SPECIAL EDITION OF THE CALABAR HISTORICAL JOURNAL (PROCEEDINGS OF THE 4TH INTERNATIONAL MULTIDISPLINARY CONFERENCE 27TH-30TH OCTOBER, 2024)
Vol. 14 (Special Edition), No. 1, June 2025 p34-50 ISSN: 2315-8816
https://thecalabarhistoricaljournal.com/

THE EVOLUTION OF CYBERSPACE AND CYBERSECURITY CHALLENGES IN NIGERIA, 2001–2022

Shammah Asu **KEKUNG**
Department of History and International Studies
University of Calabar, Calabar, Nigeria
kekungasu20@unical.edu.ng
ORCID: 0009-0008-4406-8978

&

Godspower Andrew **UDUIGWOMEN**
Department of History and International Studies
University of Calabar, Calabar, Nigeria
godspoweruduigwomen@gmail.com;
godspoweruduigwomen@unical.edu.ng
ORCID: 0000-0003-3515-0212

Abstract

Between 2001 and 2022, cyberspace in Nigeria expanded at an unprecedented pace, transforming the landscape of communication, commerce, governance, and social interaction. This rapid digital integration, however, was accompanied by a simultaneous surge in cybercrime, including financial fraud, identity theft, phishing, and cyber espionage, posing grave threats to national security, economic stability, and individual privacy. Nigeria's primary legislative response, the Cybercrime (Prohibition, Prevention, etc.) The Act of 2015 established a legal framework for prosecuting cyber offenders but has been widely criticised for weak institutional mechanisms, limited enforcement capacity, and poor inter-agency coordination. Drawing on secondary sources including academic journals, government policy documents, and reports from institutions such as the Central Bank of Nigeria (CBN) and the Economic and Financial Crimes Commission (EFCC), this article undertakes a historical and qualitative examination of Nigeria's evolving cyber threat landscape. It evaluates the adequacy of existing legislative and institutional responses, identifies structural barriers to effective cybersecurity governance, and argues that sustainable cyber resilience in Nigeria demands a multi-pronged approach encompassing infrastructural investment, human capital development, legal reform, and deepened international cooperation.

Keywords: *Cybersecurity, Cybercrime, Cyberspace, Nigeria, Digital Governance, ICT Policy, Cyber Legislation*

Introduction

The end of the Cold War in 1991 reshaped the global order in ways that extended far beyond the military and diplomatic realms. The dissolution of bipolar geopolitical competition created new space for the acceleration of economic globalisation, and with it, the rapid diffusion of information and communication technologies (ICT) across the world. For developing nations, this technological revolution promised transformative possibilities - new pathways to economic growth, more transparent governance, and deeper integration into the international economy. Yet it also brought unforeseen vulnerabilities, as digital networks became both the infrastructure of modernity and the terrain of a new category of criminal and state-sponsored threat.[1]

Nigeria's encounter with these global forces began in earnest with the return to civilian democratic rule in May 1999. Under new liberal economic policies, the telecommunications sector was deregulated, and foreign direct investment was encouraged. Mobile telephony expanded dramatically following the liberalisation of the sector in 2001, with subscriber numbers growing from fewer than 500,000 at the dawn of democracy to over 100 million by the mid-2010s.[2] Internet penetration followed a similar trajectory, driven by the proliferation of broadband infrastructure, undersea fibre-optic cables, and affordable mobile data plans.

This digital transformation reshaped virtually every dimension of Nigerian life. Banking transactions migrated online. Government agencies launched e-governance platforms. Lagos emerged as one of Africa's foremost technology hubs. And yet, this growth occurred against a backdrop of chronic institutional weakness, widespread poverty, and a youth unemployment crisis that created fertile conditions for the exploitation of digital platforms for illicit purposes.[3]

[1]H. Yusuf, "The Information Revolution and Cybersecurity Challenges," Journal of Global Security Studies 2, no. 3 (2017), p. 131.
[2]Nigeria Communications Commission, Annual Report 2020 (Abuja: NCC, 2020), 12.
[3]Wole Olatokun and Chinedu Nwafor, "The Social and Economic Dimensions of Internet Fraud in Nigeria," African Journal of Information Systems 4, no. 2 (2012): 72.

By the early 2000s, Nigeria had acquired an unfortunate international reputation for internet fraud, particularly the advance fee fraud scheme colloquially known as "419." Over time, the repertoire of cyber threats expanded considerably, encompassing phishing attacks, ransomware, business email compromise (BEC), identity theft, SQL injection, distributed denial-of-service (DDoS) attacks, and state-affiliated cyber espionage. The financial costs of cybercrime to Nigeria grew substantially, with estimates placing annual losses in the hundreds of millions of dollars by the 2010s.[4]

The passage of the Cybercrimes (Prohibition, Prevention, etc.) The 2015 act was the most consequential legislative step, representing the country's first comprehensive cybercrime statute. However, questions about the law's implementation, the capacity of enforcement agencies, and the broader structural conditions enabling cybercrime have persisted. This article examines the evolution of cyberspace and cybersecurity challenges in Nigeria between 2001 and 2022, evaluates the legislative framework, and identifies the structural barriers that continue to impede effective cyber governance.

Literature Review

Scholarship on cybersecurity in Nigeria has grown considerably since the early 2000s, though it remains concentrated in specific disciplinary silos - particularly law, computer science, and criminology. Makeri's work argues that the rapid expansion of internet access outpaced the development of regulatory infrastructure, creating a permissive environment in which cybercriminals could operate with relative impunity.[5] This argument aligns with broader

[4]E. E. A. Akpan, Critical Analysis of Cyber Security and Resilience in Nigeria, World Atlas Journal of Library and Information Science 5, no. 1 (2019): 10–11.
[5]Y. A. Makeri, "Cyber Security Issues in Nigeria and Challenges," International Journal of Advanced Research in Computer Science and Software Engineering 7, no. 4 (2017): 315.

scholarship on the regulatory gaps that accompany rapid technological diffusion in developing economies.[6]

Omodunbi *et al.* contribute a technically grounded analysis of cybercrime typologies in Nigeria, cataloguing detection and prevention challenges associated with increasingly sophisticated attack vectors such as social engineering, spear phishing, and advanced persistent threats.[7] Similarly, Ibikunle and Eweniyi foreground the structural dimension of Nigeria's cybersecurity deficit, pointing to the absence of a coherent national cybersecurity architecture during the critical early years of digital expansion.[8]

The socio-economic dimensions of cybercrime have been explored most thoroughly by Olatokun and Nwafor, who situate youth involvement in internet fraud within the structural context of unemployment, inequality, and the perceived inadequacy of legitimate economic opportunities. Their study suggests that punitive legal approaches, without corresponding investment in economic empowerment, are unlikely to substantially reduce cybercrime rates.[9]

Ajayi's analysis of cybercrime law enforcement provides a detailed account of the institutional and procedural obstacles that limit the effectiveness of existing legislation, including evidentiary challenges, judicial unfamiliarity with digital crimes, and failures in inter-agency coordination.[10] Akpan's broader study of cyber resilience adds an international comparative dimension, situating Nigeria's challenges within global trends and drawing lessons from more

[6]David S. Wall, Cybercrime: The Transformation of Crime in the Information Age (Cambridge: Polity Press, 2007), 37–42.
[7]B. A. Omodunbi et al., "Cybercrime in Nigeria: Analysis, Detection and Prevention," Journal of Engineering and Technology 1, no. 1 (2016): 38–41.
[8]F. Ibikunle and O. Eweniyi, "Approach to Cyber Security Issues in Nigeria: Challenges and Solutions," International Journal of Cognitive Research in Science, Engineering and Education 1, no. 1 (2013): 6–8.
[9]Olatokun and Nwafor, "Social and Economic Dimensions," 72–78.
[10]Emmanuel F. G. Ajayi, "Challenges to Enforcement of Cybercrime Laws and Policy in Nigeria," Journal of Internet and Information Systems 7, no. 1 (2016): 6–10.

advanced cybersecurity regimes in countries such as the United Kingdom, the United States, and South Africa.[11]

Methodology

This study adopts a historical and qualitative research methodology to examine the evolution of cybersecurity challenges in Nigeria between 2001 and 2022. The primary analytical method is content analysis, applied to a corpus of secondary sources including peer-reviewed academic articles, government policy documents, institutional reports, legislative texts, and credible online databases. Key primary documents examined include the National Cybersecurity Policy and Strategy of 2014, the Cybercrimes (Prohibition, Prevention, etc.) Act of 2015, and circulars and reports issued by the Central Bank of Nigeria, the Economic and Financial Crimes Commission, and the Nigerian Communications Commission.

International cybersecurity reports from organisations such as Interpol, the International Telecommunication Union (ITU), and the African Union were also consulted to provide a comparative regional and global perspective. A deliberate effort was made to triangulate findings across multiple source types, balancing governmental, academic, and civil society perspectives to produce a more nuanced and reliable account. The study's historical dimension involves a periodisation of Nigeria's digital development from 2001 through to the post-pandemic digital acceleration of 2021–2022.

Conceptual Framework: Cybersecurity, Cybercrime, and Cyberspace

Cyberspace is most usefully understood as a global domain encompassing the interconnected networks of digital infrastructure - including the internet, telecommunications

[11]Akpan, Critical Analysis of Cyber Security, 14–19.

networks, computer systems, and the data they process and transmit. Liarapoulos argues that the emergence of cyberspace as a distinct domain of human activity has fundamentally altered the conditions of both opportunity and threat, enabling new forms of communication and commerce while also providing new vectors for crime, espionage, and conflict.[12]

Cybersecurity, as defined by the ITU, refers to the ensemble of tools, policies, security concepts, safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies used to protect the cyber environment and the assets of organisations and users.[13] Makeri similarly emphasises that cybersecurity must be understood as a systemic challenge requiring coordinated responses across multiple societal levels.[14]

Cybercrime encompasses a broad range of offences in which computers or digital networks serve either as the instrument of criminal activity or as its target. Badamasi and Utulu identify three broad categories: cybercrimes in which the computer is the target (such as hacking and DDoS attacks), cybercrimes in which the computer is the tool (such as online fraud and identity theft), and cybercrimes in which digital content itself is the contraband.[15] Ibikunle and Eweniyi add that the boundaries between these categories have become increasingly blurred as attack methodologies grow more sophisticated.[16]

The classical framework for organising cybersecurity objectives around three pillars - confidentiality, integrity, and availability (the CIA triad) - provides a useful analytical lens. Confidentiality concerns the protection of information from unauthorised disclosure; integrity

[12]Andrew Liarapoulos, "Cybersecurity and the Information Revolution," Journal of Security Studies 12, no. 2 (2015): 131–133.
[13]Akpan, Critical Analysis of Cyber Security, 14.
[14]Makeri, "Cyber Security Issues in Nigeria," 214.
[15]B. Badamasi and S. C. A. Utulu, "Framework for Managing Cyber Crime Risks in Nigerian Universities," Conference on Information and Digital Technologies (2021): 855–856.
[16]Ibikunle and Eweniyi, "Approach to Cyber Security Issues," 4–6.

concerns the assurance that data has not been tampered with; and availability concerns ensuring that systems and data remain accessible to authorised users when needed. In the Nigerian context, threats to all three dimensions have been extensively documented across the financial, governmental, and critical infrastructure sectors.

The Evolution of Cyberspace in Nigeria, 2001–2022

- **Phase One: Liberalisation and Early Expansion (2001–2008)**

The telecommunications liberalisation of 2001, which ended the state monopoly of the Nigerian Telecommunications Limited (NITEL) and issued licences to private mobile operators, including MTN, Airtel (then Econet), and Globacom, was the catalytic event that launched Nigeria's mass digital experience. Within a few years, mobile telephony had penetrated all regions of the country, providing the first point of digital connectivity for millions of Nigerians.[17]

During this initial phase, Nigeria's cyber threat landscape was dominated by advance fee fraud. The "419" email scam, in which victims were solicited to advance funds in exchange for a promised share of a large sum, became globally notorious, generating significant diplomatic friction with Western governments and contributing to the blocklisting of Nigerian IP addresses by international financial institutions. However, these crimes were largely perpetrated by organised networks operating with minimal technical sophistication, exploiting the novelty and credulity of early internet users rather than exploiting vulnerabilities in technical systems.

- **Phase Two: Deepening Penetration and Diversifying Threats (2009–2015)**

The landing of the West Africa Cable System (WACS) and other undersea fibre-optic cables between 2009 and 2012 dramatically increased Nigeria's bandwidth capacity, reducing data

[17]Nigeria Communications Commission, Annual Report 2020, 12–15.

costs and enabling more Nigerians to access broadband internet. This period also witnessed a significant diversification and professionalisation of cybercrime. Nigerian cybercriminals began adopting more technically demanding methodologies, including phishing campaigns targeting banking customers, business email compromise schemes targeting corporate treasury departments, and malware and keyloggers to harvest financial credentials. International law enforcement agencies, including the FBI, began documenting sophisticated Nigerian cybercrime networks operating transnationally.[18]

- **Phase Three: Legislative Response and Ongoing Escalation (2015–2022)**

The passage of the Cybercrimes (Prohibition, Prevention) Act in May 2015 marked the beginning of a new phase in Nigeria's approach to cyber governance. The Act criminalised a wide range of cyber offences, established penalties for cybercriminals, created mechanisms for international cooperation, and mandated the establishment of a National Cyber Security Fund. Interpol's 2021 Africa Cyberthreat Assessment Report identified Nigeria as one of the continent's most significant sources of cyber threat activity while simultaneously recognising the government's growing institutional response.[19] Ransomware attacks on government and corporate systems, social engineering campaigns targeting remote workers, and fraud exploiting COVID-19 relief disbursements were among the most prominent incidents of this period.[20]

Nigeria's Legislative and Institutional Framework for Cybersecurity

[18]Sule Babayo et al., "Cyber Security and Cybercrime in Nigeria: Implication for National Security and Digital Economy," Journal of Intelligence and Cyber Security 4, no. 1 (2021): 5–7.
[19]Interpol, Africa Cyberthreat Assessment Report 2021 (Lyon: Interpol, 2021), 14–18.
[20]R. Sibe, "Cybercrime Convictions in Nigeria: Trends and Implications," Journal of Digital Security Studies 3, no. 2 (2022): 17–19.

Nigeria's legislative approach to cybersecurity has evolved through successive layers of policy and statute. The National Cybersecurity Policy and Strategy of 2014, developed with support from international partners and technical agencies, provided the first comprehensive articulation of Nigeria's cybersecurity objectives. The policy established a framework for protecting critical national information infrastructure (CNII), outlined responsibilities across government ministries and agencies, and set targets for public awareness, workforce development, and international cooperation. While it represented an important conceptual advance, critics noted that the Policy lacked binding force and clear accountability mechanisms.[21]

The Cybercrimes Act of 2015 addressed this gap by providing a statutory basis for prosecuting cybercrimes. Among its key provisions, the Act criminalised unauthorised access to computer systems, interception of electronic communications, cyber terrorism, identity theft, and cyberstalking. It also established provisions for the preservation of electronic evidence, mutual legal assistance in transnational cybercrime cases, and the levy of a 0.005 per cent cybersecurity tax on electronic transactions to fund the National Cyber Security Fund.[22, 23]

Implementation of the Act has been fraught with difficulties. Ajayi identifies several structural obstacles, including the limited forensic capacity of law enforcement agencies, the difficulty of establishing digital chains of evidence admissible in Nigerian courts, and the reluctance of financial institutions to cooperate fully with law enforcement due to reputational concerns.[24] The Office of the National Security Adviser (ONSA), designated as the coordinating

[21]Nigeria, National Cybersecurity Policy and Strategy (Abuja: Office of the National Security Adviser, 2014), 5–8.
[22]Ajayi, "Challenges to Enforcement," 7.
[23]Nigeria, Cybercrimes (Prohibition, Prevention, Etc.) Act (Abuja: Federal Government of Nigeria, 2015), sections 3–18.
[24]Ajayi, "Challenges to Enforcement," 8–10.

body for cybersecurity under the Policy, has faced resource constraints and inter-agency coordination challenges. The Economic and Financial Crimes Commission (EFCC), which bears primary responsibility for prosecuting cybercrime, has achieved notable convictions in high-profile cases but has struggled to address the broader ecosystem of lower-level cyber fraud.

The 2021 amendment to the Cybercrimes Act and the launch of a revised National Cybersecurity Policy in the same year represented efforts to address some of these gaps. The amendments introduced provisions targeting new threat categories, clarified evidentiary standards, and sought to strengthen coordination between the ONSA, EFCC, Nigerian Police Force, and the Central Bank of Nigeria. The revised Policy placed greater emphasis on protecting critical digital infrastructure in the financial, energy, and communications sectors, reflecting the growing recognition that cybersecurity is not merely a law enforcement issue but a national security and economic development imperative.

Structural Challenges to Effective Cybersecurity Governance in Nigeria

- **Inadequate Technological Infrastructure**

A fundamental challenge confronting Nigeria's cybersecurity effort is the underdevelopment of the digital infrastructure upon which effective cyber defence depends. Nigeria's cybersecurity architecture lacks the national-level Security Operations Centres (SOCs), threat intelligence platforms, and government-wide intrusion detection systems that characterise mature cyber regimes. The Computer Emergency Response Teams (CERTs) established at national and sectoral levels remain under-resourced and have limited reach beyond the formal banking sector.[25]

[25]Ibikunle and Eweniyi, "Approach to Cyber Security Issues," 8.

- **Weakness in Legal Enforcement Capacity**

The gap between legislative provision and operational enforcement is one of the most persistently documented features of Nigeria's cybersecurity landscape. Law enforcement agencies face acute deficits in digital forensics capacity. Prosecutorial success rates in cybercrime cases remain low relative to the volume of reported offences. Corruption within law enforcement, identified by Ajayi as a systemic challenge, further undermines investigative integrity and reduces the deterrent effect of legal sanctions.[26] The judiciary's limited familiarity with the technical dimensions of digital crime creates additional obstacles at the prosecution stage.

- **Shortage of Cybersecurity Professionals**

Nigeria faces a severe deficit of trained cybersecurity professionals. The educational system has been slow to incorporate cybersecurity into curricula at the undergraduate and professional levels. The emigration of skilled IT professionals to Europe, North America, and the Gulf states - a dimension of the broader "brain drain" affecting Nigeria's professional class - further depletes the domestic talent pool.[27] Government agencies and critical infrastructure operators consequently struggle to attract and retain personnel with the skills required to manage sophisticated cybersecurity environments.

- **Socio-Economic Drivers of Cybercrime**

The structural socio-economic conditions that predispose Nigerian youth to cybercrime have been well documented in the literature. Nigeria's youth unemployment rate, consistently above 40 per cent during the period under review, combined with deep inequality and the perceived corruption of legitimate pathways to prosperity, has created a social environment in which some

[26]Ajayi, "Challenges to Enforcement," 6–9.
[27]Makeri, "Cyber Security Issues in Nigeria," 214.

young people rationalise internet fraud as a response to systemic injustice. The cultural normalisation of cybercrime in some communities, reflected in popular music, social media culture, and the conspicuous consumption of successful fraudsters, has created social pressures that reinforce criminal behaviour patterns.[28]

- **Low Levels of Digital Literacy and Cybersecurity Awareness**

A large proportion of Nigeria's internet user population lacks the digital literacy necessary to protect themselves from common cyber threats. Phishing emails, fraudulent investment schemes, SIM swap attacks, and social engineering remain highly effective against Nigerian consumers and businesses alike, in part because public awareness campaigns have been limited in scope and impact. Financial literacy programs conducted by the Central Bank of Nigeria have made some progress in educating banking customers about fraud risks. Still, these efforts have not been sufficiently comprehensive or sustained to shift behaviour at scale.[29]

- **Reputational Damage and Its Consequences**

Nigeria's association with internet fraud has inflicted lasting reputational damage with tangible economic consequences. The fintech sector, one of Nigeria's most dynamic economic frontiers, faces particular challenges in accessing international payment networks and banking partnerships due to heightened perceptions of fraud risk. Idowu argues that this reputational deficit represents one of the highest hidden costs of Nigeria's cybercrime problem, with ramifications for foreign direct investment, e-commerce growth, and the country's integration into the global digital economy.[30]

- **Transnational Dimensions of Cybercrime Governance**

[28]Olatokun and Nwafor, "Social and Economic Dimensions," 74–76.
[29]Akpan, Critical Analysis of Cyber Security, 14–16.
[30]B. Y. Idowu, "Cyber Threats and National Security in Nigeria," National Defence College Journal (2013): 137.

Vol. 14 (Special Edition), No. 1, June 2025 p34-50 ISSN: 2315-8816
https://thecalabarhistoricaljournal.com/

A defining characteristic of cybercrime that makes it particularly resistant to unilateral national responses is its inherently transnational character. Nigerian cybercriminals have demonstrated a consistent ability to operate across borders, targeting victims in North America, Europe, and Asia while laundering proceeds through complex, multi-jurisdictional financial networks. Yar emphasises that cybercrime governance demands a global architecture of cooperation that the current patchwork of bilateral agreements and institutional linkages has not yet provided.[31]

Policy Recommendations

Sustained public investment in cybersecurity infrastructure is essential. This should encompass the establishment of a fully operational national CERT with round-the-clock monitoring capacity, the deployment of sectoral SOCs covering critical infrastructure in finance, energy, and communications, and the integration of national threat intelligence systems capable of providing early warning of emerging attacks. The National Cyber Security Fund established under the 2015 Act should be adequately capitalised and subjected to robust oversight to ensure that levies collected from financial institutions translate into concrete security improvements.[32]

Building human capital in cybersecurity must be treated as a strategic national priority. This requires curricular reform at tertiary institutions to incorporate cybersecurity as a distinct discipline, the creation of government-funded scholarship and training programs to develop forensic investigators and security analysts, and competitive compensation packages for public-sector cybersecurity roles to reduce the outflow of talent to the private sector and overseas.

[31]Majid Yar, Cybercrime and Society (London: Sage Publications, 2013), 52–55.
[32]Interpol, Africa Cyberthreat Assessment Report 2021, 20–25.

The legal and institutional framework requires further strengthening. Greater specificity is needed in areas such as cloud computing jurisdiction, data breach notification obligations, and the regulation of cryptocurrency platforms, which are increasingly used for money laundering. Judicial training programs on digital evidence and cybercrime prosecution should be institutionalised. The coordination mechanisms between the ONSA, EFCC, CBN, and other relevant agencies must be formalised and adequately resourced.

Addressing the socio-economic roots of cybercrime demands integration with broader youth development and employment policies. Targeted programs that provide legitimate technology skills training and entrepreneurship support to at-risk youth populations can redirect talent and energy toward productive ends. Nigeria must also deepen its engagement in international cybersecurity cooperation frameworks. Ratification of the African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention), alongside enhanced bilateral arrangements with key partners, would strengthen Nigeria's ability to pursue cybercriminals across borders and benefit from shared threat intelligence.[33]

Conclusion

The evolution of cyberspace in Nigeria between 2001 and 2022 represents one of the most consequential dimensions of the country's recent history. From the cautious early steps of telecommunications liberalisation to the dynamic, complex digital ecosystem of the post-pandemic era, Nigeria's digital transformation has generated enormous economic and social opportunities while simultaneously creating a sophisticated and resilient landscape of cyber threats. The country's experience illustrates, with particular clarity, the central paradox of the digital age: that

[33]Wall, Cybercrime, 37–42; Yar, Cybercrime and Society, 52–55.

the same technologies that enable development, connectivity, and innovation also create new vulnerabilities and expand the possibilities for criminal exploitation.

Nigeria's legislative response, culminating in the Cybercrimes Act of 2015 and its subsequent revision, represents a genuine and meaningful effort to establish a governance framework adequate to these challenges. Yet the gap between legislative intent and operational reality remains wide. Persistent deficits in enforcement capacity, digital infrastructure, human capital, and inter-agency coordination limit the law's effectiveness. The socio-economic conditions that drive youth into cybercrime continue to operate largely unaddressed by cybersecurity policy. And the transnational character of modern cybercrime consistently outpaces the national frameworks designed to contain it.

Achieving genuine cyber resilience in Nigeria will require a fundamental reconceptualisation of cybersecurity as not merely a technical or legal challenge but a complex governance problem requiring sustained political commitment, inter-sectoral collaboration, and long-term investment. Nigeria's size, influence, and technological dynamism position it as a potential leader in African cybersecurity governance. Realising that potential demands urgency, ambition, and the sustained coordination of governmental, institutional, and civil society efforts in the service of a digitally secure national future.

Bibliography

Ajayi, Emmanuel F. G. "Challenges to Enforcement of Cybercrime Laws and Policy in Nigeria." *Journal of Internet and Information Systems* 7, no. 1 (2016): 1–12.

Akpan, E. E. A. Critical Analysis of Cyber Security and Resilience in Nigeria. World Atlas *Journal of Library and Information Science* 5, no. 1 (2019): 10–22.

Babayo, Sule, et al. "Cyber Security and Cybercrime in Nigeria: Implications for National Security and Digital Economy." *Journal of Intelligence and Cyber Security* 4, no. 1 (2021): 1–18.

Badamasi, B., and S. C. A. Utulu. "Framework for Managing Cyber Crime Risks in Nigerian Universities." *Conference on Information and Digital Technologies* (2021): 850–862.

Central Bank of Nigeria. *Circular to Banks and Payment Service Providers on Cybersecurity Threats.* Abuja: CBN, June 25, 2018.

Ibikunle, F., and O. Eweniyi. "Approach to Cyber Security Issues in Nigeria: Challenges and Solutions." *International Journal of Cognitive Research in Science, Engineering and Education* 1, no. 1 (2013): 1–12.

Idowu, B. Y. "Cyber Threats and National Security in Nigeria." *National Defence College Journal* (2013): 130–145.

Interpol. *Africa Cyberthreat Assessment Report 2021*. Lyon: Interpol, 2021.

Liarapoulos, Andrew. "Cybersecurity and the Information Revolution." *Journal of Security Studies* 12, no. 2 (2015): 128–148.

Makeri, Y. A. "Cyber Security Issues in Nigeria and Challenges." *International Journal of Advanced Research in Computer Science and Software Engineering* 7, no. 4 (2017): 210–220.

Nigeria. *Cybercrimes (Prohibition, Prevention, Etc.) Act.* Abuja: Federal Government of Nigeria, 2015.

Nigeria. *National Cybersecurity Policy and Strategy*. Abuja: Office of the National Security Adviser, 2014.

Nigeria Communications Commission. *Annual Report 2020*. Abuja: NCC, 2020.

Olatokun, Wole, and Chinedu Nwafor. "The Social and Economic Dimensions of Internet Fraud in Nigeria." *African Journal of Information Systems* 4, no. 2 (2012): 68–94.

Omodunbi, B. A., et al. "Cybercrime in Nigeria: Analysis, Detection and Prevention." *Journal of Engineering and Technology* 1, no. 1 (2016): 37–44.

Sibe, R. "Cybercrime Convictions in Nigeria: Trends and Implications." *Journal of Digital Security Studies* 3, no. 2 (2022): 15–28.

Tamakar, A., and P. Bhupesh. "Cyber Security Threats and Countermeasures: A Review." *Turkish Journal of Computer and Mathematics Education* 9, no. 3 (2018): 1402–1410.

Wall, David S. *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Polity Press, 2007.

Yar, Majid. *Cybercrime and Society*. London: Sage Publications, 2013.

Yusuf, H. "The Information Revolution and Cybersecurity Challenges." *Journal of Global Security Studies* 2, no. 3 (2017): 128–148.