The Commonwealth

Commonwealth Cyber Journal \ 27
ISSN 2959-3018 (print), ISSN 2959-3026 (online)
thecommonwealth.org/cyber-journal

Strengthening Nigeria's Cyber Frontier: Building Cybersecurity Resilience Through Legal Innovation

Iheanyi Samuel Nwankwo[1]

Abstract

Nigeria's digital environment faces significant cyberthreats, driven by the country's increasing reliance on information and communication technology across sectors, such as finance, telecommunications and public services. Despite foundational instruments like the Cybercrime Act and the National Cybersecurity Policy, the existing cybersecurity framework is inadequate to address the sophistication and dynamic nature of modern cyberthreats. The regulatory approach remains fragmented, outdated and poorly implemented in most cases.

This article addresses a critical gap in the current cybersecurity framework by proposing a novel legal framework to strengthen Nigeria's cybersecurity regulation. It moves beyond traditional, reactive approaches, arguing for a paradigm shift towards a proactive, resilience-focused regulation that intricately weaves cyber resilience principles – preparedness, adaptability and recovery – into the legislative fabric. Cyber-resilience promotes a holistic approach to security, emphasising proactive measures to anticipate, withstand and adapt to cyber disruptions, ensuring continuity in the face of cyberthreats.

The article uniquely presents a comprehensive blueprint for strengthening Nigeria's cybersecurity posture. It outlines key components of this cyber-resilient regulatory framework, including cyber safeguard legislation mandating risk assessments and 'security by design,' robust incident response mechanisms and strengthened reactive measures. This research offers concrete legal innovations to bolster Nigeria's cybersecurity ecosystem, aiming to reduce vulnerabilities, enhance readiness and foster resilience against dynamic cyberthreats, contributing a distinctly legal perspective to the discourse on cybersecurity in developing nations.

1 Institute for Legal Informatics, Leibniz Universität, Hannover, Germany.
Email: nwankwo@iri.uni-hannover.de

1. Introduction

In today's interconnected and digitally driven world, cybersecurity has become a global concern, particularly for rapidly developing nations like Nigeria. With the increasing reliance on digital technologies for everyday activities, data protection, whether personal or not, and safeguarding the digital infrastructure have never been more crucial. Consequently, cybersecurity has emerged as a vital component of modern data governance, requiring multifaceted measures to protect digital assets and mitigate risks to the infrastructure.

Against this backdrop, Nigeria's current cybersecurity landscape is evaluated to assess its readiness to tackle emerging cyberthreats. This assessment is crucial because, as a regional economic powerhouse with an emerging hub for technological innovation, Nigeria is attractive to cybercriminals seeking to exploit vulnerabilities in such a digital ecosystem. While Nigeria recognises the importance of cybersecurity and has established foundational instruments like the Cybercrime Act 2015, the current legal framework is demonstrably inadequate to address the sophistication and dynamic nature of modern cyberthreats.

Nigeria's cybersecurity framework is characterised by a mix of regulatory, organisational and technological measures, as well as educational initiatives to create awareness at various levels in the digital ecosystem (Global Cyber Security Capacity Centre, 2018). They are, however, marked by isolated, often obsolete, instruments that provide limited coverage amid the evolving threat landscape. This calls for a new formulation of laws and regulations that consider the complex social, technical and environmental factors that shape the modern cybersecurity threat and mitigation strategy alongside an enforcement mechanism that trickles to the lowest level of IT governance.

The gap created by the current state of affairs is significant and exposes the country to various cyber risks. Reports from reputable organisations consistently highlight the numerous threats and challenges that pose significant risks to national security, businesses and individuals (CSEAN, 2023; Cybervergent, 2024; Deloitte, 2024). These reports indicate a continuous rise in cyber incidents, including ransomware attacks, data breaches across various sectors, widespread financial fraud, the proliferation of phishing scams and insider threats.

In a recent assessment of global cybercrime indices, Nigeria's ranking was alarmingly low (Bruce and Lusthaus, 2024). Several factors contribute to this. For example, since 2015, when the Cybercrime Act was enacted, no other general application law has addressed other aspects of cybersecurity in Nigeria. Moreover, many of the provisions of this Act are yet to be implemented. It took almost a decade for the designation of national critical infrastructure to be published, signalling a very slow pace of implementation (Federal Republic of Nigeria Official Gazette, 2024).[2]

2 This is provided for in the Cybercrime Act, Section 3.

This lack of legislative updates and horizontal instruments to systematically address network and device security across various sectors, mandate cybersecurity risk management and promote the adoption of security by design principles throughout the lifecycle of digital products and services, as well as encourage or require the standardisation and certification of certain digital technologies, is significant and threatens the whole cyber ecosystem in Nigeria.

Unlike many cybersecurity policy studies that focus on technical or organisational solutions, this article addresses a critical gap by exploring legal innovation as the key to building cybersecurity resilience in Nigeria. We argue for a paradigm shift from traditional, reactive and prohibition-focused measures towards a proactive, resilience-focused regulatory approach (Talmi, 2023). The article uniquely proposes integrating core cyber resilience principles into Nigeria's legal framework. By outlining a comprehensive blueprint for a cyber-resilient legal framework, this research offers distinctly legal and actionable solutions for strengthening Nigeria's cyber frontier and safeguarding its digital economy.

The proposed approach aims to support Nigerian legislators and regulatory agencies in their cybersecurity decisions and to ensure Nigerian laws and policies are strategic, relevant and adaptive in the face of ongoing threats. This flexibility will allow the regulatory framework to withstand any shock occasioned by emerging threats and adjust to the desired state. Nigeria stands the chance of learning significant lessons from global best practices.

This article is structured as follows: following this introduction, Section 2 contains the methodology. Section 3 examines the critical importance of legal inputs in cybersecurity. Section 4 analyses Nigeria's current cybersecurity regulatory landscape. Section 5 discusses the paradigm shift towards embracing resilience in cybersecurity. Section 6 explores cyber resilience as a regulatory strategy. Section 7 provides a blueprint for strengthening Nigeria's cybersecurity legislation. Section 8 addresses the implementation challenges, and Section 9 concludes.

2. Methodology

This article employs a qualitative research methodology based on document analysis to examine Nigeria's cybersecurity legal framework and propose a resilience-based blueprint for its enhancement. The research follows a doctrinal approach combined with critical policy analysis, aiming to identify gaps and weaknesses in the existing regulatory landscape and develop evidence-based recommendations for improvement. The 'resilience-based blueprint' proposed is grounded in the concept of cyber resilience, focusing on the ability of Nigeria's legal framework to not only prevent cyber incidents but also prepare for, adapt to and rapidly recover from them. This will encompass preventative measures, incident response mechanisms, recovery protocols and adaptive governance structures.

The doctrinal approach provides a systematic exposition of the principles, rules and concepts governing a legal system (Smits, 2015). It examines the relationships between these elements to address gaps in the legal framework. This method involves identifying key legal principles related to cybersecurity within Nigerian law, tracing their evolution across legislative acts and regulations, and analysing judicial interpretations in relevant case law to understand their practical application and interrelation. This approach is used to identify, describe and analyse primary and secondary legal texts, including Acts of Parliament, regulations issued by government agencies and case law, to assess their implications for cybersecurity in Nigeria.

Critical policy analysis is suited for evaluating existing policies and frameworks, identifying shortcomings and proposing more effective alternatives (Robertson and Muirhead, 2022; O'Connor and Rudolph, 2023). This approach employs a framework that systematically deconstructs the existing cybersecurity policy framework, examining its goals, instruments, target groups and underlying assumptions. This deconstruction will facilitate the identification of legislative gaps (areas not covered by law) and implementation gaps (areas where policy enactment falls short of its intended goals). This involves deconstructing the current framework, highlighting legislative and implementation gaps, and developing a normative blueprint for a stronger legal structure.

This research relies exclusively on secondary data sources. Data collection involved an extensive review of legal and policy documents, international legal instruments, government and industry reports, and academic literature. The secondary data was analysed using qualitative content analysis and framework analysis. The findings from both the doctrinal approach and the critical policy analysis, particularly the identified gaps and weaknesses in the existing framework, directly inform the development of the resilience-based blueprint.

3. Cybersecurity: the strategic imperative of legal defence

According to the EU Cybersecurity Act, cybersecurity refers to 'the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats' (European Parliament and Council, 2019).[3] This definition highlights the broad scope of cybersecurity, encompassing not only the technological and data aspects but also the safeguarding of individuals and society. It underscores the importance of comprehensive measures to defend against various cyberthreats impacting multiple aspects of life, from personal privacy to national security.

3 Cybersecurity Act, Article 2.

Addressing cybersecurity challenges requires not only technological preparedness but also a comprehensive legal framework that can effectively respond to the evolving threat landscape. The crucial role of law in cybersecurity is widely acknowledged. Bozgeyik (2023) highlights the importance of legal protections for individuals, organisations and governments against various cyberthreats. These threats include privacy violations, intellectual property infringements, disruptions to international relations and cybercrimes. Similarly, Joshi (2024) highlights the urgent need for cybersecurity laws and regulations to adjust to emerging risks, stressing the importance of global co-operation and ongoing legislative evolution to keep up with rapid technological advancements. Solove and Hartzog (2022) advocate for a holistic approach to data security law, emphasising the importance of focusing on the entire data processing systems and holding all actors in the ecosystem accountable. Their aim is for the law to prioritise prevention and mitigation rather than reactive responses to data security.

In response to increasing cyberthreats, several nations and regional groups have enacted or updated cybersecurity laws.[4] These laws establish cybersecurity standards and requirements for organisations to protect data and systems. For example, the General Data Protection Regulation (GDPR) (European Parliament and Council, 2016) mandates appropriate technical and organisational security measures for personal data protection.[5] By requiring safeguards for information assets and penalising non-compliance, these laws ensure a baseline level of protection and incentivise robust cybersecurity practices. They also define and criminalise cyber offences like hacking, unauthorised access and cyber fraud,[6] deterring cybercriminals and providing a legal basis for prosecution.

While some nations have been proactive in enacting and updating laws to address cybersecurity issues, others have fallen behind. Nigeria falls into the latter category; despite a thriving digital economy, its cybersecurity laws have not kept up with advancements. Although Nigeria's current cybersecurity framework includes, the Cybercrime Act 2015, the National Cybersecurity Policy and Strategy 2021, the Nigeria Data Protection Act (NDPA) 2023 and snippets of cybersecurity-related provisions scattered across sector-specific laws and regulations,[7] significant gaps remain in both the scope of these laws and their implementation. This gap owes mainly to the lack of a cohesive legislative strategy. Therefore, revamping the regulatory framework and adopting a holistic, law-guided approach to fortifying the country's cyber defence is necessary.

4 For example, the EU has enacted the Network and Information Security Directive (NIS2) and the Cybersecurity Act, and the US has adopted the Cybersecurity Infrastructure Security Agency (CISA) Act. CISA has issued numerous guidelines and directives to enhance cybersecurity practices across critical infrastructure sectors.

5 See GDPR, Articles 25 and 32.

6 See, for example, the Convention on Cybercrime 2001.

7 For example, the Central Bank of Nigeria (CBN) Regulation on Risk-Based Cybersecurity Framework, and Guidelines for Deposit Money Banks (DMBs) and Payment Service Providers (PSPs) 2024, the Nigerian Communications Commission (NCC) Consumer Code of Practice Regulation 2024 and the Internet Code of Practice 2019.

4. A dive into Nigeria's cybersecurity regulatory landscape

A closer examination of Nigeria's cybersecurity legal framework reveals a mixed picture. While efforts have been made to bring cybersecurity issues to light, the outcomes of these are sometimes outdated and lack the sophistication needed to address the dynamic and ever-evolving nature of cyberthreats. The earliest attempt to regulate cybersecurity in Nigeria saw the setting up of a Presidential Committee on Illegal Online Activities in 2003, in response to the increasing rate of cyber-related crimes (Ikuero, 2022). This initiative led to establishment of the National Cybersecurity Initiative (NCI). In 2004, the Federal Government formed the Nigeria Cybercrime Working Group (NCWG) to sustain the objectives of the NCI. The NCWG assisted in drafting the Computer Security and Critical Information Infrastructure Bill in 2005, which was not passed into law (IISS, 2023). In 2006, a Directorate of Cybersecurity was created under the Office of the National Security Adviser to continue the work of the NCWG.

About a decade later, in 2014, the National Cybersecurity Policy and Strategy was published, with updates in 2021 (KPMG, 2017; Ekekwe, 2021). These publications exist alongside a National Security Strategy that considers cybersecurity to be part of the national threats. Although these documents set out the government's strategic intent in addressing the country's cyber risk exposure, their lofty ideals are yet to be realised.

In 2015, a more binding legislative instrument was passed in the form of the Cybercrime Act. This Act created a prohibitive framework, proscribing certain activities that threaten cybersecurity, such as unlawful access to a computer, system interference, unlawful interception and cyberterrorism, among others. It also aimed to protect critical infrastructure in Nigeria. It envisaged that the president may designate certain computer systems, networks and information infrastructure as 'critical national information infrastructure,' which is vital to national security or Nigeria's economic and social well-being. In June 2024, the designation order was finally gazetted, nine years after the Act's enactment, signalling a very slow pace of implementation. The Cybercrime Act was amended in February 2024 to correct typographical errors, address some issues in the original document and ensure compliance with the Economic Community of West African States Court's ruling that Section 24 violated the African Charter on Human and Peoples' Rights.[8]

It is important to note that Nigeria acceded to the Council of Europe's Cybercrime Convention in July 2022. However, this will have no local effect until it is domesticated per Section 12 of the Nigerian Constitution. Unfortunately, Nigeria has not signed the African Union (AU) Convention on Cyber Security and Personal Data Protection, which was adopted by the AU in 2014 and came into force in 2023 (Ayalew, 2023).

8 Paradigm Initiative v. FRN. ECW/CCJ/JUD/16/20.

It is equally notable that other criminal laws in Nigeria, such as the Criminal Code, the Advance Fee Fraud and Other Fraud Related Offences Act 2006, the Economic and Financial Crime Commission (EFCC) Act 2004, the Terrorism (Prevention) Act 2011 and the Money Laundering Prohibition Act 2022, have aspects relating to or that could be interpreted to cover cybercrime.

However, these laws need significant reforms to cater to the complexity and sophistication of modern cybercrimes and cybersecurity. For example, the offences addressed by the Cybercrime Act were common at the time of its enactment, but new cybercrimes have emerged, and others continue to evolve. 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 adequately address emerging threats such as revenge porn, disinformation, deepfakes and ransomware (Nwafor et al., 2021; Ajayi, 2023). Clarity in the definition of offences is crucial in criminal law, and ambiguities that arise from stretching existing definitions could impede justice.

Moreover, the penalties specified in the Cybercrimes Act are not sufficiently dissuasive to prevent these crimes. Many of its fines are significantly lower than the potential damage inflicted on information systems and individuals by cybercrime (Sibe, 2024). For example, it is an offence for a government or private employee to intentionally withhold or keep electronic mail, messages or payment card information (credit/debit) that was received in error and should have been delivered to someone else. Conviction carries a penalty of up to one year imprisonment, a fine of ₦250,000 or both.[9] At today's value, this amounts to less than US$150 and is too low in our view to deter such crime.

In 2019, the National Information Technology Development Agency (NITDA) issued the Nigeria Data Protection Regulation (NDPR) to address personal data protection issues. Subsequently, the Nigeria Data Protection Act (NDPA) 2023 was enacted as a federal law dedicated to privacy and personal data protection with an aspect focusing on data security. It requires data controllers and processors to implement appropriate technical and organisational measures to ensure personal data security,[10] and to notify relevant actors of data breaches.[11] It is, however, notable that the NDPA applies only where personal data is processed. Industrial operational data,[12] for example, is outside the scope of the NDPA unless such data relates to an identified or identifiable person.

Beyond the personal data protection law, some sector-specific instruments address cybersecurity in different contexts. These include the Nigeria Communications Commission (NCC) Consumer Code of Practice Regulation 2024 (NCC Regulation 2024) and the NCC Internet Code of Practice 2019 (NCC Code 2019), as well as the Central

9 Cybercrime Act, Section 12 (3).
10 See the NDPA, Section 39.
11 See the NDPA, Section 40.
12 Industrial operational data is data generated by industrial processes and equipment, such as sensors, control systems and Internet of Things (IoT) devices. This data provides valuable insights for optimising operations, predicting equipment failures, ensuring quality control and enhancing safety and security.

Bank of Nigeria (CBN) Risk-Based Cybersecurity Frameworks and Guidelines for Deposit Money Banks (DMBs) and Payment Service Providers (PSPs) 2024 (CBN Regulation 2024). It is equally notable that the Nigerian Code of Corporate Governance 2018, developed according to the Financial Reporting Council of Nigeria Act 2011, has some relevance to cybersecurity risk management. Principle 11 of the Code recommends that the 'Board delegates some of its functions, duties and responsibilities to well-structured committees, without abdicating its responsibilities.' One such committee is the Committee Responsible for Risk Management,[13] and it is expected to include cybersecurity risks in its framework.

Consequently, the extensive list of instruments highlighted above means several agencies play different roles in enforcing cybersecurity in Nigeria. These include:

- Office of the National Security Advisor (ONSA)
- Attorney General of the Federation
- Law enforcement agencies (police, EFCC, Independent Corrupt Practices Commission, etc.)
- Nigerian Computer Emergency Response Team (ngCERT)
- NITDA
- Cybercrime Advisory Council
- Nigerian Data Protection Commission
- NCC
- CBN, etc.

In the hierarchy, ONSA is responsible for cybersecurity co-ordination efforts in Nigeria. ngCERT, domiciled in ONSA, is the apex office responsible for managing cybersecurity activities in Nigeria and co-ordinates the operation of sector-based Computer Security Incidents Response Teams (CSIRTS) hosted in NITDA, NCC and the Defence Space Administration (ONSA, 2017). However, the country faces significant challenges in enforcing and co-ordinating cybersecurity affairs. For example, ONSA, which is responsible for both traditional and cyber-related national security, appears ill-prepared to confront the complexities of contemporary cyberthreats. 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.[14]

13 Nigerian Code of Corporate Governance 2018, Principle 11.5.

14 At the time of writing, no website for ONSA and the Cybercrime Advisory Council relating to their cybersecurity roles could be found.

These enforcement gaps create an environment where cyberattacks are often concealed. Organisations are hesitant to report breaches, weakening data breach notification systems through denial and counter-accusations. A notable example is the ongoing National Identity Management Commission data breach controversy, where the Commission has repeatedly denied breaches, despite revelations of unauthorised third-party access to the National Identity Number database (Okamgba, 2024; Okonji and Ekebuike, 2024; Paradigm Initiative, 2024).

Resource constraints and a significant cybersecurity skills gap also impede Nigeria's ability to develop an effective cybersecurity regulatory framework. Many sectors face financial, technological and human resource shortages needed to build and maintain robust cybersecurity infrastructures. Small and medium-sized enterprises (SMEs) and government institutions, in particular, struggle to allocate sufficient budgets for advanced cybersecurity tools, continuous training and the recruitment of skilled personnel. These limitations leave Nigerian organisations and government institutions highly vulnerable to cyberattacks, exposing them to financial, reputational and operational risks. This calls for urgent action and co-ordination in revamping the country's regulatory framework through a resilient and multifaceted approach, combining legal reform, technical capacity-building and collaboration among domestic and global stakeholders.

5. A paradigm shift: embracing a resilience approach in cybersecurity

The concept of resilience has evolved over the years[15] and is embraced in many disciplines and fields, although the notion lacks a uniform definition (Florin and Linkov, 2016; Trump et al., 2018; Rogers, 2020; Smith, 2023; Araujo et al., 2024). In the domain of cybersecurity, it is widely acknowledged as a holistic approach to security that emphasises an organisation's ability to proactively prepare for, detect, respond to, mitigate and recover from a cyber incident to minimise the impact on its systems and services (Cisco, nd; IBM, nd). It encompasses a multifaceted approach to maintaining operational continuity in the face of cyberthreats, extending beyond the traditional focus on protection and defence, to include a broader strategy that integrates preparedness, adaptability and recovery (AL-Hawamleh, 2024).

Cyber resilience, as defined by leading cybersecurity bodies, emphasises the ability to anticipate, withstand, recover from and adapt to cyber incidents. Ross et al. (2021, p.1) define it as, 'The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.' Similarly, Goldman et al. (2021) view it as the capability to deliver and

15 The word 'resilience' comes to English from the French résilier and the Latin resilire and means jumping back, recoiling, springing back or resuming an original position.

sustain an adequate level of service despite faults and disruptions to regular operations, and Smith (2023, p.38) highlights the 'ability of a cyber system to recover from stress that causes a reduction of performance' as a core feature of cyber resilience.

These definitions converge on the core pillars of cyber resilience: the ability to anticipate, prevent, detect, respond to and recover from cyber incidents. Together, these components form a comprehensive approach aimed not only at defending against threats but also at ensuring an organisation can maintain operations during an attack and swiftly recover from such disruptions. Anticipation involves identifying potential risks before they materialise, allowing organisations to take pre-emptive action, while prevention focuses on implementing security measures that reduce the likelihood of a successful cyberattack. Detection emphasises the need for real-time monitoring systems capable of identifying malicious activity as soon as it occurs. Response involves immediate action to contain the impact of an attack, while recovery ensures operations are promptly restored to normal, minimising downtime and financial losses (Akinsanya et al., 2024).

In practice, cyber resilience involves developing detailed playbooks for managing cyber incidents and ensuring a co-ordinated response during and after attacks. Regular cybersecurity drills and simulations are crucial for assessing readiness, practising high-pressure scenarios and improving co-ordination. Consistently testing incident response procedures helps identify gaps, updates outdated processes and prepares both systems and personnel for various cyberthreats. These proactive measures enhance an organisation's ability to withstand cyberattacks with minimal disruption.

Some commentators have critiqued the growing trend of conflating cybersecurity with cyber resilience. Bygrave (2022), for instance, challenges the idea that cyber resilience should supplant the traditional concept of cybersecurity, arguing that the two serve distinct but complementary roles. It is essential to clarify that this article does not advocate for replacing cybersecurity with cyber resilience. Instead, the aim is to leverage the principles and components of cyber resilience to strengthen and enhance cybersecurity reforms. Cyber resilience is not meant to undermine the importance of traditional cybersecurity measures but to provide a more adaptive and comprehensive framework that addresses both the prevention and the recovery aspects of cybersecurity.

In this context, we propose a legal framework for cybersecurity developed through the lens of cyber resilience. The role of cyber resilience is to provide a foundational perspective – a skeleton – through which regulatory policies and strategic initiatives can be advanced more holistically. By incorporating resilience into the legal architecture, policy-makers can ensure regulations are flexible and adaptable, capable of evolving with the changing threat landscape. This approach aligns with Bygrave's conclusion that resilience-focused ideals can be adapted when reforming security rules, providing an enhanced model that better addresses the complexities of modern cyberthreats. The

incorporation of resilience thus becomes a tool for refining cybersecurity rules, ensuring they are not only proactive in preventing breaches but also robust in responding to and recovering from them.

Unpacking the components of cyber resilience and its role in cybersecurity regulatory governance is essential, given the inevitability of cyber incidents. A cyber resilience framework thus encourages proactive organisational preparedness, ranging from identifying critical assets and understanding their vulnerabilities to developing robust policies, procedures and controls to mitigate risks. This approach aligns with Björck et al.'s (2015, p.5) observation that 'the concept of resilience essentially treats adverse cyber events as part of normal operations.' Embracing this mindset enables regulators integrate countermeasures and contingency plans into the fabric of cyber safeguard laws.

6. Cyber resilience as a strategy in a regulatory framework

Several works have highlighted the importance of robust regulatory frameworks in effectively addressing cybersecurity (OECD, 2012; Björck et al., 2015; Bygrave, 2024). These works have suggested varying approaches to achieving an effective framework, including a risk-based approach. This article adds to this discussion by highlighting the components of cyber resilience as a skeleton for modelling cybersecurity regulatory frameworks for a developing nation like Nigeria.

When viewed through this lens, a cyber-resilient regulation integrates technical, organisational and operational safeguards to ensure systems can withstand and adapt to cyber disruptions through legislation. Essentially, it establishes obligations for key stakeholders, requiring them to ensure their systems are not only prepared to prevent cyberattacks but also proactively equipped to anticipate incidents, respond effectively and recover from them when disruptions occur. This approach is structured around several key components, including mandatory ex-ante risk assessments, security audits, vulnerability management, recovery planning, continuous monitoring and adherence to evolving cybersecurity standards and data protection protocols, while penalising non-compliance. Entities managing critical information infrastructure may face more stringent measures as a result of their criticality systems.

A cyber-resilient regulatory framework also accommodates reactive measures such as ex-post risk assessment, breach notification and vulnerability disclosure, to warn affected entities and giving them time to implement protective measures. Another key aspect of resilience is fostering collaboration and engagement of various stakeholders, including government agencies, private sector entities and civil society, to ensure comprehensive cybersecurity across sectors. Regulatory policies should encourage or require sharing of threat intelligence and best practices, enhancing the collective ability to respond to cyber incidents. Together, these elements foster an environment where cyber resilience is not

merely a technical goal but also a regulatory mandate, ensuring affected stakeholders operate with both proactive and reactive strategies to maintain operational integrity throughout the system lifecycle.

The EU provides an example of legislative initiatives on cybersecurity framed around resilience. This is reflected right from the titles of the legislative instruments, such as the Directive on the Resilience of Critical Entities (European Parliament and Council, 2022) and the just adopted Cyber Resilience Act (CRA) (European Parliament and Council, 2024). The CRA, for instance, introduces horizontal cybersecurity requirements by establishing EU-wide cybersecurity standards for manufacturers and developers of products with digital elements, encompassing both hardware and software.[16] The Act provides two sets of essential requirements in Annex 1 – namely, product cybersecurity requirements and vulnerability handling process requirements, designed to enhance product security by requiring manufacturers to incorporate essential cybersecurity measures from the design phase throughout the entire product lifecycle.

As can be deduced from this discussion, cyber-resilient legislation and policy frameworks are multifaceted and implemented through laws, standards, guidelines and best practices. In this regard, laws must adapt to evolving cyberthreats, allowing updates that reflect new risks and technologies. They should also be robustly enforced to motivate compliance and enhance necessary safeguards. As Kosseff (2018) notes, a focus on resilience requires cybersecurity law to be forward-looking, considering both incident prevention and recovery. This necessitates proactive laws and policies providing the procedural and substantive rules to enhance cybersecurity at all organisational levels, from boardrooms to operational management (Marchant, 2016). This ensures resilience is a core component of organisational strategy, not an afterthought.

7. A blueprint for strengthening Nigeria's cybersecurity regulation

The analysis in Section 4 revealed a cybersecurity legal landscape in Nigeria struggling to keep pace with evolving threats. Key weaknesses identified include the increasingly outdated nature of the Cybercrime Act, its reactive rather than proactive orientation and insufficiently dissuasive penalties. Furthermore, the current regulatory environment suffers from fragmentation and a lack of cohesive, overarching legislation, leading to enforcement and implementation difficulties. Existing laws also exhibit limited scope and coverage, failing to adequately address cybersecurity holistically across all sectors and neglecting the crucial aspect of cyber resilience. Finally, resource and skills gaps impede effective development and implementation.

16 "Products with digital elements" refers to any software or hardware product, including their remote data processing solutions and components, whether sold together or separately.

Recognising these critical shortcomings, this section outlines a blueprint for strengthening Nigeria's cybersecurity regulation. This proposed framework is deliberately structured to directly address each of these identified gaps, offering concrete and actionable measures to build a more robust and resilient cybersecurity ecosystem in Nigeria. The framework strengthens cybersecurity governance through a multifaceted strategy emphasising proactive measures, robust incident response and recovery, reactive requirements and accountability, and collaborative enforcement tools to address evolving threats and vulnerabilities. It includes key components designed to improve Nigeria's overall cybersecurity ecosystem.

7.1 Proactive cybersecurity measures

Nigeria needs cybersecurity legislation that prioritises proactive measures. Recognising the inevitability of cyber incidents, this legislation should prepare stakeholders to anticipate, prevent (where possible) and mitigate the impact of such incidents. Specifically, it should require the following actions from relevant stakeholders:

- **Mandatory risk assessments**

Introducing mandatory, regular and comprehensive ex-ante cyber risk assessments across sectors is a fundamental pillar of proactive cybersecurity legislation. This will be particularly crucial for industries classified as critical infrastructure, such as energy, telecommunications, finance, healthcare, the public sector and transportation, among others.[17] Legislation must require these sectors to conduct periodic systematic risk assessments to identify existing vulnerabilities, evaluate emerging threats and prioritise risk mitigation strategies. Such assessments are essential to ensure these organisations remain vigilant and adaptive in the face of evolving cyberthreats.

This requirement should be elevated to a board-level responsibility of the organisation to enhance accountability and ensure strict adherence. By integrating cyber risk management into the governance structure, senior leadership is made directly accountable for compliance, aligning cybersecurity with the broader organisational goals.

If implemented effectively across sectors, it can create a uniform standard of preparedness, foster resilience and minimise the potential impact of cyberattacks. By institutionalising regular assessments as a legal obligation, the legal system would ensure the critical sectors are continuously equipped to manage and mitigate the growing complexities of cyberthreats.

17 See Designation and Protection of Critical National Information Infrastructure Order 2024. The Schedule contains a list of identified computer systems, networks, assets and communications systems designated as critical national information infrastructure.

- Threat intelligence-sharing

A vital component of the proposed regulation is establishing robust, real-time threat intelligence-sharing platforms among relevant stakeholders. Effective cybersecurity governance hinges on the seamless exchange of actionable intelligence between key actors, including government agencies, private sector entities and international partners. In the Nigerian context, this will fill the gap in current cybersecurity efforts, which are severely hampered by the lack of a co-ordinated and systematic approach to threat intelligence-sharing.

Therefore, legislation should require the establishment of secure, centralised or decentralised platforms or networks that allow stakeholders to share timely and relevant threat information. These platforms would facilitate a more agile and co-ordinated response to cyberthreats, promoting a proactive rather than a reactive security approach. Additionally, enabling real-time intelligence exchanges would strengthen Nigeria's overall ability to effectively detect, respond to and mitigate cyber incidents, positioning the country as a significant player in international cybersecurity efforts.

- Security by design

Nigerian laws must actively promote the development of secure software and systems across all sectors. This approach, known as 'security by design,' entails embedding cybersecurity considerations at every stage of the digital technologies' lifecycle, from design and development to deployment. This strategy will make cybersecurity a foundational element rather than an afterthought in system design, potentially mitigating vulnerabilities and significantly reducing cyber risks by proactively addressing security concerns from the outset.

Likewise, legislation should promote the development of vulnerability disclosure programmes (VDPs) to improve the ability to identify and address potential threats before they can be exploited by malicious actors. These programmes offer a structured and collaborative method for security researchers, ethical hackers and other stakeholders to responsibly report security vulnerabilities. Additionally, legislative frameworks should mandate that system developers provide a Software Bill of Materials (SBOM) for their products. The SBOM serves as a comprehensive inventory of all software components, libraries and dependencies, ensuring transparency and traceability across the supply chain. This measure would not only help manage security risks related to third-party components but also encourage accountability in software development.

- Consistent system auditing and testing

In addition to ex-ante risk assessments, Nigerian cybersecurity regulations should require regular security audits and tests for critical infrastructure and high-risk organisations. These measures are vital for identifying vulnerabilities, testing the effectiveness of

security controls and confirming the efficacy of current cybersecurity measures. Regular audits ensure organisations comply with legal and regulatory requirements while continuously improving their cybersecurity protocols to address emerging threats.

For instance, penetration testing surpasses auditing by actively simulating real-world cyberattacks to assess an organisation's capacity to resist hacking attempts. By mimicking the tactics and strategies employed by malicious actors, penetration tests enable organisations to discover exploitable vulnerabilities in their systems, networks and applications before attackers can exploit them. This acts as a thorough assessment of an organisation's security defences, providing a proactive method to verify whether the implemented security measures are genuinely effective under pressure. Incorporating regular security audits and penetration testing into the legislative framework would strengthen a culture of continuous improvement in cybersecurity, encouraging organisations to stay vigilant and adaptable to the evolving threat landscape.

- **Cybersecurity awareness programmes**

Educating the public, employees and businesses about cyberthreats and best practices is essential for creating a cyber-resilient society. With the growing reliance on digital technologies, the threat landscape has become increasingly complex and widespread. To address these risks, legislation must actively contribute to cultivating a cybersecurity-aware population. This can be accomplished through policies that support and fund the development and implementation of comprehensive cybersecurity awareness and skill-building initiatives, including incorporating cybersecurity education in school curriculum.

Furthermore, fostering a culture of cybersecurity within organisations is equally critical. Legislation should mandate and promote awareness, encouraging organisations to integrate cybersecurity practices into their daily operations. This may include mandatory employee training programmes and regular cybersecurity drills.

7.2 Robust response and recovery mechanisms

While proactive strategies are crucial for mitigating cyberthreats, the inevitability of cyber incidents necessitates the inclusion of robust response and recovery mechanisms within a resilience-focused legislative framework. Legislation should mandate that all sectors, particularly the critical sectors, develop and maintain comprehensive incident response plans that outline clear, actionable steps for managing and mitigating the impact of cyberattacks. These plans must include regular drills and simulations, along with disaster recovery and business continuity solutions designed to minimise operational downtime and disruption.

- **Cyber incident response plan**

To address the rise in cyberattacks, Nigerian legislation should require structured cyber incident response frameworks for organisations. As Nigeria's digital economy expands, businesses encounter heightened risks such as data breaches and ransomware. An effective response plan facilitates prompt detection, analysis, and reaction to

security breaches, minimising damage to data and operations. Implementing these plans enhances national cybersecurity, fosters trust, and strengthens the country's digital landscape.

- **Business continuity planning**

Nigerian legislation should require organisations, especially those in critical sectors, to create and regularly test business continuity plans (BCPs). These plans should clearly describe the procedures for maintaining essential operations and ensuring service continuity during and after a cyber incident. By preparing for various scenarios, organisations can minimise downtime, lessen the impact of disruptions and continue providing essential services even during cyber crises. Regular testing of these plans through simulations and real-time exercises will ensure their effectiveness and preparedness during cybersecurity challenges.

- **Data backup and recovery**

To further strengthen resilience, legislation should mandate robust data backup and recovery mechanisms to protect against data breaches, ransomware attacks and other types of cyber intrusion. These requirements should encompass regular, encrypted data backups and secure storage practices. Moreover, organisations should create reliable recovery processes to swiftly restore systems and data after an attack. Well-maintained backup and recovery systems are crucial in minimising the impact of cyber incidents, enabling organisations to resume operations without significant data loss or prolonged downtime.

- **Disaster recovery procedures**

Comprehensive disaster recovery procedures should be mandated by law, requiring organisations to establish clear strategies for restoring IT infrastructure, systems and business operations after a cyberattack or natural disaster. These procedures should align with broader BCPs. Furthermore, disaster recovery strategies should be customised to address the unique risks facing each sector, ensuring critical systems are prioritised during the recovery process.

7.3 Reactive requirements and accountability

Nigeria's cybersecurity framework should establish reactive obligations across sectors to mitigate the impact of breaches and ensure organisations are accountable for cybersecurity failures. These measures should include mandatory breach notifications, post-incident analysis and a requirement to co-operate with relevant authorities during cybersecurity investigations. Such a framework would foster a culture of accountability and transparency, encouraging organisations to prioritise cybersecurity as a vital component of their operations.

- **Data breach notification and incident reporting**

Enacting a horizonal data breach notification law that requires organisations to notify relevant stakeholders in the event of a data breach is crucial to mitigating the harm victims may encounter afterwards. Drawing inspiration from the NDPA, prompt and transparent data breach notifications in various sectors of the economy, including where non-personal data is crucial, such as the industrial sector, can help lessen the impact of data breaches. The law should require measures such as credit monitoring for victims of a data breach. Organisations should be required to report security breaches, data leaks, ransomware attacks and other cybersecurity incidents to designated authorities to facilitate a co-ordinated response and learning lessons.

- **Post-incident analysis and integration of lessons learned**

Alongside response and recovery mechanisms, legislation should mandate that organisations perform comprehensive post-incident analyses after a cyber breach. This process should entail investigating the incident's root cause, evaluating the effectiveness of the response and pinpointing areas for improvement. The insights from these analyses must be incorporated into future risk management and incident response plans, ensuring organisations constantly enhance their cybersecurity practices.

- **Obligation to co-operate with cybersecurity investigations**

The obligation to co-operate with regulatory authorities during cybersecurity investigations is a critical component of a well-functioning cybersecurity regulatory framework. Organisations that experience cyberattacks or data breaches often possess valuable information that can help identify the source and extent of the attack while preventing future incidents. Therefore, both public and private sector entities should be required to collaborate with law enforcement agencies and cybersecurity authorities during investigations.

7.4 Strengthening the ecosystem through strong enforcement mechanisms and collaborations

Implementing robust enforcement mechanisms and encouraging collaboration among various stakeholders is crucial for building a resilient cybersecurity ecosystem in Nigeria. A comprehensive approach must focus not only on enforcing laws but also on promoting partnerships, research and the continuous development of best practices to ensure cybersecurity remains robust against evolving threats. The legal system should entail the following measures:

- **Strong enforcement mechanisms**

Reformed cybersecurity laws in Nigeria must have clear and enforceable provisions to ensure compliance. Penalties for violations, such as fines, sanctions and legal actions, should be stringent enough to dissuade individuals and organisations from engaging in cybercrime or failing to comply with established cybersecurity regulations. Enforcement

mechanisms must be backed by a competent and well-resourced regulatory body capable of investigating breaches, enforcing penalties, driving accountability and issuing clear guidance where necessary. However, this framework should remain adaptable and include a review mechanism that aligns with the rapidly changing cyberthreat landscape, allowing the regulatory environment to keep pace with innovations.

- Certification programmes and Standards

Adopting standardised certification programmes and industry benchmarks is crucial for enhancing Nigeria's cybersecurity posture. Certification frameworks such as International Organization for Standards (ISO) 27001 and the National Institute of Standards and Technology Cybersecurity Framework offer organisations structured guidelines for managing information security and reducing cyber risks. Establishing national standards that align with these international best practices can significantly strengthen the cybersecurity defences of both public and private institutions. The Standards Organisation of Nigeria (SON) has a crucial role to play in this respect. Certification programmes not only ensure compliance with best practices but also foster a culture of security awareness and continuous improvement within organisations. This should be promoted by law.

- Fostering collaborations

Public–private partnerships are essential for building a resilient cybersecurity ecosystem. Collaborations between government entities and private sector organisations facilitate the sharing of threat intelligence, enabling quicker identification of emerging cyberthreats and promoting collective responses. These partnerships allow for the pooling of expertise and resources, fostering co-ordinated efforts in mitigating cyber risks and managing incidents. Such collaboration also ensures both sectors are aligned in their cybersecurity governance approaches, thereby strengthening the nation's overall cybersecurity posture. Moreover, encouraging active international co-operation is crucial, as cyberthreats often transcend borders. By engaging with global partners at various levels, Nigeria can enhance its capacity to combat transnational cyberthreats, access valuable insights from international experiences and contribute to the global effort to establish stronger cybersecurity norms.

- Research and development

Investing in R&D is crucial for staying ahead of the rapidly evolving cyberthreat landscape. Innovation in cybersecurity technologies, methodologies and tools is essential for detecting, preventing and mitigating sophisticated cyberattacks. By supporting R&D initiatives through legislative measures, Nigeria can cultivate homegrown solutions that address unique national threats while contributing to global cybersecurity advancements. Government funding, academic involvement and private sector investment in

cybersecurity research will be vital in building advanced security infrastructure. Moreover, fostering a culture of innovation ensures Nigeria remains competitive and capable of responding to the challenges posed by new technologies.

8. Implementation considerations and addressing potential challenges

While a strong case has been made for integrating cyber resilience as a foundational element of Nigeria's national cybersecurity regulatory framework, potential challenges in implementation must also be acknowledged. Addressing these requires careful consideration in designing the framework, as outlined below.

8.1 Balancing technological neutrality with prescriptive legislation and the financial burden on SMEs

A key challenge is striking a balance between establishing a robust cybersecurity framework and ensuring technological neutrality while avoiding overly prescriptive legislation. Although this article advocates for embedding cyber resilience principles into law, it does not propose rigid mandates that could stifle innovation or impose excessive financial burdens, particularly on SMEs. Instead, the recommended framework follows a principles-based approach, setting clear cybersecurity objectives and outcomes while allowing organisations flexibility in selecting the technologies and methods to achieve them. The goal is to require essential cybersecurity capabilities – such as risk assessment, incident response and business continuity – without dictating specific technical solutions.

To mitigate the potential financial burden on SMEs, a tiered implementation approach is recommended. This could involve differentiated guidelines and expectations based on organisational size, sector criticality and risk profile. Additionally, the government could explore incentive programmes to support SMEs in adopting essential cybersecurity measures, such as subsidised training, access to affordable cybersecurity tools or tax incentives for cybersecurity investments. This balanced approach ensures the legal framework effectively raises the cybersecurity baseline across all sectors without disproportionately hindering the growth and innovation of smaller businesses.

8.2 Resource constraints, implementation and the need for a dedicated national cybersecurity agency

The effectiveness of any cybersecurity legal framework, regardless of its robustness, ultimately depends on adequate resources and effective implementation. As previously noted, resource constraints – both technical and financial – pose significant challenges to cybersecurity in Nigeria. Therefore, it is essential that the proposed framework is supported by a strong commitment to resource allocation and the establishment of a dedicated and empowered national cybersecurity agency.

The integration of cyber resilience principles into legislation should be explicitly linked to a clear mandate for a dedicated national cybersecurity agency. This agency would play a critical role in implementing the framework and providing support across all sectors. Its responsibilities should include publishing detailed, sector-specific guidelines for cyber resilience by design; developing and delivering comprehensive cybersecurity training programmes; facilitating international cooperation for knowledge-sharing and enforcement; collaborating with the national CSIRT on vulnerability management and penetration testing initiatives; and, critically, ensuring the continuous review and updating of the legal framework and associated guidelines in response to the evolving cyberthreat landscape. Without such a dedicated and well-resourced agency to champion and operationalise these obligations, even the most robust legislation risks remaining largely aspirational.

8.3 Reconciliation with existing laws

The implementation of certain mechanisms within the proposed blueprint – such as threat intelligence-sharing – requires careful alignment with existing legal provisions, particularly the NDPA and the Lawful Interception of Communications Regulations 2019. These regulations govern privacy and lawful interception, which are inherently intertwined with cybersecurity practices.

To ensure compliance, the design and implementation of threat intelligence platforms and protocols must be conducted with full cognisance of these existing legal frameworks. A comprehensive legal review should be incorporated into the implementation process to establish clear protocols that balance effective threat intelligence-sharing with fundamental rights, including privacy and data protection. This legal reconciliation is critical in building a secure, transparent and ethically responsible cybersecurity ecosystem in Nigeria.

8.4 Security by design in procurement

To further embed security by design principles at a national level, cybersecurity considerations should be integrated into national procurement regulations governing the acquisition of information and communication technology (ICT) equipment, systems and software solutions. Given that government agencies and public institutions are among the largest procurers of technology, prioritising cybersecurity at the procurement stage can significantly enhance national security.

Procurement guidelines should be updated to mandate the inclusion of cybersecurity requirements in tender specifications and evaluation criteria. This proactive approach would incentivise vendors to offer more secure products and services, ultimately strengthening the security posture of the public sector and, by extension, the national

digital ecosystem. Embedding security by design into procurement practices is a critical step towards fostering a cybersecurity-conscious culture from the foundation of technology acquisition and deployment.

9. Conclusion

This article has demonstrated the inadequacy of Nigeria's current cybersecurity framework against evolving cyberthreats. We have identified critical gaps: a static Cybercrime Act, fragmented regulation, a reactive posture and enforcement challenges. To address these, we propose a novel, comprehensive blueprint centred on cyber resilience and legal innovation – a necessary but complex undertaking.

Distinct from technical or organisational cybersecurity studies, this article offers a legal and actionable framework. Our blueprint represents a paradigm shift to proactive, resilient cybersecurity, uniquely integrating cyber resilience principles into legislation. Moving beyond reactive prohibition, it emphasises preparedness, anticipation and recovery, directly addressing identified gaps through proactive measures, threat intelligence-sharing, uniform laws and robust enforcement. Its ultimate success, however, depends on nuanced and effective implementation in Nigeria's complex environment.

The transformative potential of this framework thus hinges on implementation. While it offers a pathway to bolster Nigeria's cyber defences, safeguard its digital economy and build trust through proactivity and resilience, significant challenges remain. Bridging resource gaps – financial, infrastructural and expertise-related – requires strategic investment. Beyond resource allocation, inter-agency co-ordination, particularly having a dedicated lead agency, is crucial. A truly resilient ecosystem demands a holistic, long-term approach integrating legal reform with investment in ICT infrastructure, capacity-building, cybersecurity awareness and public–private partnerships. We believe these challenges are surmountable through strategic planning, phased implementation, stakeholder engagement and unwavering national commitment to cybersecurity leadership.

In conclusion, this article offers a timely roadmap for strengthening Nigeria's cybersecurity. Adopting cyber resilience and implementing legal innovations provides a clear, though complex, path to a resilient, adaptive framework. This strategic shift is imperative for Nigeria to fully realise digital benefits while mitigating risks, ensuring a secure digital future. We urge Nigerian law-makers and policy-makers to consider this blueprint, recognising that legal innovation, sustained effort and resource commitment are foundational to a resilient cyber frontier.

References

Ajayi, J. (2023) 'Fake News on Steroids: The Urgent Need for Nigeria to Regulate Artificial Intelligence'. 15 December www.linkedin.com/pulse/fake-news-steroids-urgent-need-nigeria-regulate-artificial-john-ajayi-nnnke/

AL-Hawamleh, A. (2024) 'Cyber Resilience Framework: Strengthening Defenses and Enhancing Continuity in Business Security'. *International Journal of Computing and Digital Systems* 15(1): 1315–1331.

Araujo, M., Machado, B. and Passos, F. (2024) 'Resilience in the Context of Cyber Security: A Review of the Fundamental Concepts and Relevance'. *Applied Sciences*, 14. https://doi.org/10.3390/app14052116

Akinsanya, M., Ekechi, C. and Okeke, C. (2024) 'The Evolution of Cyber Resilience Frameworks in Network Security: A Conceptual Analysis'. *Computer Science & IT Research Journal* 5(4): 926–949.

Ayalew, Y. (2023) 'The African Union's Malabo Convention on Cyber Security and Personal Data Protection Enters into Force Nearly After a Decade. What Does It Mean for Data Privacy in Africa or Beyond?' EJIL, 15 June www.ejiltalk.org/the-african-unions-malabo-convention-on-cyber-security-and-personal-data-protection-enters-into-force-nearly-after-a-decade-what-does-it-mean-for-data-privacy-in-africa-or-beyond/

Björck, F., Henkel, M., Stirna, J. and Zdravkovic, J. (2015) 'Cyber Resilience – Fundamentals for a Definition'. In A. Rocha, A. Correia, S. Costanzo and L. Reis (eds) *New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Computing, vol. 353*. https://doi.org/10.1007/978-3-319-16486-1_31

Bozgeyik, H. (2023) 'Importance of Cyber Law'. *Uzbek Journal of Law and Digital Policy* 2(2). https://doi.org/10.59022/ujldp.104

Bruce, M. and Lusthaus, J. (2024) 'World-First Cybercrime Index Ranks Countries by Cybercrime Threat Level'. University of Oxford, 11 April. www.infosec.ox.ac.uk/article/world-first-cybercrime-index-ranks-countries-by-cybercrime-threat-level

Bygrave, L. (2022) 'Cyber Resilience Versus Cybersecurity as Legal Aspiration. In T. Jančárková, G. Visky and I. Winther (eds) *14th International Conference on Cyber Conflict: Keep Moving*. CCDCOE Publications.

Bygrave, L. (2024) 'The Emergence of EU Cybersecurity Law: A Tale of Lemons, Angst, Turf, Surf and Grey Boxes'. Faculty of Law Legal Studies Research Paper 2024-04. Oslo: University of Oslo.

Cisco (nd) 'What Is Cyber Resilience?' www.cisco.com/c/en/us/solutions/hybrid-work/what-is-cyber-resilience.html (accessed 26 November 2024).

CSEAN (Cyber Security Experts Association of Nigeria) (2023) 'National Cyber Threat Forecast 2024'. https://csean.org.ng/national-cyber-threat-forecast-2024/

Cybervergent (2024) 'Ransomware Attacks in Nigeria'. 16 May. www.cybervergent.com/articles/ransomware-attacks-in-nigeria-5025e

Deloitte (2024) 'Nigeria Cybersecurity Outlook 2024'. www.deloitte.com/ng/en/services/risk-advisory/perspectives/Nigeria-Cybersecurity-Outlook-2024.html

Ekekwe, N. (2021) 'The Updated Nigeria's National Cybersecurity Policy and Strategy'. Tekedia, 24 February. www.tekedia.com/the-updated-nigerias-national-cybersecurity-policy-and-strategy/

European Parliament and Council (2016) 'Regulation (EU) 2016/679 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)'. OJ L 119, 4.5.2016, pp. 1–88.

European Parliament and Council (2019) 'Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) 526/2013 (Cybersecurity Act)'. OJ L 151, 7.6.2019, pp. 15–69.

European Parliament and Council (2022) 'Directive (EU) 2022/2557 of 14 December 2022 on the Resilience of Critical Entities and Repealing Council Directive 2008/114/EC'.

European Parliament and Council (2024) 'Regulation (EU) 2024/2847 of 23 October 2024 on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulations (EU) 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)'. OJ L 2847 20.11.2024, p. 1.

Federal Republic of Nigeria Official Gazette (2024) 'Designation and Protection of Critical National Information Infrastructure Order'. 25 June. https://cert.gov.ng/ngcert/resources/cnii-gazette.pdf

Florin, M. and Linkov, I. (eds) (2016) *IRGC Resource Guide on Resilience*. Lausanne: EPFL International Risk Governance Center.

Global Cyber Security Capacity Centre (2018) 'Cybersecurity Capacity Review Nigeria'. Oxford: University of Oxford.

Goldman, H., McQuaid, R. and Picciotto, J. (2011) 'Cyber Resilience for Mission Assurance'. *IEEE International Conference on Technologies for Homeland Security (HST)*.

IBM (nd) 'What Is Cyber Resilience?' www.ibm.com/topics/cyber-resilience (accessed 25 November 2024).

IISS (International Institute for Strategic Studies) (2023) 'Cyber Capabilities and National Power'. Vol. 2. https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/09/cyber-capabilities-and-national-power-vol-2/cyber-capabilities-and-national-power_volume-2.pdf

Ikuero, F. (2022) 'Preliminary Review of Cybersecurity Coordination in Nigeria'. *Nigerian Journal of Technology* 41(3): 521-526.

Joshi, A. (2024) 'Study of Cybersecurity Laws and Regulations'. *Indian Journal of Law* 2(3): 7-14.

Kosseff, J. (2018) 'Defining Cybersecurity Law'. *IOWA Law Review* 103: 985-1031.

KPMG (2017) 'Building Cyber Security & Resilience in a Digital Africa'. May. https://assets.kpmg.com/content/dam/kpmg/ng/pdf/advisory/ng_building_cyber_security_resilience.pdf

Marchant, G. (2016) 'Advancing Resilience through Law'. In M. Florin and I. Linkov (eds) *IRGC Resource Guide on Resilience*. Lausanne: EPFL International Risk Governance Center.

Nwafor, I, Nwafor, N. and Alozie, J. (2021) 'Revenge Pornography in Nigeria: A Call for Legal Response and Cyber-Censorship of Content by Internet Service Providers'. *African Journal of Legal Studies* 13(2): 1-27.

O'Connor, K. and Rudolph, S. (2023) 'Critical Policy Analysis in Education'. Oxford Research Encyclopedia of Education, 22 March. https://oxfordre.com/education/education/display/10.1093/acrefore/9780190264093.001.0001/acrefore-9780190264093-e-1831

OECD (Organisation for Economic Co-operation and Development) (2012) 'Cybersecurity Policy Making at a Turning Point: Analyzing a New Generation of National Cybersecurity Strategies for the Internet Economy'. Digital Economy Paper 211. Paris: OECD.

Okamgba, J. (2024) 'NIMC Facing Multiple Unauthorized Accesses to NIN Data – Stakeholders'. Punch, 25 June. https://punchng.com/nimc-facing-multiple-unauthorised-accesses-to-nin-data-stakeholders/

Okonji, E. and Ekebuike, A. (2024) 'Again, NIMC Denies Data Breach, Assures Nigerians of Database Security'. This Day, 4 July. www.thisdaylive.com/index.php/2024/07/04/again-nimc-denies-data-breach-assures-nigerians-of-database-security/

ONSA (Office of the National Security Advisor) (2017) 'Action Plan for Implementation of the National Cybersecurity Strategy'. Draft. https://cert.gov.ng/ngcert/resources/draft-action-plan-ncss.pdf

Paradigm Initiative (2024) 'Major Data Breach: Sensitive Government Data of Nigerian Citizens Available Online for Just 100 Naira'. Press Statement, 20 June. https://paradigmhq.org/major-data-breach-sensitive-government-data-of-nigerian-citizens-available-online-for-just-100-naira/

Rogers, P. (2020) 'The Evolution of Resilience'. *Connections Quarterly Journal* 19(3): 13–32.

Robertson, L. and Muirhead, B. (2022) 'Critical Policy Analysis', in *Digital Privacy: Leadership and Policy*. Ontario Tech University. https://ecampusontario.pressbooks.pub/digitalprivacyleadershipandpolicy/chapter/critical-policy-analysis/

Ross, R., Pillitteri, V., Graubart, R. et al. (2021) *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*. NIST Special Publication 800-160, Vol. 2, Rev. 1. https://csrc.nist.gov/pubs/sp/800/160/v2/r1/final

Sibe, R. (2024) 'Cybercrime and the Challenge of Static Legislations in Nigeria'. Forbes, 29 April. www.forbes.com/councils/forbestechcouncil/2024/04/29/cybercrime-and-the-challenge-of-static-legislations-in-nigeria/

Smith, S. (2023) 'Towards a Scientific Definition of Cyber Resilience'. *Proceedings of the 18th International Conference on Cyber Warfare and Security.*

Smits, J. (2015) 'What Is Legal Doctrine? On the Aims and Methods of Legal-Dogmatic Research'. Working Paper. 2015/06. Maastricht: Maastricht European Private Law Institute.

Solove, D. and Hertzog, W. (2022) *Breached! Why Data Security Law Fails and How to Improve It*. New York: Oxford University Press.

Talmi, N. (2023) '10 Bold Suggestions for Creating a Cyber Resilience Framework'. https://cybeready.com/guide-to-cyber-resilience/creating-a-cyber-resilience-framework

Trump, B., Florin, M. and Linkov, I. (eds) (2018) *IRGC Resource Guide on Resilience (vol. 2): Domains of Resilience for Complex Interconnected Systems*. Lausanne: EPFL International Risk Governance Center.

About the author

Iheanyi Samuel Nwankwo LLB, BL, LLM, PhD, is a senior research associate at the Institute for Legal Informatics at Leibniz Universität Hannover, Germany. His research focuses on data protection law, cybersecurity law, and emerging technologies, with a particular interest in systematising data protection impact assessments.