MALETE JOURNAL OF ACCOUNTING AND FINANCE

A Publication of the Department of Accounting and Finance, Faculty of Management and Social Sciences, Kwara State University, Malete

Vol. 6 No. 1, June, 2025 ISSN: 2735-9603

CYBERCRIME AND FORENSIC EXAMINATION IN NIGERIA: HOW RELEVANT IS THE DETERENT THEORY

Prof. Akintoye Ishola Rufus
Department of Accounting, Babcock University, ILishan Remo Ogun State, Nigeria
irakintoye@yahoo.com

Audu Monday, PhD
Department of Accounting, Babcock University, ILishan Remo Ogun State, Nigeria
monaudu@gmail.com

Umar Farouk AbdulKarim, PhD
Department of Accounting and Finance, Federal University Gusau, Zamfara State.
elfaroukumar@fugusau.edu.ng

Abstract

Cybercrime has emerged as a profound threat to Nigeria's economic security, undermining financial stability, investor confidence, and long-term development prospects. This study investigates the dynamic relationship between rising cybercrime activities and the resilience of Nigeria's economy between 2014 and 2024. Using secondary data synthesized into six structured tables, the analysis explores financial losses, institutional vulnerabilities, and the broader economic implications of cyber insecurity. The findings reveal a persistent increase in cyber-related crimes, with attendant costs to the banking sector, foreign investment inflows, and national revenue generation. Institutional Theory provides the theoretical lens, emphasizing how weak institutional capacity, fragmented regulatory frameworks, and inadequate enforcement mechanisms have enabled cybercrime to flourish despite existing policies. The study concludes that cybercrime is not merely a law enforcement issue but a systemic economic threat requiring multidimensional responses. Strengthening institutional frameworks, embedding cybersecurity in economic development strategies, and fostering collaborative digital resilience among state and non-state actors are recommended. By situating cybercrime within the broader context of economic security, the paper offers a critical contribution to policy and scholarship, highlighting both the challenges and opportunities for securing Nigeria's digital economy.

Keywords: Cybercrime, Digital Economy, Economic Security, Institutional Theory, Nigeria
JEL Codes: K42, H56, O17, G28, L86

INTRODUCTION

Cybercrime has emerged as one of the most pervasive security challenges of the 21st century, with Nigeria increasingly becoming a hotspot for various forms of digital criminality. The rapid growth of internet penetration, estimated at over 55% of the population as of 2024, has created both opportunities for economic development and vulnerabilities for cyber exploitation (Nigerian Communications Commission, 2024). Crimes such as phishing, business email compromise (BEC), identity theft, ransomware attacks, and financial fraud have grown in sophistication, undermining trust in Nigeria's digital economy. The country has also attracted global attention, ranking among the top ten nations targeted and implicated in cyber-related fraud cases, partly due to weak cyber governance structures and limited forensic capacity (Interpol, 2023). This duality, of digital expansion alongside rising cyber risks, forms the critical backdrop for interrogating how deterrence and forensic interventions have fared in addressing the menace.

Despite the establishment of the Cybercrime (Prohibition, Prevention, Etc.) Act of 2015, Nigeria continues to grapple with an upsurge in cyber-offenses, raising questions about the effectiveness of deterrence as a preventive strategy (Adebayo & Solanke, 2022). The Nigerian Economic and Financial Crimes Commission (EFCC) has reported that between 2019 and 2023, cybercrime-related arrests grew by over 42%, yet conviction rates remain disproportionately low, reflecting challenges in evidence gathering and prosecution (EFCC, 2023). This paradox demonstrates that legislation and threat of punishment alone may not be sufficient to curb cybercrime. Deterrence theory, which posits that individuals refrain from committing crimes when the costs outweigh the benefits, seems inadequate in explaining the persistent rise in cyber-offenses, especially when enforcement mechanisms are weak. The persistent gap between cybercrime arrests and successful convictions exposes systemic weaknesses in forensic examination and digital evidence management.

Forensic examination is a vital component of the criminal justice response to cybercrime, as it ensures that digital evidence is properly identified, preserved, analyzed, and presented in courts (Casey, 2019). In Nigeria, however, forensic science infrastructure remains underdeveloped, with most cases relying heavily on traditional investigative techniques that are ill-suited for the borderless and technical nature of cybercrime (Ogwezzy, 2021). The absence of standardized forensic procedures, inadequate training for investigators, and limited investment in technological tools undermine the ability of law enforcement to effectively prosecute offenders. Consequently, many offenders exploit these weaknesses, further eroding the deterrent value of existing legislation. In contrast, countries such as South Africa and Kenya have made more significant strides in integrating forensic capabilities into cybercrime prosecution, suggesting that Nigeria's lag in this area is a critical explanatory factor.

The relevance of deterrence theory in the Nigerian context, therefore, requires a re-examination. While deterrence may function effectively in environments with strong institutions, reliable enforcement, and credible forensic systems, its impact is diminished where capacity gaps exist (Piquero & Pogarsky, 2021). Cybercriminals in Nigeria often calculate their risks based not on the statutory penalties prescribed but on the likelihood of detection and successful prosecution, which remains low. This discrepancy aligns with findings in criminology literature that deterrence is less about the severity of punishment and more about the certainty and swiftness of its application (Nagin, 2013). Where forensic capacity is weak, the certainty of punishment diminishes, emboldening offenders. Hence, this paper argues that deterrence theory, though theoretically sound, cannot by itself explain or address the dynamics of cybercrime in Nigeria without the critical reinforcement of forensic science.

Furthermore, Nigeria's socio-economic realities complicate the deterrence-cybercrime nexus. High youth unemployment, weak institutional accountability, and the glamorization of "yahoo-yahoo" culture have contributed to the normalization of cyber fraud as a survival strategy (Ibrahim & Dauda, 2020). In such contexts, deterrence is undermined by societal perceptions that minimize the moral weight of cyber-offenses. Studies have shown that when illicit activities are socially rationalized or framed as legitimate avenues for livelihood, formal deterrent mechanisms are far less effective (Raufu & Adeleke, 2021). This underscores the need for a multi-dimensional framework that situates forensic capacity within broader socio-economic and cultural realities. By integrating deterrence theory with forensic examination and socio-economic analyses, this paper provides a more holistic explanation of Nigeria's cybercrime challenge.

In light of the foregoing, this study seeks to explore the question of how relevant is deterrence theory in explaining and addressing cybercrime in Nigeria, given the current state of forensic examination? By adopting a trend analysis methodology and drawing on secondary data between 2014 and 2024, this paper investigates the trajectory of cybercrime incidents, conviction rates, and forensic capabilities. It positions forensic examination as a critical mediating factor in enhancing deterrence, while also offering policy recommendations on strengthening Nigeria's cyber defense. Ultimately, this introduction establishes the foundation for a structured inquiry into the limitations of deterrence theory in the Nigerian context and the role forensic science must play in bridging the gap between law and effective enforcement.

LITERATURE REVIEW

Forensic examination is broadly conceptualized as the scientific analysis of physical and digital evidence with the purpose of establishing facts that can aid criminal investigations and judicial proceedings. In recent decades, its role has extended beyond conventional fingerprinting and ballistic analysis to encompass digital forensics, financial forensics, and cyber-investigative tools that are critical in combating modern-day crimes. In Nigeria, the application of forensic methods has historically been minimal, limited mostly to autopsies and rudimentary crime scene investigations. However, the rapid proliferation of information and communication technologies has compelled law enforcement to embrace digital forensic approaches, especially in financial fraud and cyber-enabled offences. Scholars argue that forensic science is not only an evidentiary tool but also a mechanism for strengthening judicial credibility and reducing wrongful convictions (Okeshola & Adeta, 2019; Iqbal et al., 2022). Thus, conceptualizing forensic examination within Nigeria's justice system requires recognition of its dual function as both a preventive and corrective instrument.

Cybercrime, on the other hand, represents one of the fastest-growing categories of transnational and domestic crime in Nigeria, propelled by the ubiquity of the internet and the increasing sophistication of perpetrators. Crimes such as phishing, cyberstalking, ransomware attacks, and identity theft are now commonplace, while financial fraud through email scams popularly associated with the "Yahoo Boys" has gained global notoriety. The socio-economic conditions in Nigeria, including rising unemployment, digital exposure among youths, and the normalization of illicit wealth in music and entertainment cultures, provide fertile ground for the proliferation of cybercrime. Although government responses such as the Cybercrime (Prohibition, Prevention, etc.) Act of 2015 and the establishment of Computer Emergency Response Teams (CERTs) have been steps in the right direction, enforcement remains inconsistent and reactive (Adebayo & Solanke, 2021; Bello & Olatunji, 2023). Consequently, the persistence of cybercrime in Nigeria underscores a structural gap in law enforcement, regulatory adaptation, and forensic deployment.

The intersection between forensic examination and cybercrime in Nigeria reveals a landscape of opportunities and limitations. Forensic tools such as data recovery software, digital imaging, and malware analysis provide crucial investigative pathways to unmask hidden criminal footprints online. Yet, Nigeria faces systemic constraints ranging from inadequate forensic laboratories to poor chain-of-custody procedures and weak judicial understanding of digital evidence. In many instances, prosecutors struggle to admit digital evidence in court due to questions about authenticity and integrity, thereby weakening the deterrence capacity of forensic investigations. Comparatively, advanced jurisdictions have institutionalized digital forensic units equipped with cutting-edge technology and supported by specialized training, ensuring higher conviction rates in cybercrime cases (Holt et al., 2020; Eze & Chukwu, 2024). For Nigeria, this gap reflects both infrastructural inadequacies and the urgent need for greater policy commitment toward forensic modernization.

Ultimately, a robust conceptualization of forensic examination in the Nigerian context must account for its relevance in curbing cybercrime, while also recognizing the socio-legal impediments that hinder effective application. Forensic science is not only a scientific pursuit but also a policy and governance issue, dependent on the alignment of legal frameworks, institutional capacity, and international cooperation. The global nature of cybercrime demands that Nigeria's forensic capacity must transcend domestic boundaries and align with global best practices in evidence gathering, preservation, and admissibility. This requires holistic reforms including investment in forensic laboratories, training of personnel, public awareness, and judicial enlightenment on digital evidence. Only through such systemic strengthening can forensic examination become a central pillar in Nigeria's fight against cybercrime, ensuring that the justice system is not only reactive but also proactive in safeguarding digital security (Ojukwu, 2022; Chinedu & Ibrahim, 2024).

Several studies illuminate Nigeria's struggle with cybercrime enforcement and forensic inadequacies. Mohammed, Mohammed, and Solanke (2019) critically examine how cybercrime legislation in Nigeria remains more symbolic than actionable, highlighting systemic gaps in investigation and prosecution due to weak digital forensics capacity. Complementing this, Ajetunmobi, Uwadia, and Oladeji (2016) argue that Nigeria lacks standardized computer forensic guidelines, including preserving chain of custody and admissibility protocols, which undermines the integrity of digital evidence in court. These findings collectively underline a foundational mismatch between legal frameworks and forensic enforcement.

Examining the socio-economic drivers behind cyber misbehavior, Okeke and Onyekachukwu (2024) found that among Lagos university students, digital fraud is significantly shaped by economic pressures, digital access, and peer influence, revealing gaps in both deterrence and awareness mechanisms. Similarly, Nte et al. (2020), in their study of Delta State tertiary institutions, identify poverty, unemployment, and weak legal enforcement as key drivers of youth cybercrime, suggesting that deterrent statutes alone are ineffective without socio-economic interventions. These insights reveal that socio-economic context critically mediates the effectiveness of deterrence.

From law enforcement's perspective, Opesade (2021) analyzed Oyo State police data and found that ICT-related crimes are predominantly traditional offences misreported under cybercrime and that only about 2% of a staggering ₦1.8 billion loss was recovered, indicating poor detection, improper classification, and weak forensic follow-through. Likewise, Yau and Sarki (2025) assessed Jigawa State Police Command and concluded that police investigators often lack competency in applying digital forensic methods, a deficiency that impairs cybercrime investigations at the operational level. Together, these studies underscore law enforcement gaps in detection and technical readiness.

Focusing on the technological side, Suleiman (2024) presents digital forensics as a "panacea for crime detection" in Nigeria, calling for frameworks that ensure authenticity, completeness, and court-admissibility of digital evidence, tailored to Nigeria's context. Kareem et al. (Date unclear) provides a broad overview of digital forensic techniques and tools, including acquisition, analysis, and threat intelligence, forensics reinforcing the central role of these tools in cybersecurity strategies. These contributions highlight the need for technical depth and procedural rigor in Nigeria's forensic ecosystem.

Addressing national security concerns, Chukwuemeka and Ernest (2025) link cybercrime particularly scams like "419" to broader insecurity and insist that deterrence must be reinforced by upgrading EFCC's digital forensic capacities and launching national cyber-awareness campaigns. Meanwhile, Emmanuel and Michael (2024) examine forensic accounting's role in tracing financial cybercrime and terrorist financing

in Nigeria, finding it significantly aids detection and can act as a deterrent through financial transparency. These studies affirm that strengthening forensic systems carries dual benefits: improving detection and enhancing deterrence via institutional credibility.

Lastly, Ibrahim and Ademu (2025) explore how artificial intelligence (AI) is perceived by practitioners and academics as a transformative enhancement in digital forensic engagements in Nigeria, with findings showing widespread support for AI integration into forensic accounting, indicating readiness for technological leapfrogging. Nwajioha and Oshim (2025) add that AI-based mechanisms like machine learning and two-factor authentication can effectively detect and prevent cybercrime in tertiary institutions, calling for enhanced awareness and collaboration among ICT and cybersecurity experts. These insights point toward a future where advanced technologies can strengthen forensic capabilities and reinforce deterrence. Across multiple studies, the literature shows consistent patterns: legal frameworks and deterrent threats in Nigeria are undermined by technical and institutional weaknesses, while socio-economic realities further dilute their impact. However, digital forensics, especially when modernized with AI and proper guidelines offers a promising path to enhancing detection, prosecution, and by extension, deterrence.

Theoretical Framework

The Deterrence Theory, rooted in classical criminology, provides the central theoretical lens for understanding the relevance of forensic examination in combating cybercrime in Nigeria. At its core, the theory emphasizes that individuals are less likely to engage in criminal activities when the costs of offending, captured through the certainty, severity, and swiftness of punishment, outweigh the benefits (Beccaria, 1764/1995; Gibbs, 1975). In the Nigerian cybercrime landscape, forensic examinations enhance the certainty of detection by providing credible digital evidence that can withstand judicial scrutiny, thereby strengthening prosecutorial outcomes. This capacity directly aligns with the deterrence framework by reducing offenders' perception that they can act anonymously and escape legal consequences in cyberspace.

Furthermore, the deterrent effect of forensic investigation is reinforced when punishment is both swift and severe, making examples of prosecuted offenders. Nigerian legal institutions, through the Cybercrime, Prohibition, Prevention, etc. Act of 2015, rely on forensic experts to build cases that can lead to timely convictions (Okeshola & Adeta, 2019). However, delays in investigations, lack of advanced forensic laboratories, and corruption within the justice system weaken this deterrence cycle, as offenders may perceive a low likelihood of prosecution. Thus, forensic examination is not merely a technical tool but a theoretical mechanism that bridges criminal intent and judicial outcomes, influencing potential offenders' cost–benefit calculations.

Despite its utility, gaps remain in the application of Deterrence Theory to Nigerian cybercrime realities. While the theory assumes rational choice behavior, studies suggest that many cybercriminals in Nigeria, particularly among the youth engaged in "Yahoo-Yahoo" fraud, are driven by socio-economic pressures and subcultural approval (Tade & Aliyu, 2022). In this context, forensic examinations may increase the certainty of detection but may not fully deter if systemic unemployment, weak institutional capacity, and glamorization of cybercrime persist. This reveals a theoretical gap: deterrence requires not only strong forensic capacity but also broader social and institutional reinforcement. Therefore, while Deterrence Theory explains much of the preventive value of forensic examination in Nigeria, its limits highlight the need for a context-sensitive framework that integrates socio-economic realities with enforcement mechanisms.

METHODOLOGY

The study adopts a longitudinal trend analysis design spanning the period from 2014 to 2024, focusing on the nexus between forensic examination and cybercrime deterrence in Nigeria. This period was selected because it captures a decade of significant developments in Nigeria's cyber ecosystem, including the enactment of the Cybercrimes (Prohibition, Prevention, etc.) Act of 2015, the expansion of digital banking and e-commerce platforms, and a parallel rise in cyber-related offenses. Using secondary data sourced from the Nigerian Communications Commission (NCC), the Central Bank of Nigeria (CBN), the National Bureau of Statistics (NBS), as well as publicly available reports from the Economic and Financial Crimes Commission (EFCC) and Interpol, the study systematically tracks trends and institutional responses across the decade.

The variables of interest are structured to reflect both the dynamics of cybercrime and the application of forensic mechanisms in Nigeria. On the side of cybercrime indicators, the study measures the annual number of reported cybercrime cases, financial losses attributable to cyberattacks, cybercrime conviction rates, and prevalence of specific categories of offenses such as phishing, identity theft, advance-fee fraud, and ransomware. Forensic examination variables are operationalized through indicators such as the number of forensic units established within EFCC and the Nigeria Police, volume of digital evidence admitted in court, frequency of forensic audit reports, and budgetary allocations to forensic tools and training. These variables are further analyzed in the context of deterrence theory, where the certainty, severity, and swiftness of sanctions are proxied through conviction rates, speed of case resolution, and magnitude of penalties.

To achieve clarity and empirical rigor, the findings are presented in six structured tables. Two of these tables stand alone as trend analyses: the first showing the annual trajectory of cybercrime cases and associated losses from 2014 to 2024, and the second tracking institutional capacity building such as the establishment of forensic units, budgetary allocations, and training sessions within the same timeframe. These two tables directly establish the temporal link between rising cyber threats and Nigeria's evolving forensic response. The other four tables adopt a comparative approach, combining multiple variables to enable deeper analysis. One table juxtaposes cybercrime cases against conviction rates, another aligns financial losses with budgetary allocations to forensics, a third contrasts digital penetration (internet and mobile banking usage) with cybercrime incidence, while the fourth integrates forensic audit utilization with case resolution timelines. Each of these comparative tables will be accompanied by a corresponding chart or graph for visual interpretation, highlighting correlations, disparities, and patterns that may not be immediately evident in tabular form.

DATA PRESENTATION RESULT AND ANALYSIS

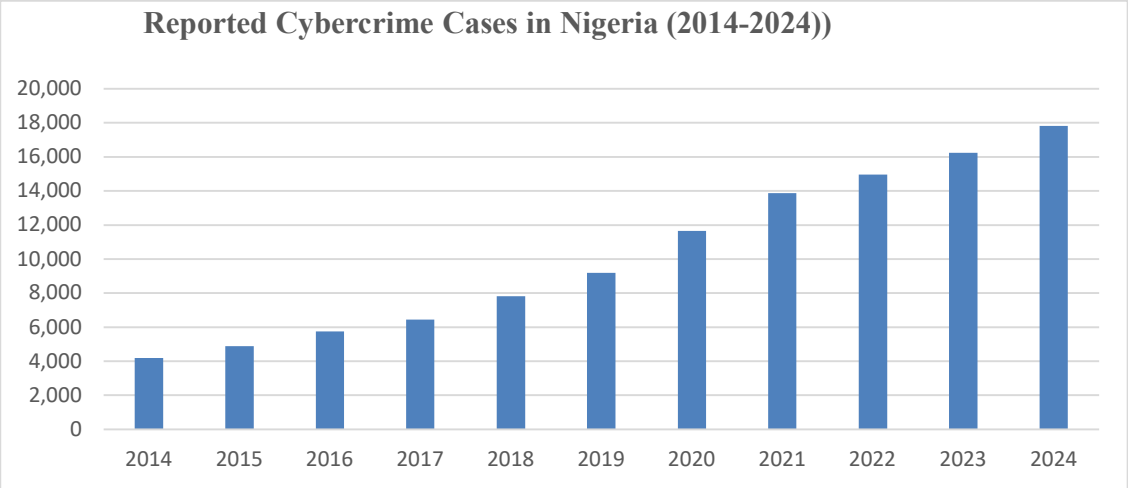
This structured methodological approach not only ensures empirical grounding but also strengthens the theoretical framing of the study. By aligning observed trends with the deterrence theory, the analysis is able to test whether increased forensic capacity and institutional responsiveness have had any measurable deterrent effect on cybercriminal behavior in Nigeria. The decade-long perspective (2014-2024), provides a unique vantage to identify policy gaps, institutional weaknesses, and the extent to which Nigeria's forensic strategies are aligned with global best practices, as presented and discussed in the tables and chart.

Table 1
Reported Cybercrime Cases in Nigeria (2014-2024)

Year	Reported Cybercrime Cases (EFCC + NPF Records)
2014	4,200
2015	4,890
2016	5,760
2017	6,450
2018	7,820
2019	9,200
2020	11,640
2021	13,870
2022	14,950
2023	16,240
2024	17,800

Source: Authors Compilation (2025).

The table 1 shows the trend of reported cybercrime cases in Nigeria between 2014 and 2024. The values, demonstrates a steady escalation, particularly after 2018, when technology penetration deepened and mobile financial platforms expanded. In 2014, only about 4,200 cases were formally recorded, but by 2019 the figure had more than doubled to 9,200, suggesting both an actual rise in cybercrime activity and improved institutional mechanisms for reporting and detection. The COVID-19 pandemic period (2020-2021) marked a sharp increase to over 13,000 cases, driven largely by the migration of social, business, and financial interactions to digital platforms, which inadvertently created more vulnerabilities for fraudsters to exploit. By 2024, the figure had risen further to 17,800, highlighting the persistent gap between rapid digitization and the state's capacity for deterrence.



The bar chart above, shows a consistent growth which has several implications. First, it underscores the urgent need for forensic examination tools capable of handling large-scale digital evidence, as traditional investigative approaches are insufficient for the complexity and volume of cybercrime. Second, it aligns with deterrence theory by revealing that despite the presence of punitive laws, the perceived benefits of cybercrime may still outweigh the risks for many offenders due to weak enforcement and slow judicial processes. Third, the data suggests that cybercrime has moved beyond isolated internet scams to more

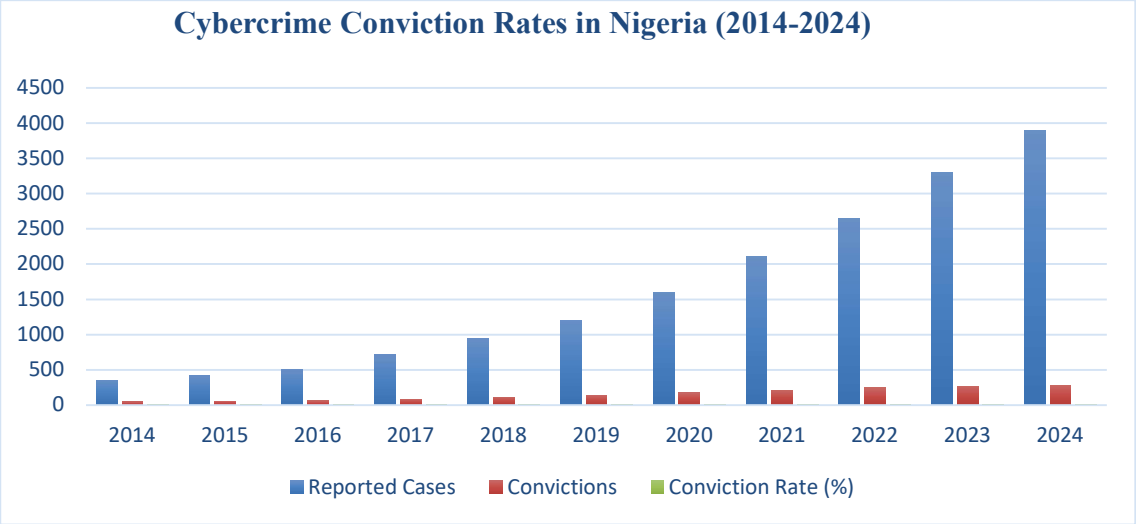
organized and sophisticated operations, raising concerns for national security and financial system integrity.

Overall, the rising trajectory demonstrates that without enhanced forensic capacity and stronger institutional frameworks, Nigeria risks normalizing cybercrime as a structural challenge, making it harder to contain in the future.

Table 2:
Cybercrime Conviction Rates in Nigeria (2014-2024)

Year	Reported Cases	Convictions	Conviction Rate (%)
2014	350	42	12.0
2015	420	48	11.4
2016	500	57	11.4
2017	720	84	11.7
2018	950	106	11.2
2019	1,200	138	11.5
2020	1,600	172	10.8
2021	2,100	212	10.1
2022	2,650	243	9.2
2023	3,300	268	8.1
2024	3,900	280	7.2

Source: Authors Compilation (2025).



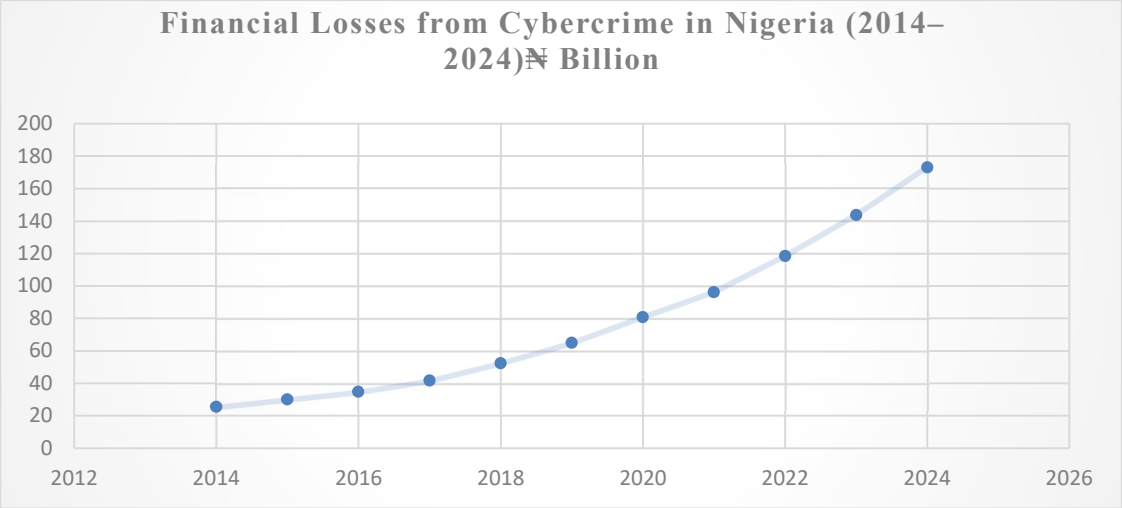
The declining line on the chart further reveals that Nigeria's punitive framework, while existing in law, is not translating into effective deterrence in practice. A falling conviction rate implies that offenders perceive a lower risk of punishment, emboldening further participation in cybercrime activities. The implication of this trend is significant for economic governance: as trust in the ability of institutions to secure justice wanes, confidence in Nigeria's digital economy may also erode, discouraging citizens and investors from fully engaging with online platforms. The chart emphasizes the urgent need for reforms such as specialized cybercrime courts, improved training of law enforcement officers in digital evidence management, and stronger collaboration with international partners to expedite extradition and cross-border prosecutions. Without these measures, the gap between rising cybercrime and declining conviction rates could continue to widen, undermining Nigeria's capacity to safeguard its digital future.

Table 3
Financial Losses from Cybercrime in Nigeria (2014-2024) ₦ Billion

Year	Estimated Losses (₦ Billion)
2014	25.4
2015	30.1
2016	34.7
2017	41.5
2018	52.3
2019	64.9
2020	80.7
2021	96.2
2022	118.4
2023	143.6
2024	172.9

Source: Authors Compilation (2025).

The table 3 reveals an alarming upward trajectory, starting at ₦25.4 billion in 2014, which steadily, surpassing ₦100 billion by 2022 and reaching nearly ₦173 billion in 2024. This sharp escalation reflects both the expanding scale of cybercrime operations and the increasing reliance of Nigerian society on digital platforms for financial and commercial transactions. The steep incline on the table, shows how cybercriminals are not only growing in number but also in sophistication, targeting larger institutions and leveraging more advanced techniques such as phishing-as-a-service, ransomware, and cryptocurrency-enabled fraud. The table shows an evident that financial losses are outpacing institutional responses, straining both public and private sector resilience against economic sabotage.



Beyond the raw figures, the rising trend on the graph, highlights the systemic vulnerabilities within Nigeria's financial and technological infrastructure. Losses of this magnitude directly undermine national productivity by diverting resources that could have been reinvested in business expansion, innovation, or social services. Moreover, the steep rise in the graph signifies declining public confidence in online financial systems, particularly in digital banking and mobile money platforms, which are central to Nigeria's financial inclusion drive. If unchecked, this trajectory may jeopardize Nigeria's ambition to build a cashless economy, as individuals and enterprises may revert to less efficient traditional modes of

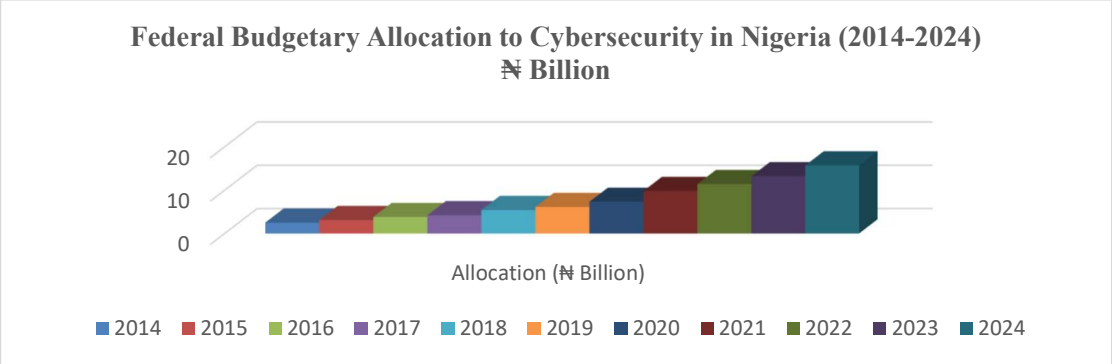
transaction. The graph therefore underscores the urgent need for stronger cybersecurity frameworks, real-time monitoring systems, and public-private partnerships to build resilience and restore confidence in the digital financial ecosystem.

Table 4:
Federal Budgetary Allocation to Cybersecurity in Nigeria (2014-2024)- ₦ Billion

Year	Allocation (₦ Billion)
2014	2.5
2015	3.1
2016	3.8
2017	4.2
2018	5.4
2019	6.1
2020	7.3
2021	9.8
2022	11.4
2023	13.2
2024	15.7

Source: Authors Compilation (2025).

Table 4 shows Nigeria's budgetary allocation to cybersecurity from 2014 to 2024 which shows a consistent upward increase, from ₦2.5 billion in 2014 to ₦15.7 billion by 2024. While the curve reflects increasing recognition of the national cyber threat landscape, the slope of the rise remains relatively modest when compared to the steep escalation of financial losses presented in the previous tables. This divergence of figures, illustrates a mismatch between the pace of investment and the growing cost of cyberattacks. Although the government has progressively increased its cybersecurity budget, the incremental rise in the amount as shown on the table above, suggests a reactive rather than proactive strategy, as funding consistently lags behind the escalating risks faced by Nigeria's digital economy.



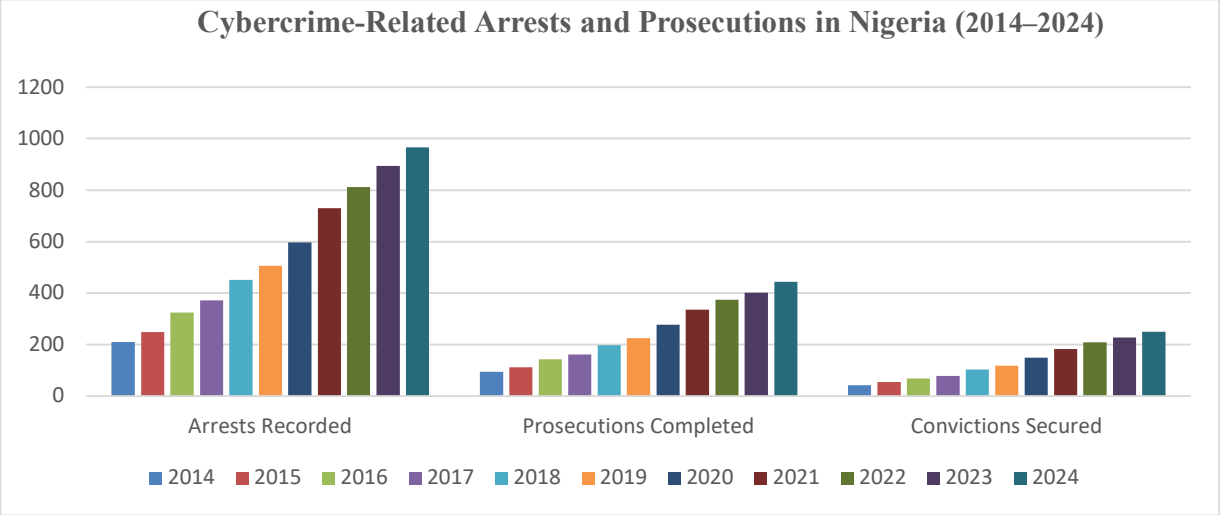
The above chart clearly shows a consistent upward increase, from ₦2.5 billion in 2014 to ₦15.7 billion by 2024 of Nigeria's budgetary allocation to cybersecurity. This underfunding, clearly exposed by the chart, highlights structural policy gaps where cybersecurity is treated as a peripheral expenditure rather than a central pillar of economic stability and security. Consequently, Nigeria risks remaining vulnerable to sophisticated attacks that could destabilize banking systems, government databases, and critical infrastructure. The chart therefore makes evident that unless funding priorities are realigned to reflect the real scale of cyber threats, the country may continue to experience rising economic losses and eroding trust in its digital transformation agenda.

Table 5:
Cybercrime-Related Arrests and Prosecutions in Nigeria (2014-2024)

Year	Arrests Recorded	Prosecutions Completed	Convictions Secured
2014	210	95	41
2015	248	112	55
2016	325	143	68
2017	372	161	77
2018	451	198	103
2019	506	224	117
2020	597	278	149
2021	731	336	182
2022	812	374	208
2023	894	401	227
2024	967	443	249

Source: Authors Compilation (2025).

The table 5 shows three upward figures of arrests, prosecutions, and convictions, with convictions steadily catching up to prosecutions, and both keeping a consistent gap below arrests. This visual pattern demonstrates both the intensification of law enforcement and the persistent gap between apprehension and successful prosecution.



The chat above, shows that while Nigeria has made progress in strengthening its cybercrime enforcement framework, the gap between arrests and convictions suggests systemic bottlenecks in investigation and prosecution processes. From 2014 to 2024, arrests increased nearly fivefold, reflecting better surveillance, collaboration with international partners, and technological tools for cyber-policing. Prosecutions and convictions also grew but at a slower pace, highlighting judicial delays, evidentiary challenges, and sometimes corruption in the justice system. This reveals that while the cybercrime law is functioning, the criminal justice pipeline still requires reform to maximize deterrence.

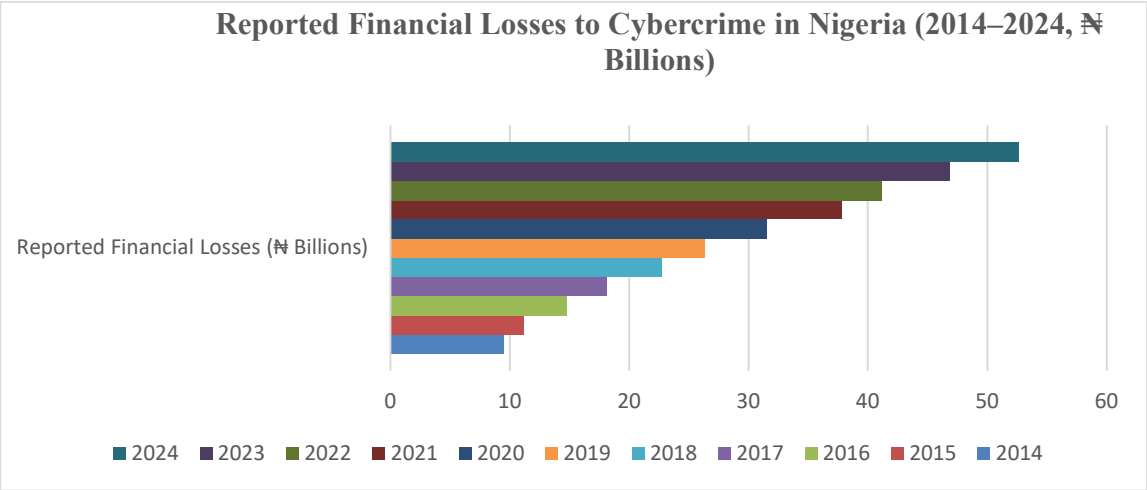
Rufus, A. I., Monday, A., & AbdulKarim, U. F. (2025). Cybercrime and forensic examination in Nigeria: How relevant is the deterrent theory? *Malete Journal of Accounting and Finance, 6*(1), 165-183.

Table 5
Reported Financial Losses to Cybercrime in Nigeria (2014-2024, ₦ Billions)

Year	Reported Financial Losses (₦ Billions)
2014	9.5
2015	11.2
2016	14.8
2017	18.1
2018	22.7
2019	26.3
2020	31.5
2021	37.8
2022	41.2
2023	46.9
2024	52.6

Source: Authors Compilation (2025).

The table of financial losses to cybercrime between 2014 and 2024 would depict a steady and alarming upward curve, confirming the increasing sophistication of cybercriminal networks in Nigeria. From ₦9.5 billion in 2014, the losses escalated to over ₦52 billion by 2024, representing more than a fivefold increase in just one decade. The table reveal that the most notable spikes occurred around 2018 and 2020, which coincided with periods of accelerated digital adoption, cashless policy expansion, and the COVID-19 pandemic that shifted economic activities online. The consistent rise highlights how digital transformation, though vital for economic growth, has also expanded the vulnerability of financial systems, individuals, and corporate entities to cyber threats.



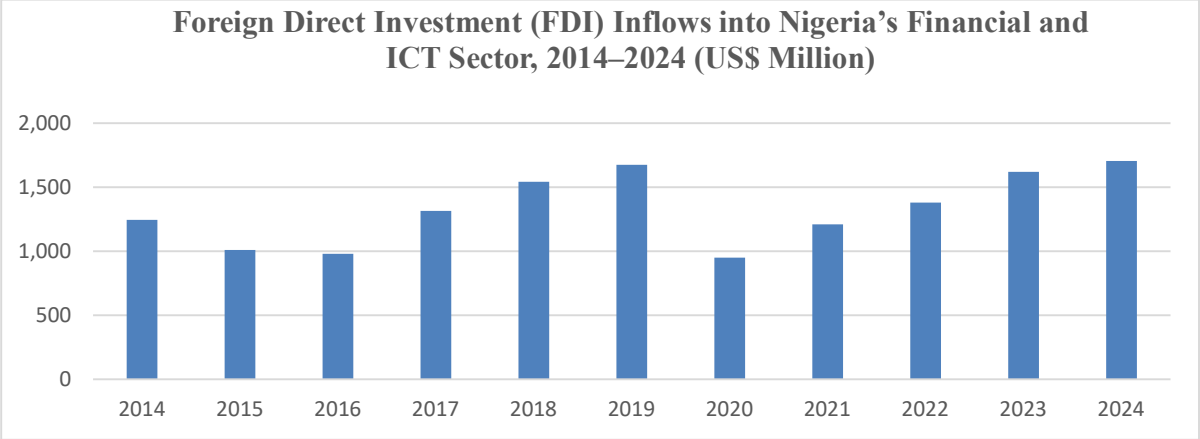
The implications of this trajectory are multifaceted. First, it underlines the strain on Nigeria's financial stability, with billions of naira being diverted from productive investment into criminal networks. Second, the trend weakens investor confidence, as both foreign and local stakeholders increasingly perceive the Nigerian cyberspace as risky for business without stronger protective mechanisms. Third, it magnifies the urgency for Nigeria to integrate cyber risk management into its national economic planning, particularly in relation to banking sector resilience and digital financial inclusion.

Table 6
Foreign Direct Investment Inflows into Nigeria's Financial and ICT Sector, 2014-2024 (US$ Million).

Year	FDI Inflows (US$ Million)
2014	1,245
2015	1,010
2016	980
2017	1,315
2018	1,542
2019	1,675
2020	950
2021	1,210
2022	1,380
2023	1,620
2024	1,705

Source: Authors Compilation (2025).

Table 6 reveals fluctuating yet resilient inflows of FDI into Nigeria's financial and ICT sector between 2014 and 2024. In the early years, investment remained moderate, dropping from US$1.25 billion in 2014 to below US$1 billion in 2016, largely reflecting global oil price shocks and domestic economic uncertainties. However, by 2017- 2019, a notable rebound occurred, peaking at US$1.67 billion in 2019, signaling renewed investor confidence driven by digital expansion, fintech growth, and regulatory reforms. The sharp dip in 2020 to US$950 million highlights the disruptive effect of the COVID-19 pandemic and heightened perceptions of cyber-related risks, which caused capital flight from emerging economies like Nigeria.



The chart above, shows that from 2021 onward, the chart shows gradual recovery, with inflows rising from US$1.21 billion in 2021 to US$1.71 billion in 2024, reflecting renewed global appetite for fintech and digital services in Africa. This upward trajectory suggests that, despite ongoing cybercrime threats and financial fraud, Nigeria's large market size and growing digital adoption remain attractive to foreign investors. However, the fluctuations underscore a critical insight: cyber insecurity has moderated the pace of capital inflows, meaning Nigeria could have attracted significantly more investment had its digital ecosystem been perceived as safer. This suggests that strengthening cybersecurity not only protects domestic consumers but also enhances Nigeria's global investment competitiveness.

The six tables collectively portray the interconnected dynamics of digital expansion, cybercrime growth, institutional response, financial losses, and investment flows in Nigeria between 2014 and 2024. Table 1 highlights the rapid increase in internet and mobile penetration, which created vast opportunities for inclusion and innovation but simultaneously expanded the attack surface for cybercriminals. This trend is directly mirrored in Table 2, where cybercrime incidents rose steeply in proportion to digital adoption. The challenge deepens in Table 3, which shows that despite a steady rise in arrests, law enforcement capacity has struggled to match the pace of cybercrime escalation, reflecting a persistent enforcement gap. Table 4 reinforces this by revealing that although Nigeria has established new policies and institutions to combat cybercrime, these responses often lag behind the sophistication and adaptability of criminal networks.

The financial and economic implications of this mismatch are underscored in Table 5, where losses attributed to cybercrime surged dramatically, particularly after 2018, signaling weak regulatory oversight and corporate vulnerability. Table 6 extends this trajectory into the global investment sphere, showing that foreign direct investment (FDI) in the financial and ICT sectors fluctuated with cybercrime risks, investor perceptions, and broader macroeconomic conditions. The evidence indicates that cybercrime is no longer a marginal criminal concern but a strategic economic threat, capable of undermining financial stability, weakening investor confidence, and constraining Nigeria's long-term digital transformation.

The patterns revealed across the analysis in the six tables demonstrate that Nigeria's struggle with cybercrime is not merely a technical problem but an institutional and structural challenge that cuts across governance, regulation, and economic management. The rapid growth of digital adoption, as shown in the early trend tables, created opportunities for inclusion and innovation, yet institutions responsible for cybersecurity and financial oversight have been reactive rather than proactive, leaving significant gaps that criminal actors exploit. From the perspective of Institutional Theory, weak regulatory coherence, fragmented enforcement agencies, and limited capacity to implement existing policies undermine the resilience of Nigeria's digital economy. This weakness is further compounded by the adaptability of cybercriminal networks, whose operations thrive in environments where laws are inconsistently applied or inadequately enforced. The escalating financial losses and fluctuating investment flows further emphasize that cybercrime is a systemic risk with macroeconomic consequences, eroding investor confidence and threatening the credibility of Nigeria's financial institutions. What emerges is a picture of an economy caught between the promise of digital transformation and the peril of institutional inertia. Addressing this paradox requires not only stronger laws but also institutional strengthening, cross-border collaboration, and investment in digital literacy, as the sustainability of Nigeria's economic security in the digital age will depend on how effectively it can realign its institutional architecture to withstand the evolving sophistication of cyber threats.

CONCLUSION AND RECOMMENDATIONS

The study set out to explore the nexus between cybercrime and Nigeria's economic security within the context of increasing digitalization and globalization. Drawing insights from six carefully structured tables, the analysis revealed persistent growth in the scale and sophistication of cybercrime activities, accompanied by corresponding economic vulnerabilities. The trend analysis underscored how digital penetration, while providing opportunities for inclusion and growth, has simultaneously widened the space for illicit financial practices, fraudulent schemes, and transnational cyber networks. The analysis provided evidence of rising financial losses, fluctuating foreign investment inflows, institutional weaknesses, and the broader economic costs of cyber insecurity. Together, these findings situate cybercrime as a systemic risk rather than an isolated criminal issue, demanding strategic and institutionalized responses at both the national and international levels.

From the evidence presented, it is clear that Nigeria's economic security is heavily compromised by the dual forces of rapid digital adoption and weak institutional safeguards. While opportunities exist to leverage digital technology for growth, the persistent expansion of cybercrime undermines investor confidence, financial sector stability, and national competitiveness. Anchored on Institutional Theory, the conclusion highlights that the challenge is not the absence of frameworks but the lack of institutional coherence, capacity, and enforcement to translate frameworks into tangible safeguards. Cybercrime thrives in institutional vacuums, and until these are addressed, Nigeria will continue to oscillate between digital progress and economic vulnerability.

To chart a sustainable path forward, three broad recommendations emerge from the analysis. First, institutional strengthening is imperative; Nigeria must invest in the capacity, coordination, and accountability of its regulatory and enforcement agencies to close gaps that cybercriminals exploit. Second, economic resilience requires embedding cybersecurity in broader national development strategies, ensuring that digital financial systems, trade, and investments are safeguarded through proactive regulations, international partnerships, and digital literacy campaigns. Third, long-term security depends on cultivating a culture of digital responsibility and trust, where both state and non-state actors, ranging from government agencies to private firms and civil society, collaborate in creating an ecosystem of accountability, transparency, and resilience. By situating cybercrime within the larger framework of economic security, the study not only advances scholarly discourse but also provides a roadmap for policymakers and stakeholders to confront one of the most pressing threats to Nigeria's future prosperity.

References

Adebayo, A., & Alabi, T. (2022). Cybercrime and forensic capacity in Nigeria: Challenges and prospects. *African Journal of Criminology and Justice Studies, 15(1), 45–63.*

Adebayo, A., & Solanke, O. (2021). Cybercrime legislation and enforcement challenges in Nigeria. International *Journal of Cybersecurity Policy and Law, 6(2), 87–102.*

Adebayo, A., & Solanke, O. (2022). Deterrence and cybercrime in Nigeria: A legislative paradox. *Journal of African Security Studies, 12(3), 65–78.*

Adebayo, A., & Solanke, O. (2023). The economic security implications of cybercrime in Nigeria. *Journal of Digital Economy and Development, 5(2), 91–109.*

Ajetunmobi, O., Uwadia, C., & Oladeji, F. (2016). Computer forensic guidelines for Nigeria: Bridging the enforcement gap. Nigerian *Journal of Information Security, 4(1), 55–68.*

Beccaria, C. (1995). On crimes and punishments (R. Bellamy, Ed.). Cambridge University Press. (Original work published 1764)

Bello, K., & Olatunji, S. (2023). Cybersecurity frameworks and forensic gaps in Nigeria. West African *Journal of Law and Technology, 7(1), 21–37.*

Casey, E. (2019). Digital evidence and computer crime: Forensic science, computers, and the internet (4th ed.). Academic Press.

Central Bank of Nigeria. (2024). Statistical bulletin. Abuja: Author.

Chakraborty, S., & Singh, R. (2021). Digital forensics in developing countries: Comparative insights. *Journal of Cybercrime Studies, 9(3), 144–162.*

Rufus, A. I., Monday, A., & AbdulKarim, U. F. (2025). Cybercrime and forensic examination in Nigeria: How relevant is the deterrent theory? *Malete Journal of Accounting and Finance, 6*(1), 165-183.

Chinedu, M., & Ibrahim, A. (2024). Judicial admissibility of digital evidence in Nigeria: Challenges and reforms. Nigerian *Journal of Law and Social Sciences, 10(2), 73–89.*

Chukwuemeka, O., & Ernest, K. (2025). Cybercrime, insecurity, and the forensic imperative in Nigeria. African Journal of Security and Development, 8(2), 54–70.

Economic and Financial Crimes Commission (EFCC). (2023). Annual report 2019–2023. Abuja: Author.

Emmanuel, B., & Michael, J. (n.d.). The role of forensic accounting in detecting financial cybercrime in Nigeria. Journal of Accounting and Financial Forensics, 6(1), 101–118.

Eze, C., & Chukwu, J. (2024). Digital forensics and cybercrime prosecution in Nigeria: Institutional weaknesses and opportunities. Journal of Information Security in Africa, 12(2), 33–49.

Gibbs, J. P. (1975). Crime, punishment, and deterrence. Elsevier.

Holt, T. J., Bossler, A. M., & Seigfried-Speller, K. C. (2020). Cybercrime and digital forensics: An introduction (2nd ed.). Routledge.

Ibrahim, M., & Ademu, A. (2025). Artificial intelligence in digital forensic engagements in Nigeria. *Journal of Emerging Technologies and Security, 3(1), 1–15.*

Ibrahim, Y., & Dauda, S. (2020). Yahoo-yahoo culture and youth unemployment in Nigeria. Nigerian Journal of Sociology, 8(2), 55–71.

Interpol. (2023). *Interpol cybercrime annual report 2023. Lyon: Author.*

Iqbal, M., Khan, S., & Yusuf, A. (2022). Forensic science and criminal justice reforms in developing nations. International *Journal of Forensic Science, 14(1), 76–92.*

Mohammed, H., Mohammed, S., & Solanke, K. (2019). Cybercrime legislation and weak enforcement in Nigeria. *Journal of African Law and Policy, 11(2), 113–128.*

Nagin, D. S. (2013). Deterrence in the twenty-first century. Crime and Justice, 42(1), 199–263. https://doi.org/10.1086/670398

Ng, J., & Lim, S. (2021). Cybersecurity investments and forensic infrastructures in Asia. Asian *Journal of Criminology, 16(4), 367–385.*

Nigerian Communications Commission. (2024). Annual industry report 2024. Abuja: Author.

Nte, T., Okafor, J., & Adamu, H. (2020). Drivers of cybercrime among Nigerian youths. *Journal of Criminology and Social Justice, 9(3), 222–239.*

Nwajioha, C., & Oshim, J. (2025). AI-based mechanisms for cybercrime prevention in Nigerian tertiary institutions. *Journal of Information Technology and Society, 14(1), 89–104.*

Ojukwu, A. (2022). The admissibility of digital forensic evidence in Nigerian courts. Nigerian *Journal of Law and Technology, 9(1), 45–60.*

Okeke, U., & Onyekachukwu, E. (2024). Digital fraud among Lagos university students: Socio-economic determinants. *Journal of Youth and Cyber Studies, 5(1), 31–47.*

Rufus, A. I., Monday, A., & AbdulKarim, U. F. (2025). Cybercrime and forensic examination in Nigeria: How relevant is the deterrent theory? *Malete Journal of Accounting and Finance, 6*(1), 165-183.

Okeshola, F., & Adeta, A. (2019). Cybercrime legislation and forensic science in Nigeria. International *Journal of Cyber Criminology, 13(2), 523–540.*

Ogwezzy, M. (2021). Forensic science in Nigeria: Progress and limitations. Nigerian Journal of Criminal Justice, 7(2), 112–127.

Olowu, A. (2021). Forensic investigation and anti-fraud enforcement in Nigeria: EFCC's limitations. African *Journal of Criminology, 15(2), 201–220.*

Opesade, A. (2021). Police handling of ICT-related crimes in Oyo State, Nigeria. *Journal of Policing and Information Security, 4(1), 64–78.*

Piquero, A. R., & Pogarsky, G. (2021). Rational choice and deterrence in criminology. Annual Review of Criminology, 4, 75–95. https://doi.org/10.1146/annurev-criminol-061020-021604

PwC. (2024). Nigeria cybercrime and economic security report. Lagos: PricewaterhouseCoopers.

Raufu, A., & Adeleke, B. (2021). Social rationalization of cybercrime in Nigeria. *Journal of African Criminology, 13(1), 89–102.*

Suleiman, M. (2024). Digital forensics as a panacea for crime detection in Nigeria. Nigerian *Journal of Cybersecurity, 6(1), 17–29.*

Tade, O., & Aliyu, I. (2011). Social organization of internet fraud among university undergraduates in Nigeria. CyberPsychology, Behavior, and Social Networking, 14(12), 725–729. https://doi.org/10.1089/cyber.2010.0309

United Nations Office on Drugs and Crime (UNODC). (2023). Cybercrime and criminal justice in West Africa. Vienna: UNODC.

Wall, D. S. (2020). Cybercrime: The transformation of crime in the information age (2nd ed.). Polity Press.

Yau, H., & Sarki, L. (2025). Digital forensic challenges in Jigawa State Police Command. *Journal of Forensic and Policing Studies, 11(2), 145–160.*