable to escalating cyber threats that threaten national security, economic stability, and public trust.

7. Low Public Awareness of Cybersecurity

Widespread digital illiteracy in Nigeria undermines the country's cyber resilience. Many individuals and organisations lack basic cyber hygiene, making them vulnerable to phishing, identity theft, and other threats. This is worsened by limited public education and the absence of cybersecurity in school curricula. As internet use grows, especially via mobile devices, uninformed digital habits pose a rising national risk.

Recommendations

The shortcomings identified above highlight the need for a comprehensive reform of cybersecurity regulation in Nigeria. The 2024 amendment to the Cybercrime Act is insufficient to tackle these issues, and it is in this light that the following recommendations are made to legislative stakeholders.

1. Conduct a comprehensive study on the effectiveness and implementation of the Cybercrime Act

A comprehensive study should be conducted to assess the effectiveness and implementation of the Cybercrime Act for the past ten years since its enactment. This would help identify gaps in substantive law and enforcement mechanisms and suggest ways to bridge the gaps in the future.

In any case, this study should lead to the amendment of several provisions of the Act, particularly those related to offences and penalties (including Section 24 (2)). The amendment should address new and emerging cybercrimes, especially considering advancements in technologies such as artificial intelligence, blockchain, and quantum computing, among others.

2. Enact a horizontal Cybersecurity Act

A federal legislation of general application on cybersecurity should be enacted to address proactive cybersecurity obligations throughout the ICT supply chain and across sectors in Nigeria. Such a horizontal cybersecurity law should have provisions on network and information security, risk management, cyber resilience, certifications, skills building, and public awareness campaigns.

Cyber safety provisions for vulnerable groups such as children should be included, except the legislature considers enacting a standalone cyber safety law.

3. Include periodic review mechanisms in cybersecurity regulations

Future cybersecurity laws in Nigeria should include provisions for periodic reviews and updates to ensure they remain relevant in light of evolving cyber threats and technological innovations. Such periodic review should be conducted through multi-stakeholder consultations involving government agencies, industry experts, academia, and civil society, and should result in evidence-based adjustments to legal, technical, and operational frameworks to address emerging risks, close regulatory gaps, and align with international best practices.

4. Address cybercrime victim support

Cybersecurity legislation in Nigeria should provide for victim support, including both physical and psychological assistance, particularly for victims of cyberstalking, online harassment, and identity theft. This would mean amending the current Cybercrime Act to include clear provisions mandating victim assistance services, such as counseling, legal aid, reporting hotlines, and mechanisms for swift redress, while also requiring law enforcement agencies to be trained in victim-sensitive approaches and ensuring coordination with relevant social services and NGOs.

5. Stakeholder engagement and greater transparency in the legislative process

Mechanisms should be established to ensure meaningful engagement with relevant stakeholders, including cybersecurity experts, civil society, and the tech industry, during the review and reform of cybercrime and cybersecurity laws. This will promote more thorough, informed legislative processes and help address gaps and inadequacies in legal reforms.

6. Domestication of relevant international cybercrime instruments

To strengthen Nigeria's legal framework against cybercrime and align it with global standards, the National Assembly should take urgent steps to domesticate the Council of Europe's Convention on Cybercrime (Budapest Convention), in accordance with Section 12 of the 1999 Constitution (as amended). Domestication will enable Nigerian law enforcement, judicial authorities, and other stakeholders to leverage the Convention's provisions on international cooperation, evidence sharing, and harmonisation of cybercrime offences.

7. Create a centralised authority for cybersecurity enforcement

A centralised national authority responsible for coordinating and enforcing cybersecurity policies, standards, and incident response across all sectors should be established, moving the responsibility away from the NSA. This authority should have clear legal powers to oversee compliance, investigate cyber threats, coordinate national cyber defence efforts, and facilitate collaboration between government agencies, the private sector, and international partners. Its mandate should include threat intelligence sharing, setting security standards, capacity building, providing guidance, and ensuring a timely response to cyber incidents, thereby eliminating fragmented efforts and strengthening Nigeria's overall cybersecurity posture.

Recommendations

8. Establish a national cyber defence framework leveraging citizen expertise

A national cyber defence framework that integrates the expertise of citizens, including ethical hackers, cybersecurity researchers, and tech professionals, in defending national critical infrastructure and cyberspace. This framework should create structured collaboration channels such as vulnerability disclosure programs, public-private partnerships, and a voluntary cyber reserve corps. It should also promote responsible hacking initiatives, incentivise citizen contributions through recognition or rewards, and ensure appropriate legal protections for individuals who act in good faith to strengthen national cybersecurity.

9. Intensify skill-building and public awareness measures

Adopt a comprehensive cybersecurity policy that prioritises continuous capacity-building initiatives and workforce development strategies to equip both public and private sector actors with the skills needed to address evolving cybersecurity threats. This should include specialised training programs, certification schemes, public awareness campaigns on cyber hygiene, integration of cybersecurity education in academic curricula, and partnerships with international organisations to align with global best practices.

Conclusion

The pervasive integration of digital technology into every aspect of modern life means that cybersecurity can no longer be treated as a niche concern but as a fundamental pillar of national security and economic resilience. Nigeria's current cybersecurity framework, however, is struggling to keep pace with the rapidly evolving threat landscape. A reliance on an outdated Cybercrime Act, a fragmented and sector-specific regulatory approach, weak institutional capacity, and low public awareness have created significant vulnerabilities.

The recommendations outlined in this brief—from enacting a foundational, horizontal Cybersecurity Act to establishing a dedicated national enforcement authority and fostering a new generation of cyber-aware citizens and professionals—offer a roadmap for comprehensive reform. By moving from a reactive to a proactive and holistic regulatory posture, Nigeria can effectively mitigate cyber threats, build a resilient digital ecosystem, and enhance its standing in the global digital economy. The time for incremental adjustments has passed; a bold and strategic overhaul of the nation's cybersecurity governance is now imperative.

References

- Abuh Ibrahim Sani and Ibrahim Yakub, “Evaluating Nigeria's Readiness Against State-Sponsored Cyber Attacks: A Comparative Study of Cybersecurity Policies, Incident Response, and International Cooperation.” Journal of Computational Analysis and Applications, VOL. 34, NO. 4, 2025.
- EU Directive 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC.
- Iheanyi Nwankwo, “Strengthening Nigeria’s Cyber Frontier: Building Cybersecurity Resilience Through Legal Innovation.” Commonwealth Cyber Journal vol. 3, 2025, ISSN 2959-3018 (print), ISSN 2959-3026 (online) thecommonwealth.org/cyber-journal.
- Japanese Active Cyberdefence Law 2025.
- Miranda Bruce, et al., “Mapping the global geography of cybercrime with the World Cybercrime Index”, Published: April 10, 2024, https://doi.org/10.1371/journal.pone.0297312.
- UK Online Safety Act 2023.
- U.S Mission in Nigeria, “Preventing Misuse of the Cybercrimes Act: Protecting Free Speech And Unlocking Economic Growth” Published: June 11, 2025, https://ng.usembassy.gov/preventing-misuse-of-the-cybercrimes-act-protecting-free-speech-and-unlocking-economic-growth/