International Journal of Advanced Technology and Social Sciences (IJATSS)
Vol.4, No.3, 2026: 197-214

A Critical Analysis of Cybercrime Trends in Nigeria (2018–2025): Patterns, Drivers, and Policy Responses

Julius Bolade Anjorin
Miva Open University, Jabi, Abuja, FCT
Corresponding Author: Julius Bolade Anjorin; juliusanjorin@gmail.com

A R T I C L E I N F O

Keywords: Cybercrime Trends, Nigeria, Digital Forensics, Cybersecurity Policy, Financial Crime, Business Email Compromise

Received : 5 December
Revised : 23 January
Accepted: 23 February

A B S T R A C T

The digital transformation of Nigeria's economy over the past decade has been accompanied by a parallel escalation in cybercriminal activity, presenting complex challenges for policymakers, law enforcement agencies, and citizens alike. This study examines the evolution of cybercrime trends in Nigeria between 2018 and 2025, with attention to the shifting modus operandi of cybercriminals, the socioeconomic and technological drivers facilitating these offences, and the adequacy of institutional and legislative responses. The period witnessed a marked transition from crude advance-fee fraud schemes toward sophisticated tactics including business email compromise, ransomware attacks on corporate and governmental networks, and the weaponization of social media platforms for sextortion and cyberbullying. Financial sector losses attributed to cyber-enabled fraud exceeded ₦56 billion between 2021 and 2024, though underreporting suggests the actual figure may be substantially higher. The study identifies key drivers including the expanding attack surface created by rapid mobile money adoption, persistent infrastructural deficits in digital forensic capabilities, and the emergence of transnational organized criminal networks operating within and beyond Nigeria's borders. Policy responses examined include the Cybercrimes (Amendment) Act 2024, the establishment of the Nigeria Data Protection Commission, and institutional coordination mechanisms such as the Joint Case Team on Cybercrimes. The findings suggest that while legislative frameworks have strengthened considerably, implementation deficits, capacity constraints, and limited international cooperation continue to impede effective cybercrime control. The study recommends enhanced investment in digital forensic infrastructure, mandatory cybersecurity curricula at tertiary institutions, and the development of a comprehensive national cybersecurity strategy aligned with evolving threat landscapes

DOI: https://doi.org/10.59890/ijatss.v4i2.182
E-ISSN: 3026-2410
https://aprmultitechpublisher.my.id/index.php/ijatss/index

INTRODUCTION

The expansion of digital technologies across Nigerian society has fundamentally transformed the nature of economic transactions, social communication, and governmental service delivery. Since the liberalization of the telecommunications sector in the early 2000s, internet penetration has grown exponentially, with the Nigeria Communications Commission reporting active mobile subscriptions exceeding 220 million by the fourth quarter of 2024. This digital revolution has undoubtedly yielded substantial developmental dividends, positioning Nigeria as one of Africa's most vibrant digital economies and attracting significant foreign investment in financial technology, e-commerce, and related sectors.

However, this connectivity has also created unprecedented opportunities for criminal exploitation. The same digital infrastructure that enables seamless banking transactions and cross-border commerce has proven equally accessible to actors whose intentions are decidedly less benign. As Craig Jones, former Director of Cybercrime at INTERPOL, observed in a recent interview, the expansion of Africa's digital footprint, particularly through mobile money platforms, has rendered the continent increasingly susceptible to cyberattacks, with Nigerian institutions featuring prominently among the targets (Jones, 2025). The INTERPOL Africa Cyberthreat Assessment Report estimates that cyber incidents have cost the continent over $3 billion since 2019, a figure that many analysts consider conservative given significant underreporting (Jones, 2025).

LITERATURE REVIEW

The Nigerian context presents complexities. Unlike developed economies where cybercrime often represents an extension of existing criminal enterprises, Nigeria's experience has been shaped by unique historical, economic, and social factors. The notorious "419" advance-fee fraud, which gained international notoriety during the 1990s, established a template for online deception that has since evolved considerably. Contemporary Nigerian cybercriminals, often colloquially referred to as "Yahoo Boys," have demonstrated remarkable adaptability, moving beyond crude email solicitations toward sophisticated schemes that exploit weaknesses in corporate payment systems, manipulate financial markets through misinformation campaigns, and leverage social engineering techniques honed through years of practice.

The period between 2018 and 2025 represents a particularly significant phase in this evolutionary trajectory. These years witnessed several transformative developments: the rapid expansion of mobile money services following the Central Bank of Nigeria's regulatory reforms, the COVID-19 pandemic-induced acceleration of digital adoption across all sectors, the emergence of cryptocurrencies as both a payment mechanism for cybercriminals and a target for exploitation, and the passage of amended legislation intended to strengthen Nigeria's cybercrime control architecture. Understanding the patterns that emerged during this period, the factors that drove them, and the effectiveness of policy responses constitutes an essential scholarly endeavour with significant practical implications.

A growing body of literature has examined various dimensions of Nigeria's cybercrime challenge. Afolabi and Dogi's recent study of Economic and Financial Crimes Commission intelligence operations in the Federal Capital Territory highlighted the critical role of well-executed intelligence gathering in enhancing investigation efficiency, while also noting persistent public concern regarding cybercrime's implications for national security (Afolabi & Dogi, 2025). Sibe and Kaunert's comprehensive investigation into digital forensic readiness across Nigerian financial crime agencies revealed substantial deficiencies in forensic resources and capabilities, deficiencies that directly impact case processing and conviction rates (Sibe & Kaunert, 2024). Their work, published in 2024, represents one of the most systematic examinations to date of the institutional constraints hampering effective cybercrime control.

Nevertheless, significant gaps remain in the scholarly understanding of how cybercrime patterns have evolved during this critical period, particularly regarding the interplay between technological change, criminal innovation, and policy adaptation. This study seeks to address these gaps through a longitudinal analysis of available data, situating observed trends within broader theoretical frameworks concerning the relationship between digital transformation and criminal opportunity structures. By examining not only what has occurred but also why it has occurred and how institutions have responded, the analysis aims to contribute both to academic knowledge and to policy development.

The theoretical orientation adopted here draws primarily on routine activity theory, which posits that crime occurs when motivated offenders, suitable targets, and the absence of capable guardianship converge in time and space. In the digital context, this framework requires adaptation to account for the distinctive characteristics of virtual environments, where spatial and temporal boundaries operate differently. Nevertheless, the theory's emphasis on opportunity structures provides valuable insights into how Nigeria's digital transformation has simultaneously created new targets, attracted motivated offenders, and, in some respects, weakened traditional guardianship mechanisms. The analysis also engages with scholarship on transnational organized crime, recognizing that contemporary Nigerian cybercrime increasingly operates across borders, involving collaboration with foreign actors and targeting victims worldwide.

This study proceeds as follows. Section 2 outlines the methodological approach, including data sources and analytical techniques. Section 3 presents the empirical findings regarding cybercrime patterns and trends, organized by offence type and sectoral impact. Section 4 analyses the drivers underlying these trends, examining technological, economic, social, and institutional factors. Section 5 evaluates the policy responses that have emerged during the study period, assessing their strengths and limitations. Section 6 discusses the implications of these findings for theory and practice, while Section 7 concludes with recommendations for future action.

METHODOLOGY

This study adopts a qualitative documentary research design supplemented by quantitative trend analysis of publicly available secondary data. The decision to rely on secondary sources reflects both practical considerations and the nature of the phenomenon under investigation. Primary data collection on cybercrime faces well-documented challenges, including issues of access to offender populations, reluctance among victims to report offences, and the reluctance of law enforcement agencies to share sensitive operational data. Secondary sources, while presenting their own limitations, offer the advantage of covering extended time periods and providing data collected through consistent methodologies.

Data Sources

Data were drawn from multiple sources to enable triangulation and cross-verification. The primary sources included:

Reports from Law Enforcement and Regulatory Agencies: Annual reports and periodic publications from the Nigeria Police Force National Cybercrime Centre (NPF-NCCC), the Economic and Financial Crimes Commission (EFCC), and the Independent Corrupt Practices and Other Related Offences Commission (ICPC) were systematically reviewed. These documents contain statistics on reported offences, arrests, prosecutions, and convictions, though reporting formats varied across agencies and over time.

Data from Banking and Financial Sector: The Nigeria Deposit Insurance Corporation's annual reports on bank frauds and forgeries provided detailed information on financial losses attributable to cyber-enabled crime, including breakdowns by fraud type and channel. Additional data were obtained from the Central Bank of Nigeria's publications on electronic payment system trends and fraud incidence.

Telecommunications Industry Data: The Nigeria Communications Commission's subscriber and internet penetration statistics were used to contextualize cybercrime trends within broader patterns of digital adoption. These data enabled analysis of the relationship between connectivity expansion and crime incidence.

Legislative and Policy Documents: Primary legal materials including the Cybercrimes (Prohibition, Prevention, Etc.) Act 2015, the Cybercrimes (Amendment) Act 2024, the Nigeria Data Protection Regulation 2019, and the Nigeria Data Protection Act 2023 were analyzed to assess the evolution of the legal framework. Accompanying explanatory memoranda and legislative debates provided insight into policy intent.

Media and Industry Reports: Given the limitations of official data, particularly regarding underreporting, news media accounts and industry publications were consulted to identify incidents and trends that may not have been captured in official statistics. These sources were treated with appropriate caution and used primarily for illustrative purposes and triangulation.

Data Extraction and Analysis

Data extraction followed a structured protocol designed to ensure consistency across sources. For quantitative data, information on offence types, geographical distribution, demographic characteristics of offenders where

available, financial losses, and case outcomes was recorded in a structured database. Temporal coding enabled analysis of trends across the 2018 – 2025 period. For qualitative data from reports and policy documents, thematic analysis was employed to identify recurring patterns in the framing of cybercrime challenges and policy responses.

Limitations

Several limitations warrant acknowledgment. Official crime statistics are notoriously unreliable as measures of actual crime incidence, given substantial underreporting by victims and recording practices that may vary across agencies and over time. This is particularly acute for cybercrime, where shame, fear of reprisal, or lack of confidence in law enforcement may deter reporting. The data presented should therefore be understood as reflecting minimum levels of activity rather than comprehensive counts. Additionally, changes in reporting systems and classification practices over the study period complicate longitudinal comparisons. The analysis addresses these limitations through triangulation across sources and cautious interpretation of trends, but the possibility of artefactual findings cannot be eliminated.

RESULTS

Overall Trajectory and Scale

The period under examination witnessed a substantial increase in both the volume and sophistication of cybercriminal activity targeting Nigerian individuals, businesses, and government institutions. Official statistics from the Nigeria Police Force National Cybercrime Centre indicate that reported cybercrime incidents rose from approximately 3,800 in 2018 to over 16,500 in 2024, representing a more than fourfold increase across the seven-year period. However, these figures almost certainly understate the true scale, as victimization surveys conducted by the NOIPolls in collaboration with cybersecurity firms have consistently suggested that fewer than one in five cybercrime victims report their experiences to law enforcement authorities.

The Attorney-General of the Federation, Lateef Fagbemi, SAN, characterized the situation as a "national emergency" during the second National Consultations on the Cybercrime and Cybersecurity Legal Framework in October 2025 (The Guardian Nigeria, 2025). Citing recent data, Fagbemi noted that Nigeria now ranks fifth globally in terms of cybercrime prevalence based on first quarter 2025 figures, with the country experiencing an average of 4,388 weekly cyber-attacks and estimated annual economic losses of approximately $500 million (The Guardian Nigeria, 2025). These figures, while alarming, require contextualization within Nigeria's broader economic landscape; relative to the size of the economy, cybercrime losses, though substantial, remain lower than in several developed nations with more deeply digitized economies.

Evolution of Offence Types

The composition of cybercrime in Nigeria has undergone significant transformation during the study period. Table 1 presents reported offences by category for selected years, illustrating these shifts.

Table 1. Reported Cybercrime Offences by Category, Nigeria 2018–2024 (Selected Years)

Offence Category	**2018**	**2020**	**2022**	**2024**	**% Change 2018–2024**
Advance fee fraud	1,842	1,956	1,873	1,621	-12.0%
Phishing	342	891	1,567	2,843	+731.3%
Business Email Compromise	156	643	1,892	3,167	+1,930.1%
Ransomware	23	187	643	892	+3,778.3%
Identity theft	445	667	892	1,234	+177.3%
Cyberstalking/harassment	287	543	987	1,456	+407.3%
Sextortion	45	234	678	1.023	+2,173.3%
Unauthorized cryptocurrency transactions	NA	NA	234	567	NA
Others	660	879	1,234	2,897	+338.9%
Total	**3,800**	**6,000**	**10,000**	**15,700**	**+313.2%**

Source: Compiled from Nigeria Police Force National Cybercrime Centre annual reports, 2018–2024

Several observations emerge from the above data. First, traditional advance-fee fraud, while remaining prevalent, has declined in relative terms, constituting a diminishing proportion of overall cybercrime. This does not necessarily indicate a reduction in absolute prevalence but rather reflects the more rapid growth of other offence types. Second, business email compromise (BEC) and phishing have experienced explosive growth, with BEC incidents increasing nearly twentyfold across the period. This pattern aligns with global trends and reflects the increasing sophistication of Nigerian cybercriminal networks, which have identified corporate payment systems as particularly lucrative targets (Jones, 2025).

The emergence of sextortion as a significant offence category deserves attention. The Attorney-General noted during the October, 2025 consultations that nearly 60 percent of cybercrime victims in Nigeria are under 30 years of age, with sextortion featuring prominently among offences affecting young people (Federal Ministry of Justice, 2025; The Guardian Nigeria, 2025). This trend has been linked to the proliferation of social media platforms and dating applications, which provide offenders with both a hunting ground for potential victims and a mechanism for establishing the trust necessary to solicit compromising material.

Ransomware attacks, while still less common than in some other jurisdictions, have increased substantially, with high-profile incidents affecting financial institutions, healthcare facilities, and government agencies. The ransomware attack on a major Nigerian bank in 2023, which temporarily disrupted customer access to funds and reportedly resulted in substantial financial losses, illustrated the vulnerability of critical infrastructure to this form of attack. Craig Jones's observation that ransomware can cause particularly severe harm in healthcare settings, potentially endangering lives through system shutdowns, underscores the gravity of this threat (Jones, 2025).

Sectoral Distribution of Impact

The impact of cybercrime has not been evenly distributed across economic sectors. The financial services industry has borne the brunt of attacks, reflecting both its attractiveness as a target and its extensive digital footprint. Table 2 presents data on bank fraud losses attributed to cyber-enabled channels.

Table 2. Bank Fraud Losses Attributable to Cyber-Enabled Channels, Nigeria 2018–2024

Year	Number of Reported Fraud Cases	Amount Involved (₦ million)	Actual Loss (₦ million)	Primary Channels
2018	25,043	8.42	5.12	ATM, Web
2019	37,817	12.65	7.89	Web, Mobile
2020	52,285	18.93	11.34	Mobile, POS, Web
2021	68,945	24.67	14.89	Mobile, POS, BEC
2022	71,689	31.56	18.23	Mobile, POS BEC
2023	78,342	42.89	24.67	BEC, Mobile, POS
2024	85,671	56.34	31.89	BEC, Mobile, Crypto

Source: Nigeria Deposit Insurance Corporation Annual Reports, 2018–2024

The data reveal a consistent upward trajectory in both the number of reported fraud cases and the associated financial losses. Particularly notable is the acceleration in losses during the latter half of the study period, with actual losses increasing from ₦14.89 billion in 2021 to ₦31.89 billion in 2024. This pattern coincides with the increased prevalence of business email compromise and the growing use of cryptocurrency channels for fraud proceeds. The Nigeria Deposit Insurance Corporation's reports indicate that mobile channels have consistently featured among the primary vectors for fraud, reflecting the centrality of mobile money in Nigeria's financial landscape and, as Jones noted, the susceptibility of mobile phone-based systems to malware and SIM-swapping attacks (Jones, 2025).

Beyond the financial sector, government institutions have emerged as significant targets. The Joint Task Force on Cybercrime reported a 156 percent increase in attacks on government networks between 2020 and 2023, with incidents ranging from website defacement to more sophisticated attempts to penetrate sensitive databases. The motivations behind these attacks appear mixed, encompassing politically motivated hacktivism, financial crime targeting government payment systems, and, in some cases, state-sponsored espionage, though the latter remains difficult to verify given classification constraints.

Geographical Distribution

Cybercrime in Nigeria exhibits distinct geographical patterns that reflect the uneven distribution of digital infrastructure, economic opportunity, and law enforcement capacity. Lagos State, as the commercial nerve centre and host to the nation's largest concentration of financial institutions and technology companies, accounts for the highest absolute number of reported cybercrime incidents. The

Federal Capital Territory, Abuja, and Ogun State follow, reflecting their economic significance and proximity to Lagos.

However, a focus on reported incidents risks obscuring the geography of cybercriminal activity, which often differs from the geography of victimization. Many perpetrators of cybercrime operate from locations far removed from their victims, exploiting the anonymity afforded by digital communications. Afolabi and Dogi's study of EFCC intelligence operations in the Federal Capital Territory highlighted the concentration of cybercriminal activity in certain neighbourhoods of Abuja, where clusters of young men engage in various forms of online fraud (Afolabi & Dogi, 2025). Similar patterns have been observed in Ibadan, Port Harcourt, and Benin City, with the latter achieving notoriety as a hub for Yahoo Boys.

Offender Characteristics

Available data on offender characteristics, drawn primarily from arrest and prosecution records, must be interpreted cautiously given potential biases in enforcement patterns. Nevertheless, consistent patterns emerge across multiple studies and data sources. Offenders are predominantly male, typically aged between 18 and 35, and often possess secondary or tertiary education. Sibe and Kaunert's analysis of cybercrime caseloads found that a substantial proportion of convicted offenders had completed at least secondary schooling, with many having attended universities or polytechnics (Sibe & Kaunert, 2024).

This educational profile complicates simplistic narratives that attribute cybercrime to poverty or lack of opportunity. While economic pressures undoubtedly play a role, the skills required for sophisticated cybercrime operations, including social engineering, technical proficiency, and in some cases programming ability, suggest that many offenders possess human capital that could, under different circumstances, be directed toward legitimate employment. The phenomenon has been characterized by some observers as a form of "criminal innovation" emerging at the intersection of limited legitimate opportunities and abundant illicit ones.

The transnational dimension of Nigerian cybercrime warrants emphasis. As Craig Jones noted, criminal groups in Africa have become increasingly sophisticated, forming business-like enterprises and collaborating with foreign actors who travel to Nigeria to work alongside local groups (Jones, 2025). This internationalization of Nigerian cybercrime has significant implications for enforcement, requiring coordination across jurisdictions and complicating investigation and prosecution efforts.

Drivers of Cybercrime Trends

Understanding the factors that have shaped the cybercrime patterns documented above requires analysis across multiple levels, from macro-level structural conditions to micro-level individual motivations. The drivers identified here should be understood as interconnected rather than discrete, with each reinforcing and amplifying the others.

Technological Drivers

The expansion of Nigeria's digital infrastructure has fundamentally altered the opportunity structure for cybercrime. Internet penetration increased from approximately 47 percent of the population in 2018 to over 75 percent by

2024, according to Nigeria Communications Commission data. This connectivity, while socially and economically beneficial, has dramatically expanded the pool of potential victims accessible to cybercriminals. Every new internet user represents a potential target, and the rapid pace of adoption has outstripped the development of digital literacy and cybersecurity awareness.

The proliferation of mobile money has been particularly significant. Nigeria's fintech sector has experienced explosive growth, with mobile money transactions increasing from ₦2.3 trillion in 2018 to over ₦18.7 trillion in 2024. This growth has been accompanied by a corresponding increase in mobile-enabled fraud. The susceptibility of mobile platforms to malware, SIM-swapping, and social engineering attacks creates vulnerabilities that cybercriminals have proven adept at exploiting. Jones's observation that mobile phones constitute "the backbone of the African region" for money transfer underscores the centrality of this vector (Jones, 2025).

The emergence of cryptocurrencies has introduced additional complexities. Cryptocurrencies offer cybercriminals mechanisms for receiving payments that operate outside traditional financial systems, complicating efforts to trace and recover funds. The Cybercrimes (Amendment) Act 2024 introduced specific provisions addressing unauthorized cryptocurrency transactions, reflecting legislative recognition of this challenge (Onibokun & Co, 2025; Uche, 2025). However, the inherently borderless nature of cryptocurrency systems means that domestic legislative responses alone cannot fully address the issue.

Economic Drivers

Economic conditions have undoubtedly contributed to the prevalence of cybercrime, though the relationship is more complex than simple deprivation models suggest. Nigeria has experienced persistent economic challenges during the study period, including slow growth, high youth unemployment, and inflationary pressures that have eroded living standards. The National Bureau of Statistics reported youth unemployment rates exceeding 42 percent in 2023, with particularly acute conditions among university graduates.

For some young Nigerians facing limited legitimate economic opportunities, cybercrime presents an attractive alternative. The potential returns from successful fraud operations can far exceed what is available through formal employment, particularly for those without connections to secure well-paying positions. This economic calculus is reinforced by peer effects within communities where cybercrime has become established; as Afolabi and Dogi noted, the normalization of cybercrime within certain youth subcultures creates powerful social pressures toward participation (Afolabi & Dogi, 2025).

However, it would be a mistake to reduce Nigerian cybercrime to a simple function of economic desperation. Many offenders possess skills and educational qualifications that would enable legitimate employment, suggesting that factors beyond economic necessity are at play. The prestige associated with successful cybercriminals in some communities, the thrill of outsmarting authorities, and the desire for rapid wealth accumulation in a society where visible consumption carries significant social weight all contribute to the attraction of cybercrime.

Institutional and Enforcement Drivers

The capacity of Nigerian institutions to prevent, investigate, and prosecute cybercrime has consistently lagged the sophistication of offenders. Sibe and Kaunert's comprehensive study of digital forensic readiness across Nigerian financial crime agencies identified substantial deficiencies in resources, training, and infrastructure (Sibe & Kaunert, 2024). Their findings revealed that many investigators lack access to basic forensic tools, that training in digital evidence handling is often inadequate, and that case backlogs contribute to lengthy pretrial detention and low conviction rates.

These capacity constraints have multiple dimensions. At the individual level, the shortage of trained digital forensic examiners means that many cases proceed without thorough technical investigation. At the organizational level, inter-agency competition and coordination failures impede information sharing and collaborative case development. The Solicitor-General of the Federation, Beatrice Jedy-Agba, emphasized during the October 2025 consultations that coordination requires "all institutions and sectors to work hand in hand with strategies guided by data, knowledge, and best practices" (Federal Ministry of Justice, 2025). Yet achieving such coordination has proven challenging in practice.

Legislative frameworks, while improving, have also presented challenges. The Cybercrimes Act 2015, groundbreaking at the time of its enactment, struggled to keep pace with technological change. The 2024 amendments addressed some deficiencies, introducing provisions on cryptocurrency transactions and strengthening penalties for certain offences. However, as critics have noted, some amendments, particularly those expanding surveillance powers and criminalizing "false" or "misleading" posts, raise concerns about potential misuse and their impact on fundamental rights (Onibokun & Co, 2025; Uche, 2025). The challenge of balancing security imperatives with rights protections remains incompletely resolved.

International cooperation, essential given the transnational character of much cybercrime, has been inconsistent. While Nigeria has participated in INTERPOL operations and benefited from capacity-building initiatives, the absence of a comprehensive mutual legal assistance framework with key partner countries continues to impede cross-border investigations. The Attorney-General's reference to Nigeria's alignment with the Budapest Convention and the United Nations Convention on Cybercrime (2024) signals intention to strengthen international cooperation, but translating intention into operational reality requires sustained effort (Federal Ministry of Justice, 2025).

Social and Cultural Drivers

Social and cultural factors have received less scholarly attention than economic or institutional drivers, yet they appear significant in shaping cybercrime patterns. The phenomenon of the "Yahoo Boy" has achieved cultural salience beyond the realm of crime, featuring in popular music, films, and social media discourse. This cultural embedding both reflects and reinforces the normalization of cybercrime within certain youth subcultures.

The celebration of material wealth in popular culture, combined with narratives of rapid success through non-traditional means, creates a cultural environment in which cybercrime can appear as a legitimate pathway to social mobility. The ostentatious consumption displayed by successful offenders in some communities, including luxury cars, designer clothing, and prominent social media presence, serves as advertisement for the criminal lifestyle. Counter-narratives emphasizing the risks and consequences of cybercrime, including arrest, imprisonment, and the harm caused to victims, struggle to achieve comparable visibility.

Intergenerational dynamics also play a role. Parents and elders in some communities lack digital literacy, limiting their ability to monitor and guide young people's online activities. The Attorney-General's call for parents to "learn to protect their data, report suspicious activity, and use technology responsibly" reflects recognition that effective prevention requires engagement across generations.

Policy Responses and Evaluation

The period under examination witnessed significant evolution in Nigeria's policy and legislative response to cybercrime. This section analyses key developments, assessing their strengths and limitations.

Legislative Developments

The Cybercrimes (Prohibition, Prevention, Etc.) Act 2015 represented Nigeria's first comprehensive legislative response to cybercrime, establishing a legal framework for offences including hacking, identity theft, cyberstalking, and online fraud. The Act created institutional mechanisms including the office of the National Security Adviser's cybersecurity coordination and the Computer Emergency Response Team. For its time, the legislation was forward-looking, addressing a range of offences and providing for international cooperation (Onibokun & Co, 2025).

By the early 2020s, however, the limitations of the 2015 Act had become apparent. Technological change had outpaced legislative provisions, with emerging threats including ransomware and cryptocurrency fraud inadequately addressed. Enforcement challenges, including limited technical capacity among investigators and prosecutors, further constrained effectiveness. The Cybercrimes (Amendment) Act 2024 sought to address these gaps through several key reforms.

The expanded surveillance powers have proven particularly controversial. While proponents argue that the ability to intercept communications without prior judicial authorization in urgent cases is necessary for effective law enforcement, civil society organizations including Paradigm Initiative have expressed concern about potential misuse and the adequacy of safeguards (Federal Ministry of Justice, 2025). Gbenga Sesan, Executive Director of Paradigm Initiative, has advocated for civil society inclusion as "co-creators" in digital policy-making, suggesting that current consultation processes may not adequately incorporate rights perspectives (Federal Ministry of Justice, 2025).

The provisions on online speech have also attracted criticism. The criminalization of "false" or "misleading" posts, coupled with requirements for social media platforms to remove "offensive" content promptly, raises questions about definitional clarity and the potential for content-based censorship. During parliamentary debates, some legislators expressed concern that these provisions could be weaponized against journalists and political opponents, though supporters argued that robust protections for free expression would prevent such misuse (Uche, 2025).

Institutional Developments

Alongside legislative reform, the study period witnessed institutional developments aimed at strengthening cybercrime control capacity. The Nigeria Police Force National Cybercrime Centre (NPF-NCCC) has expanded its operations, establishing dedicated cybercrime units across multiple states and developing specialized investigative capabilities. The Centre's participation in international operations, including INTERPOL-coordinated actions against cybercriminal networks, has enhanced Nigeria's engagement with global law enforcement partners.

The establishment of the Nigeria Data Protection Commission (NDPC) under the Nigeria Data Protection Act 2023 represents a significant institutional innovation. Building on the foundation of the Nigeria Data Protection Regulation 2019, the NDPC provides dedicated oversight of data protection compliance, with powers to investigate breaches, issue guidance, and impose penalties. This institutionalization of data protection governance aligns Nigeria more closely with international standards and creates mechanisms for addressing privacy dimensions of cybercrime (Onibokun & Co, 2025).

The Joint Case Team on Cybercrimes (JCTC), inaugurated in 2025, exemplifies efforts to enhance inter-agency coordination. Bringing together the Ministry of Justice, law enforcement agencies, digital forensics experts, and the judiciary, the JCTC aims to streamline investigation and prosecution processes. The Attorney-General described the JCTC as Nigeria's "operational bridge for international cooperation through the 24/7 Network under the Budapest Convention and the Mutual Legal Assistance framework" (Federal Ministry of Justice, 2025). Whether this mechanism can overcome historical coordination challenges remains to be seen, but its establishment represents recognition of the coordination imperative.

Capacity-Building Initiatives

Significant investments in capacity building have occurred, though questions persist regarding their sufficiency and sustainability. The Attorney-General's reference during the October, 2025 consultations to the evolution of Nigeria's cybercrime capabilities, from a "shipping container with three people" to a "purpose-built three-storey building in Abuja" (Jones, 2025), illustrates the physical infrastructure improvements that have occurred. Training programs for investigators, prosecutors, and judges have expanded, supported by international partners including UNODC, the Council of Europe, and bilateral donors (Federal Ministry of Justice, 2025).

However, Sibe and Kaunert's research suggests that capacity deficits remain substantial. Their assessment of digital forensic readiness across Nigerian

financial crime agencies revealed gaps in equipment, training, and standard operating procedures that directly impact case processing (Sibe & Kaunert, 2024). They argue that while some progress has been made, the scale of the challenge requires more systematic and sustained investment than has yet occurred.

Public awareness and education represent another dimension of capacity building. The annual Cybercrimes Awareness Campaign, which included an awareness walk through Abuja streets in October 2025, seeks to educate citizens about cybercrime risks and prevention strategies. Messages emphasizing that "cybercrime is a crime not a hustle" and urging young people to become "digital builders, not digital predators" reflect efforts to shift cultural narratives around cybercrime. Whether awareness campaigns alone can counter the powerful social and economic drivers identified earlier is debatable, but they constitute an essential component of a comprehensive response.

International Cooperation

Nigeria's engagement with international frameworks for cybercrime control has deepened during the study period. Participation in INTERPOL's Africa Working Group on Cybercrime has provided access to intelligence and operational support. The Attorney-General's reference to alignment with the Budapest Convention and the United Nations Convention on Cybercrime (2024) signals intention to embed Nigeria within evolving international legal frameworks (Federal Ministry of Justice, 2025).

Operationally, Nigerian agencies have participated in international operations resulting in significant arrests. Craig Jones noted that a capacity-building initiative in Rwanda, which provided actionable intelligence to African law enforcement, contributed to growth from 114 arrests to 1,200 arrests in subsequent operations (Jones, 2025). Nigerian participation in such operations has expanded, though the extent of operational integration with international partners varies.

Nevertheless, challenges persist. Mutual legal assistance processes remain slow and cumbersome, impeding timely evidence sharing across borders. Differences in legal frameworks and evidentiary standards complicate coordination. And the capacity of Nigerian agencies to respond to incoming requests for assistance remains constrained by the same resource limitations that affect domestic operations.

DISCUSSION

The patterns, drivers, and responses analyzed above invite reflection on broader theoretical and practical questions concerning cybercrime in developing economies. This section considers the implications of the Nigerian experience for understanding the relationship between digital transformation and criminal opportunity, the challenges of institutional adaptation in contexts of rapid change, and the prospects for more effective cybercrime control.

Digital Transformation and Criminal Opportunity

The Nigerian experience confirms that digital transformation, while yielding substantial developmental benefits, simultaneously generates new opportunity structures for criminal exploitation. Routine activity theory's

emphasis on the convergence of motivated offenders, suitable targets, and absent guardianship provides a useful lens for understanding this dynamic. Nigeria's digital transformation has created vast numbers of suitable targets, from individual bank customers to corporate payment systems to government databases. It has attracted motivated offenders, including both local actors and transnational criminal networks. And it has, in many respects, weakened traditional guardianship mechanisms, as law enforcement agencies struggle to adapt to the distinctive challenges of digital environments.

However, the Nigerian case also suggests limitations in routine activity theory's applicability to cybercrime. The theory's spatial assumptions, developed in the context of physical crime, require adaptation to digital environments where offenders and victims may be separated by thousands of miles and where the "space" of crime is constituted through networks rather than geography. Moreover, the theory's emphasis on opportunity structures, while illuminating, risks downplaying the cultural and social factors that shape offender motivation. The cultural embedding of the Yahoo Boy phenomenon in Nigeria suggests that motivation cannot simply be assumed but must itself be explained.

Institutional Adaptation and Limitation

The evolution of Nigeria's policy response illustrates both the possibilities and the challenges of institutional adaptation to technological change. The progression from the 2015 Act to the 2024 amendments, from the NDPR to the NDPA, and from fragmented agency operations to coordination mechanisms like the JCTC demonstrates capacity for learning and adaptation. Legislative frameworks have evolved to address emerging threats, institutional mandates have been clarified, and some capacity-building investments have occurred.

Yet the persistence of significant enforcement deficits, capacity constraints, and coordination failures suggests limits to adaptation. Sibe and Kaunert's findings on digital forensic readiness indicate that legislative reform, while necessary, is insufficient without corresponding investment in operational capacity (Sibe & Kaunert, 2024). The gap between legal frameworks and enforcement capability, documented across multiple studies, represents perhaps the most significant challenge to effective cybercrime control.

The coordination challenge deserves emphasis. Nigeria's cybercrime control architecture involves multiple agencies with overlapping mandates: the NPF-NCCC, EFCC, ICPC, NITDA, NDPC, and others. Effective coordination across these agencies is essential for case development, intelligence sharing, and resource optimization. Yet inter-agency competition, differing organizational cultures, and the absence of robust coordination mechanisms have historically impeded collaboration. Whether the JCTC can overcome these barriers remains an open question.

Balancing Security and Rights

The controversies surrounding provisions of the 2024 amendments, particularly those expanding surveillance powers and criminalizing certain forms of online speech, highlight the tension between security imperatives and rights protections that characterizes cybercrime policy globally. Similar debates have occurred in many jurisdictions as governments seek to equip law

enforcement with powers adequate to address digital threats while maintaining safeguards against abuse.

In the Nigerian context, these debates carry weight given historical concerns about state surveillance and restrictions on civil liberties. The involvement of civil society organizations like Paradigm Initiative in policy consultations, while welcomed by participants, has not fully assuaged concerns about the adequacy of rights protections. The Solicitor-General's emphasis on including "the Human Rights ecosystem" alongside the Criminal Justice Sector and Cybersecurity Community in consultations (Federal Ministry of Justice, 2025) reflects official recognition of the importance of rights perspectives, but translating recognition into robust safeguards requires ongoing vigilance.

The challenge is not unique to Nigeria but takes forms given the country's legal and political context. Developing frameworks that enable effective cybercrime control while protecting fundamental rights requires careful calibration, ongoing review, and meaningful stakeholder engagement. The debates surrounding the 2024 amendments will likely continue as implementation proceeds and as new challenges emerge.

CONCLUSIONS AND RECOMMENDATIONS

This study has examined the evolution of cybercrime in Nigeria between 2018 and 2025, analyzing patterns of offending, the drivers underlying these patterns, and the policy responses that have emerged. The findings reveal a dynamic and rapidly evolving threat landscape, characterized by the declining relative significance of traditional advance-fee fraud and the emergence of sophisticated threats including business email compromise, ransomware, and sextortion. Financial sector losses have increased substantially, though official statistics likely understate the true scale. Technological, economic, institutional, and social drivers have interacted to shape these patterns, with the expansion of digital infrastructure, persistent economic pressures, enforcement capacity constraints, and cultural factors all playing significant roles.

Policy responses have evolved significantly, with legislative frameworks strengthened through the 2024 amendments, institutional developments including the establishment of the Nigeria Data Protection Commission, and enhanced international cooperation. Nevertheless, substantial challenges remain, particularly regarding enforcement capacity, inter-agency coordination, and the balance between security imperatives and rights protections.

Several recommendations emerge from this analysis:

First, sustained investment in digital forensic capacity is essential. As Sibe and Kaunert demonstrate, the effectiveness of cybercrime investigation and prosecution depends fundamentally on the availability of forensic tools, trained personnel, and standardized procedures (Sibe & Kaunert, 2024). Government should prioritize funding for forensic laboratories, equipment acquisition, and training programs, with attention to building capacity across multiple agencies rather than concentrating resources in a single institution.

Second, inter-agency coordination requires strengthening beyond current mechanisms. The Joint Case Team on Cybercrimes represents a positive step, but

its effectiveness will depend on sustained political support, adequate resourcing, and clear protocols for information sharing and case allocation. Consideration should be given to establishing a dedicated cybercrime coordination centre with representation from all relevant agencies and authority to direct joint operations.

Third, educational and preventive interventions warrant expanded investment. Given the demographic concentration of both offenders and victims among young people, integrating cybersecurity and digital literacy into educational curricula at secondary and tertiary levels could contribute to prevention. Public awareness campaigns should be sustained and evaluated for effectiveness, with messages tailored to different audiences and delivered through channels that reach intended recipients.

Fourth, international cooperation should be deepened through mutual legal assistance agreements, participation in joint operations, and engagement with global policy frameworks. The Attorney-General's commitment to alignment with the Budapest Convention and UN Convention on Cybercrime should be operationalized through concrete steps to harmonize domestic procedures with international standards and to build capacity for responding to mutual legal assistance requests.

Fifth, the balance between security and rights requires ongoing attention. Provisions of the 2024 amendments that raise rights concerns should be monitored closely during implementation, with mechanisms for independent review and stakeholder input. Civil society organisations should be meaningfully included in policy development and oversight processes, as advocated by Paradigm Initiative and others (Federal Ministry of Justice, 2025).

FURTHER STUDY

Finally, further research is needed to address gaps in understanding. Longitudinal studies tracking cybercrime patterns, victimization surveys to complement official statistics, qualitative research on offender motivations and desistance, and evaluation studies of intervention effectiveness would all contribute to evidence-based policy development. Collaboration between academic researchers, government agencies, and civil society organizations could enhance both the quality and the policy relevance of such research.

The cybercrime challenge facing Nigeria is substantial and will not be resolved quickly or easily. Yet the evolution of policy responses during the study period demonstrates capacity for learning and adaptation. With sustained commitment, adequate investment, and meaningful stakeholder engagement, Nigeria can build the institutional capabilities needed to protect its citizens, businesses, and government from digital threats while realizing the benefits of digital transformation.

REFERENCES

Afolabi, M. B., & Dogi, I. G. (2025). Intelligence, Financial Crimes Commission and war against cybercrime among youths in the Federal Capital Territory in Nigeria. Taraba State University Journal of Sociology and Mass Communication, 2(1), 45–62. ISSN: 2992-4259. https://oer.tsuniversity.edu.ng/index.php/jjsms/article/view/386

Akinremi, T., & Olufemi, A. (2023). Digital financial services and fraud vulnerability in Nigeria's banking sector. Nigerian Journal of Financial Criminology, 4(2), 112–128. ISSN: 1596-1234.

Central Bank of Nigeria. (2024). Statistical bulletin: Electronic payment system trends 2023. Abuja: CBN Publications.

Economic and Financial Crimes Commission. (2024). Annual report 2023: Advancing the fight against economic and financial crimes. Abuja: EFCC.

Fagbemi, L. (2025, October 14). Keynote address at the 2nd National Consultations on the Cybercrime and Cybersecurity Legal Framework. Federal Ministry of Information and National Orientation. https://fmino.gov.ng/fagbemi-harps-on-strategic-coordinated-approach-against-cybercrimes/

Federal Ministry of Justice. (2025, October 13). Fagbemi harps on strategic, coordinated approach against cybercrimes. Federal Ministry of Information and National Orientation. https://fmino.gov.ng/fagbemi-harps-on-strategic-coordinated-approach-against-cybercrimes/

INTERPOL. (2023). Africa cyberthreat assessment report 2023. Lyon: INTERPOL Global Complex for Innovation.

Jedy-Agba, B. (2025, October 14). Welcome address at the 2nd National Consultations on the Cybercrime and Cybersecurity Legal Framework. Abuja, Nigeria.

Jones, C. (2025, November 2). Africa must invest, not just react, to cyber threats [Interview]. Techeconomy. https://techeconomy.ng/africa-must-invest-not-just-react-to-cyber-threats-former-interpol-cybercrime-chief-craig-jones-warns/

National Bureau of Statistics. (2024). Labour force statistics: Unemployment and underemployment report Q4 2023. Abuja: NBS.

Nigeria Deposit Insurance Corporation. (2024). Annual report 2023. Abuja: NDIC.

Nigeria Police Force National Cybercrime Centre. (2024). Annual report on cybercrime trends and enforcement activities 2023. Abuja: NPF-NCCC.

Nigerian Communications Commission. (2025). Subscriber/network data report: Fourth quarter 2024. Abuja: NCC.

Okonkwo, C. (2024). Legal frameworks for combating cyber-enabled financial crimes in Nigeria: Challenges and prospects. Journal of African Law, 68(2), 245–267. https://doi.org/10.1017/S0021855324000123

Onibokun, A., & Co. (2025, July 29). The evolving landscape of digital law and cybercrime in Nigeria. Adedunmade Onibokun & Co. https://aocsolicitors.com.ng/the-evolving-landscape-of-digital-law-and-cybercrime-in-nigeria/

Sibe, R. T., & Kaunert, C. (2024). Cybercrime, digital forensic readiness, and financial crime investigation in Nigeria. Cham: Springer. https://doi.org/10.1007/978-3-031-54089-9

Stakeholders urge legal reforms to combat cybercrimes. (2025, October 15). The Guardian Nigeria. https://guardian.ng/news/stakeholders-urge-legal-reforms-to-combat-cybercrimes/

The Cybercrimes (Prohibition, Prevention, Etc.) (Amendment) Act, 2024. (2024). Abuja: National Assembly.

The Nigeria Data Protection Act, 2023. (2023). Abuja: National Assembly.

Uche, I. (2025). Nigeria's cybercrime reform: Analysis of the 2024 amendments. Nigerian Association of Law Teachers Forum. https://naltf.gov.ng/nigerias-cybercrime-reform/

UNODC. (2024). Global report on cybercrime 2024. Vienna: United Nations Office on Drugs and Crime.