Digital Forensic Accounting on Cybercrime Deterrence in Africa's Digital Transformation

Inweregbu, Onyekachi Anthony Ph.D
Department of Accountancy,
Kingsley Ozumba Mbadiwe University, Ideato.
Ideato South L.G.A. Imo State, Nigeria

Ikwudinma Adaobi Eugenia
Ph.D. Student Department of Accounting,
Alex Ekwueme Federal University,
Ndufu-Alike Ebonyi State, Nigeria

Fort-Edward Uchenna Ugochi Ph.D
Department of Finance and Innovation Technology
Federal University of Technology, Owerri
Imo State, Nigeria

Obiah Mmadubuike Emmanuel
Department of Accountancy,
School of Business Management Technology,
Dr. B U Nzeribe State Polytechnic,
Awo-mamma, Oru-East L.G.A; Imo State,
Ph.D. Student Department of Accounting,
Alex Ekwueme Federal University,
Ndufu-Alike Ebonyi State, Nigeria
madoxlimoz@gmail.com; +2348067580007

https://doi.org/10.56201/ijefm.v11.no10.2026.pg223.240

Abstract
*This study examined digital forensic accounting on cybercrime deterrence in Africa's digital transformation, specifically analyzing the Economic and Financial Crime Commission (EFCC) in Enugu, Nigeria. The research adopted descriptive survey with structured questionnaire. The population for the study consisted of 129 respondents, including criminal investigators, cybercrime analysts, etc. A sample size of 98 was determined using the Taro Yamane formula, ensuring a 95% confidence level and a 5% error tolerance for reliability. Findings shows that forensic accounting has significant effect on cybercrime deterrence (R-value of 75.3%; p-value < 0.05). Additionally, the study found that forensic accounting accounted for (60%; p-value < 0.05) of the variance in digital era. The study concludes that forensic accounting is vital for cybercrime deterrence in Africa's digital era. Based on the findings, it recommends that financial institutions, government agencies, and other establishments should strengthen digital forensic accounting capacity and skills improvement a*nd *provide continuous training and professional development in*

investigative, analytical, communication, digital-forensic, and data-analysis skills. This would enhance the ability of forensic accountants to identify emerging cybercrime techniques, investigate suspicious transactions, and provide reliable evidence for fraud deterrence. Again, relevant regulatory institutions should integrate forensic accounting with stronger digital control and monitoring systems. Such measures would improve the early detection and prevention of cybercrime, reduce financial losses, and contribute to a safer environment in Africa's digital transformation.

Keywords: *Digital Forensic Accounting, Cybercrime, Cybercrime Deterrence, Digital Transformation*

Background of the Study

In this present era of rapid technological improvement, deterrent with dependable computer forensic skills and a demonstrated sense of independence is an indispensable tool for accountants to detect significant misstatements and errors that could have gone unnoticed thereby reducing the quality of cybercrime (Ugochukwu & Okenwa, 2021; Raji, Igbekoyi, Ogungbade & Nana**,** 2023). The 21st century has witnessed a profound transformation in the way institutions, and individuals conduct their activities, basically as a result of the rapid adoption of digital technologies and the internet. This transformation has created new opportunities for digital application in Africa. Olagunju, Otu and Zamani (2025) observe that the increasing adoption of digital technologies has fundamentally changed the contemporary business environment. The internet has consequently developed into a global network connecting millions of computers and users across different countries. However, the global and borderless nature of the internet has made cybercrime one of the major challenges confronting modern economies. The Nigerian cyber-fraudsters in Ibadan, Canadian cyberbullies in Toronto, Russian ransomware criminals in Moscow, Chinese political hackers in Harbin, and Jamaican lottery scammers in Montego Bay may use materially similar computer technologies to perpetrate crimes despite operating in different social, political, and economic environments (Lazarus, Button & Adogame, 2022). This demonstrates the global character of cybercrime and the difficulty associated with identifying perpetrators, tracing illegal transactions, recovering stolen assets, and bringing offenders to justice.

However, Africa has not been excluded from these developments. Nwankwo (2020) notes that Africa's reputation has suffered considerably because of the increasing incidence of cybercrime. The internet has therefore opened a window for both legitimate and illegitimate transactions, with internet fraud being one of the most prominent forms of illegitimate activity (Lazarus et al., 2022). In Nigeria, the Cybercrime (Prohibition, Prevention, Etc.) Act, 2015 recognizes several technology-related offences, including unauthorized access to computer systems or networks for fraudulent purposes, manipulation of payment technologies, and the introduction or transmission of malicious software capable of damaging computer data or systems (Cybercrime Act, 2015). Cybercrime encompasses a broad range of activities and is continuously evolving as criminals develop new methods of exploiting technological and financial systems. Chukwuka (2022) identifies various forms of cybercrime, including hacking, software piracy, cyberstalking, illegal trading, cybersquatting, internet fraud, money laundering, phishing, cyberbullying, online trafficking, child pornography, and cyberterrorism. Similarly, Eneisik and Ogbonna (2021) argue that internet scammers continuously develop new techniques for carrying out fraudulent schemes, meaning that the known forms of cybercrime represent only a portion of the wider cybercrime landscape. Lazarus et al. (2022), through the Tripartite Cybercrime Framework, further explain

that cybercrime can be motivated by socio-economic factors, psychological motives, and geopolitical considerations. These may include online fraud motivated by financial gain, cyberbullying motivated by psychological or social factors, and cyber espionage associated with political or geopolitical interests.

The increasing sophistication of cybercrime has significant implications for Africa's financial and economic systems. Financial crimes such as fraud, money laundering, embezzlement and corruption can weaken financial institutions, reduce investor confidence, increase the cost of doing business, and undermine public trust in economic institutions. FATF (2020) emphasizes that financial crimes pose a significant threat to global economic stability and national development. In developing economies, where institutional resources for cybersecurity, law enforcement, financial monitoring and technological investigations may be constrained, the consequences can be particularly serious. Funds obtained through cybercrime may also be transferred across jurisdictions, converted into other assets, or concealed through complex financial transactions, making detection and recovery difficult, including digital currencies, which create challenges relating to regulation, cybersecurity, financial crime, and monetary policy.

The challenge is further compounded by the fact that sophisticated fraud is not necessarily committed by individuals with limited technological knowledge. Veledar, Bašić and Čolpa (2022) contend that some of the largest frauds are perpetrated by intelligent, experienced, and creative individuals who possess a strong understanding of internet controls and system vulnerabilities, and producing reliable evidence for investigation and prosecution. In this context, forensic accounting has become increasingly relevant as an approach for detecting, investigating, preventing, and responding to financial crimes. Forensic accounting combines accounting knowledge with auditing, investigation, financial analysis, information technology, and legal principles to examine financial activities and identify evidence of fraud or other financial misconduct. It places considerable emphasis on the investigation of irregular transactions, identification of fraudulent schemes, tracing of assets, quantification of financial losses, and presentation of financial evidence in a form that can support legal proceedings. Its investigative orientation makes it potentially valuable in addressing cybercrime-related financial activities. In cases where cybercrime has already occurred, forensic accounting techniques can assist investigators in determining how funds were obtained, where they were transferred, the individuals or entities involved, and the extent of financial losses suffered. Such information can provide valuable evidence to law enforcement agencies, financial institutions, regulatory authorities, and the courts.

Digital forensic accounting has become a relatively new sub-discipline of forensic science that is increasingly becoming popular. Digital forensics experts are trained to conduct various kind of digital forensic investigation including some aspects of cybercrime investigation. Although, digital evidence can be fragile and large in volume, digital forensic professionals can automate the various phases of investigation for best result (**Ali & Hafidh, 2024**). Digital forensic accounting can therefore serve as an important component of a broader cybercrime deterrence framework by strengthening financial controls, improving fraud detection, supporting investigations, and enhancing accountability in Africa. The Nigerian experience provides a useful context for understanding this relationship. The Cybercrimes Act and its subsequent amendments criminalize several cyber-related offences, including computer-related fraud, credit card fraud, contract scams, and manipulation of automated teller machines and point-of-sale terminals (Wigwe & Partners, 2025). Beyond preventing financial losses, effective cybercrime deterrence has implications for Africa's broader digital era. At the macroeconomic level, persistent financial crime can undermine

institutional credibility and investor confidence, thereby affecting the environment necessary for sustainable economic development.

Despite the growing importance of cybercrime prevention and forensic accounting, there remains a need for greater empirical understanding of how forensic accounting contributes specifically to cybercrime prevention and economic development in the African context. Much of the discussion surrounding cybercrime focuses on cybersecurity, law enforcement, legislation, and technological solutions, while comparatively less attention may be given to the role of specialized accounting and financial investigation in identifying and preventing cyber-enabled financial crimes. This creates a need to examine whether and to what extent forensic accounting can serve as an effective mechanism for addressing cybercrime and strengthening economic development.

It is against this background that this study investigates forensic accounting on cybercrime deterrence in Africa's digital era. The study seeks to examine the effect of forensic accounting on cybercrime deterrence in Africa and assess the impact of forensic accounting on digital era of Africa. By examining the relationship between forensic accounting, and cybercrime deterrence, the study is expected to contribute to the growing body of knowledge on financial crime control and provide useful insights for policymakers, financial institutions, businesses, forensic accounting practitioners, law enforcement agencies, and other stakeholders involved in Africa's digital economic transformation.

Statement of the Problem

Cybercrime has emerged as one of the most widespread and dangerous forms of fraud in the 21st century, posing serious threats to individuals, businesses, financial institutions, governments, and national economies across the world. Hansa (2022) observes that the expansion of the cyber world has enabled fraudsters to access and manipulate victims' personal and financial information through various methods. Such information can be used to obtain financial benefits illegally and, in some cases, the proceeds of cybercrime may be channelled into other criminal activities, including terrorism. The problem of cybercrime is particularly significant in Africa because of the rapid growth of digital technologies and electronic financial transactions across the continent. Cybercriminals continuously develop new techniques for compromising computer systems, obtaining confidential information, manipulating financial transactions, and transferring illicit funds across jurisdictions with difficult mechanisms to detect, investigate, and prevent these crimes effectively. The complexity of cybercrime further constitutes a major problem for law enforcement agencies, financial institutions, forensic accountants, auditors, and other stakeholders responsible for preventing and investigating financial crimes. Awodiran, Ogundele, Idem and Anwana (2023) explain that cybercrime occurs through computers and the internet in different forms and is particularly complex because of the nature and diversity of electronic transactions involved. Also cybercriminals can transfer illicit proceeds rapidly between accounts, jurisdictions, financial institutions, and digital platforms. The increasing use of digital and virtual currencies has further complicated financial investigations because transactions may involve sophisticated technological systems, multiple layers of financial intermediaries, and acquiring and interpreting the digital and financial evidence required to investigate cybercrime effectively. This creates an important role for forensic accounting, because forensic accountants possess expertise in examining financial records, identifying unusual transactions, tracing assets, analysing financial patterns, investigating fraud, and providing evidence that can support legal proceedings. Awodiran et al. (2023) therefore identify forensic accounting as an important means of addressing the increasing level of cybercriminality.

Despite the potential contribution of forensic accounting, the persistence and increasing sophistication of cybercrime raise questions about the effectiveness and adequacy of existing forensic accounting practices in preventing cyber-related financial crimes in Africa. Furthermore, the consequences of cybercrime extend beyond individual financial losses to the broader economic development of African countries. Therefore, the problem of cybercrime is not merely a technological or law-enforcement issue; it is also an economic development concern.

There is insufficient empirical clarity on the extent to which forensic accounting can effectively prevent cybercrime and contribute to broader digital era in Africa. The gap is particularly important because effective cybercrime deterrence may enhance confidence in digital financial systems, protect financial resources, strengthen institutional accountability, and create a more secure environment for investment. However, evidence from previous studies (Muideen, Abiodun, Udosen & Anwana, 2023; Okoye & Mbanugo, 2020; Ojo-Agbodu, Abiola & Ndubusi, 2022; Ikpe, 2024), suggests that forensic accounting may contribute to reducing, detecting, and preventing fraud. Awodiran et al. (2023) report that fraud reduction, detection, and prevention stimulated by forensic accounting, together with effective managerial roles, have a positive and statistically significant relationship with fraud control. The authors further indicate that minimising cybercrime requires a combination of management control systems, bank reputation, and forensic accounting components. However, the continuing prevalence of cybercrime raises the need for further investigation into the extent to which forensic accounting can specifically contribute to cybercrime deterrence and, ultimately, economic development within the African context.

Consequently, this study seeks to investigate the effect of forensic accounting on cybercrime deterrence in Africa and assess its impact on economic development. Specifically, the study addresses the concern of whether the application of forensic accounting techniques can significantly improve the detection and deterrence of cybercrime and whether such improvement can translate into positive economic development outcomes in Africa.

Objective of the Study

The main objective was to investigate effect of forensic accounting on cybercrime prevention in Africa's economic development. Specifically, the study was to:

1. Examine the effect of digital forensic accounting on cybercrime deterrence in Africa

2. Assess the impact of digital forensic accounting on digital transformation in Africa

Research Questions

From the above statement of research problem, the following questions are generated.

1. How does digital forensic accounting affect cybercrime deterrence in Africa?

2. What is the impact of digital forensic accounting on digital transformation in Africa?

Research Hypotheses

From the above objectives the followings research hypotheses were formulated:

$H0_1$. Digital forensic accounting has a significant effect on cybercrime deterrence in Africa

$H0_2$. Digital forensic accounting significantly impacts the digital transformation in Africa

Conceptual Framework

Digital Forensic accounting

Forensic accounting has emerged as an important area of accounting practice in response to the increasing sophistication and complexity of financial fraud, cybercrime, and other forms of

economic crime, and present financial evidence for investigative and legal purposes. According to Okoye et al. (2020), forensic accounting is a relatively new branch of accounting practice that involves the application of specialized skills in accounting, finance, quantitative methods, law, and research in the collection, analysis, interpretation, and evaluation of financial evidence to support criminal proceedings. Similarly, Oni (2021) describes forensic accounting as the application of analytical, arithmetical, auditing, financial, quantitative, legal, research, and investigative skills acquired by accountants in gathering evidence and supporting adjudication in legal matters without causing harm or molestation to the accused. They may also examine particular operational or financial areas for indications of fraudulent activity even where no obvious red flags exist (Olagunju, Otu & Zamani, 2025; Veledar, Bašić & Čolpa, 2022). The practice of forensic accounting can broadly be categorized into litigation advisory services, investigative services and preventive functions, which contributes to strengthening corporate governance, restoring public confidence, and improving organizational awareness of fraud risks and detection mechanisms (Ukpabi et al., 2021; Dan'azumi et al., 2020; Eze & Osuji, 2023; Ukangwa et al., 2023). This multidisciplinary nature makes forensic accounting particularly relevant to contemporary financial crime because fraudulent activities increasingly involve both financial and technological dimensions.

Forensic accountants may also be retained by law-enforcement and anti-corruption agencies to investigate suspected financial crimes. In Nigeria, for example, agencies such as the Economic and Financial Crimes Commission (EFCC), the Independent Corrupt Practices and Other Related Offences Commission (ICPC), and the Federal Inland Revenue Service (FIRS) may engage professionals with forensic accounting expertise in the investigation of financial misconduct. Similar investigative functions are performed by relevant law-enforcement agencies in other jurisdictions, including the Federal Bureau of Investigation in the United States.

However, Digital forensics also referred to as "cyber forensics" and "computer forensics" is a new sub-discipline of forensic science. The first Digital Research Forensic Workshop defined digital forensics as: The use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations (Ali & Hafidh, 2024). Digital forensics is guided by a scientific protocol and it is often conducted to aid investigation or prosecution. Digital evidence can be usually collected or retrieved from electronic and digital devices such as desktop computers, laptops, tablets, servers, smart phones, Global Positioning Systems (GPS), drones, Close Circuit Television (CCTV) systems, digital video recorders, SIMcards, digital cameras etc. (Ali & Hafidh, 2024). The increasing digitization of financial transactions has further expanded the scope of forensic accounting. The emergence of cyber-enabled fraud means that forensic accountants increasingly require digital knowledge, skills, and abilities in addition to traditional accounting and auditing competencies. They may be involved in the capture, collection, preservation, identification, extraction, analysis, documentation, and presentation of digital evidence obtained from computers and other digital systems (Ali & Hafidh, 2024), for financial-crime-related purposes (Raji, Igbekoyi, Ogungbade & Nana, 2023). The integration of forensic accounting and technology has therefore transformed the profession from a predominantly traditional financial investigation function into a broader multidisciplinary approach to financial and cybercrime.

Cybercrime

Cybercrime represents a broad category of criminal activities involving computers, digital devices, computer networks, information systems, and the internet. Its multidisciplinary nature has resulted in different definitions from legal scholars, criminologists, sociologists, victimologists, and ethicists, reflecting the diverse perspectives through which criminal behaviour is understood (Ajibade, n.d.). In its broadest sense, crime may involve fraudulent or deceptive conduct through which an individual intentionally misrepresents or conceals material facts in order to obtain an unfair advantage, resulting in economic loss, legal injury, or unlawful gain.

The Black's Law Dictionary (1990), as cited by Oni (2021), describes crime in terms of the intentional perversion of truth or violation of a law intended to induce another person to surrender something of value or a legal right. Under the authority of the EFCC, crime may involve non-violent criminal and illicit activities undertaken to generate illegal wealth, either individually or collectively, in violation of laws regulating economic activities and administration (Kankpang, Ogar-Abang & Animpuye, 2024). Esonwune and Ogiri (2024) similarly view crime as deliberate lying intended to obtain an advantage or dishonestly deprive another person of something to which that person is entitled.

Within this broader concept of crime, cybercrime can be understood as criminal conduct facilitated, committed, or targeted through digital technologies. Cybercrime may therefore involve deliberate deception conducted through the internet or other digital platforms with the intention of inducing individuals or organizations to surrender assets, financial resources, personal information, or lawful rights (Ehimen & Bola, 2009 in Okpa, Gwambeka, Waziri & Mamman, 2025; Ajibade, n.d.). The United Nations Office on Drugs and Crime (UNODC, 2013), as cited in Olagunju et al. (2025), describes cybercrime as criminal acts committed through computers or the internet, including offences directed against computer data and systems, content-related offences, and online fraud. More broadly, cybercrime involves the commission of illegal activities through digital technologies, particularly computers, computer networks, and the internet, either as the target of the offence or as the means through which the offence is committed. Cybercrime may consequently range from financial fraud and intellectual-property theft to cyberterrorism, child exploitation, hacking, data theft, and other activities capable of threatening digital governance and national security (Olagunju et al., 2025; Oluwamuye & Adedipe, 2025). Cybercrime may involve obtaining digital information without authorization, accessing classified information improperly, gaining entry into non-public computer systems, or breaching protected computer systems (Nwankwo, 2020; Olagunju et al., 2025).

The growth of digital financial services has particularly intensified the relationship between cybercrime and financial fraud in the cyberspace (Daraojimba, Farayola, Olatoye, Mhlongo & Oke, 2023). Therefore, the expansion of digital platforms for trading financial products and services has consequently created additional opportunities for financial crime, particularly in emerging economies (Bukar, Adebisi & Abdulrahman, 2025 in Smith, 2021). The implications of cybercrime for economic development are substantial because individuals, businesses, financial institutions, and governments may suffer financial losses, reputational damage, disruption of operations, and loss of confidential information. The growing prevalence of cybercrime has consequently increased the need for forensic accountants who possess digital competencies. Forensic accountants are increasingly required to combine conventional accounting expertise with digital investigative capabilities to trace financial transactions, identify digital footprints, reconstruct financial events, and establish evidential links between cyber activities and financial outcomes (Ali & Hafidh, 2024).

Cybercrime Deterrence

Cybercrime deterrence refers to the proactive measures, strategies, systems, controls, and institutional mechanisms designed to reduce the likelihood of cybercrime and fraudulent activities occurring. Whereas cybercrime investigation primarily focuses on identifying and reconstructing criminal activities after or while they occur, deterrence seeks to address vulnerabilities before they are successfully exploited. The objective is therefore to establish an environment in which opportunities for fraudulent and cybercriminal activities are minimized and potential offenders are discouraged from engaging in such conduct. Fraud deterrence involves recognizing potential fraudulent activity and taking appropriate measures to stop it before it occurs (Ibukunoluwa, 2024). It can consequently be regarded as a strategic shield consisting of policies, procedures, controls, technologies, and institutional practices designed to protect organizations from fraudulent activities. These measures are intended to deter potential perpetrators and reduce organizational vulnerabilities (Onyema, Ojo-Agbodu & Adebayo, 2024).

The deterrent dimension of fraud prevention is also important. Anowu, Nyor, Agbi, Nelson and Saliu (2021) argue that the fear of detection and the prospect of facing substantial penalties can discourage individuals from engaging in dishonest or fraudulent activities. The effectiveness of such measures depends, in part, on the credibility of sanctions and the effectiveness of enforcement mechanisms (Enofe et al., 2014 in Okeke & Okoye, 2025).

A comprehensive cybercrime-deterrence framework should consequently incorporate strong internal controls, continuous monitoring, auditing technologies, information-security measures, employee training, ethical programmes, fraud-awareness initiatives, and effective reporting mechanisms. In this context, forensic accounting represents an important component of cybercrime prevention because it links financial analysis with investigation, technology, internal control, and legal processes.

Theoretical Framework

A theoretical framework is a structure that depicts and supports the scientific investigation, underpins research work, holds the system of research, and provides perspectives by which scientific research can be viewed based on results of existing studies or theories. The theoretical framework provides a building block on which scientific inquiry could be discussed and explained. The underpinning theories for the study are the White-Collar Crime and Space Transition Theory of Cybercrime.

Theory of White-Collar Crime

The Theory of White-Collar Crime was developed by Edwin H. Sutherland in 1939. Sutherland introduced the concept of *white-collar crime* during his presidential address to the 34th Annual Meeting of the American Sociological Society. He subsequently developed the theory further through his works on *White Collar Crime* and the 1947 edition of *Principles of Criminology*. The theory emerged in response to the dominant criminological view at the time that criminal behaviour was largely associated with biological, psychological, or socio-economic characteristics of lower-class individuals. Sutherland's primary reason for developing the theory was to draw attention to criminal activities committed by individuals of high social status in the course of their occupations, particularly business executives, professionals, and persons in positions of trust. He argued that criminal behaviour is not restricted to disadvantaged groups and that individuals occupying respectable social positions can also engage in fraudulent and other illegal activities.

The theory is closely associated with Sutherland's concept of differential association**,** which explains that criminal behaviour is learned through interaction and communication with other people, particularly within intimate or close social groups. The theory therefore provides a basis for understanding occupational fraud and the exploitation of internal-control weaknesses. It also highlights the importance of equipping forensic accountants with the skills necessary to identify patterns of fraudulent behaviour, investigate financial irregularities, and strengthen organizational controls.

Space Transition Theory of Cybercrime

Space Transition Theory (SPT) was developed by K. Jaishankar in 2008 to explain criminal behaviour in cyberspace. The theory was developed because traditional criminological theories were considered insufficient to fully explain the distinctive characteristics of cybercrime, particularly the influence of anonymity, identity flexibility, spatial mobility, and the absence of conventional social controls in cyberspace.

Jaishankar (2008) proposed that individuals may behave differently in cyberspace from how they behave in the physical world. The theory is based on the assumption that the transition between physical and cyberspace can alter an individual's behavioural constraints and create opportunities for criminal conduct. Cyberspace provides characteristics such as anonymity, identity flexibility, dissociative behaviour, and reduced immediate social and physical deterrence, which can encourage individuals to engage in criminal activities that they might otherwise avoid in physical space. Space Transition Theory is founded on seven major propositions**.**

Thus, cyberspace weakens some of the social, familial, occupational, and community constraints that regulate behaviour in physical environments. In the Nigerian context, the movement of some youths from conventional forms of crime into internet-enabled fraud can be examined through this perspective. The theory is further supported by the observation that traditional criminal groups increasingly use the internet to facilitate activities such as fraud, extortion, money laundering, intimidation, and theft more efficiently and with reduced risks (Jaishankar, 2008). Cyberspace therefore provides an environment in which offenders can interact across geographical boundaries, establish criminal networks, and engage in fraudulent activities with greater anonymity.

Application of the Theories to the Study

These theories will help to broaden forensic accountants and other stakeholders' knowledge about cybercrime prevention and why it occurs. Few studies showed that the standard denominations in all fraudulent activities are deception, knowledge of the act by at least one party, the victim of the fraud, and personal gain to at least one party, which could be the individual or corporate entity that misled the other party. The Theory of White-Collar Crime and Space Transition Theory provide complementary explanations of financial and cyber-enabled fraud. Sutherland's theory explains who may commit fraud and how criminal behaviour is learned**,** emphasizing social interaction, occupational environments, techniques, motives, and rationalizations. Space Transition Theory, on the other hand, explains how and why individuals may transfer or express criminal behaviour in cyberspace**,** emphasizing anonymity, identity flexibility, reduced social constraints, and the fluid movement between physical and virtual environments. The theories provide a useful theoretical foundation for examining the relationship between digital forensic accounting and cybercrime prevention in Africa's economic development**.**

Empirical Review

Nwokoro, Chima, Ndom and Iheonu (2022), investigated from the perceptions of youths on the incessant engagement of unscrupulous youths in cybercrime in Owerri Municipal in Imo state Nigeria, and the factors that predispose them to engage in this crime. The study posed three research questions, and adopted a mixed method approach, whereby 300 youths selected from Owerri municipal in Imo state were shared questionnaires to fill and submit, and another 10 youths interviewed. About 285 questionnaires were retrieved and used for the analysis. The findings showed that yahoo-yahoo is a type of cybercrime perpetrated with the aid of the internet and social media handles, of which the Facebook app is mostly used. Factors such as youth unemployment/lack of alternative income sources, influence of peer pressure and corrupt friends, and fast-money-making syndrome perpetuate the engagement of youths in cybercrime. The study equally showed that the perpetrators of this cybercrime target their victims through anchor social media such as Facebook, WhatsApp, Instagram and Tweeter, of which the Facebook was reportedly mostly used. Muideen, Abiodun, Udosen and Anwana (2023), examined the association between digital forensic accounting and cyber fraud. Primary source was used in gathering data, through a survey questionnaire. The population of the study comprised of accounting professionals (excluding partners) in the "Big Four" accounting firms in Nigeria. The study employed correlation as the technique of data analysis. The results revealed that digital forensic accounting has a negative and significant association with phishing scams, advance fee fraud and credit card fraud. Hence, the use of digital forensic accounting, therefore, minimizes the incidence of cyber frauds in Nigeria. Okoye and Mbanugo (2020), examined forensic accounting as a tool for fraud detection and prevention in public tertiary institutions in South East Nigeria. The study aimed to determine how forensic accounting helps reduce fraud cases in these institutions. A descriptive survey design was adopted, with a population of 470 accounting staff from seven public tertiary institutions. A total of 350 responses were collected. Analysis of Variance (ANOVA) was used to test the hypotheses. The study found that the use of forensic accounting significantly reduces fraud cases in tertiary institutions, with a significant difference between forensic accountants and traditional external auditors in detecting and preventing fraud. (see also Ewa, Adesola & Eseneyen, 2020; Ojo-Agbodu, Abiola & Ndubusi, 2022; Agbo, Idimoasho & Kwanum, 2023).

Akeke and Atah (2023), investigated the influence of forensic accounting techniques on fraud prevention in tertiary institutions in Cross River State, Nigeria. The study used a survey research design, with 152 auditors from the bursary departments of the institutions participating. A questionnaire, titled "Forensic Accounting Techniques on Fraud Prevention" (FATFP), was used to collect data. The Cronbach's alpha reliability coefficient of the instrument was 0.79. Data were analysed using standard deviation, mean, and independent t-tests at the 0.05 significance level. The findings indicated that computer-assisted audit techniques and interview audit techniques significantly influenced fraud prevention in tertiary institutions. (see also Ikpe, 2024; Adekunle, 2024; Asah & Obiora, 2022; Mvunabandi & Nomlala, 2022; Esonwune & Ogiri, 2024; Kankpang, Ogar-Abang & Animpuye, 2024; Ogunleye & Fanimokun, 2025).

Research Methodology

The researchers adopted survey research design for the study. The population for this study comprises all the staff associated with Economic and Financial Crime Commission and stakeholders in Enugu. From this population, a sample of 129 respondents were selected, consisting of 80 senior staff, 30 junior staff members, 15 corpse members in EFCC Community Development Service (CDS), and 4 volunteers. This study adopted random sampling techniques,

which makes it possible for all the workers to have equal opportunity of being selected as the representative sample. Based on the sample size of ninety-eight (98) inhabitants, a normal confidence level of 95% and error tolerance of 5% was used. Primary source of data was adopted using structured questionnaire with a 5-point Likert scale to acquire data from the targeted respondents. Meanwhile, validity was assessed through expert review, where professionals in the relative field evaluated the questionnaire to confirm that it adequately captured the study's variables. Their feedback helped refine the wording, structure, and relevance of the questions, ensuring that they effectively measured access to investigation, financial literacy, criminal analysis, cybercrime analysis, and internet indicators. Reliability was tested using the Cronbach's alpha coefficient, which measures the internal consistency of the questionnaire items. A reliability coefficient of 0.7 or higher was considered acceptable, indicating that the instrument produced stable and consistent results. Quantitative data collected were analyzed, presented and interpreted using descriptive statistics. For advanced analysis, the study used multiple regression method which evaluated the effect contribution of each latent variables. This was tested at a significance level of 5% or 0.05 with the aid of Statistical Package for Social Sciences (SPSS). The data were analyzed and presented to validate and test the stated hypotheses.

Results Hypotheses One: Digital forensic accounting has no significant effects on cybercrime deterrence in Africa.

Table 1: Model Summary

Model R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.868a 0.753	0.745	1.72781

• **Predictors:** (Constant), Investigative Skills, Analytical Skills, and Communication Skills
Source: SPSS output, 2026

Table 1 above gives us the R-value, which represents the correlation between the observed value and predicted value of the dependent variable which gives 86.8 percent. This shows that there is an adequate level of relationship between cybercrime deterrence and digital forensic accounting. The R2 value which is an indication of the coefficient of determination from the model summary is .753 which indicates that 75.3% of cybercrime deterrence is stimulated by the digital forensic accounting while the remaining 24.7% of cybercrime deterrence is stimulated by other unidentified variables.

Table 2: Coefficientsa

Model		Unstandardized Coefficients B	Unstandardized Coefficients Std. Error	Standardized Coefficients Beta	T	Sig.
1	(Constant)	8.862	1.812		4.890	0.000
	Investigative	2.182	0.135	0.880	16.127	0.000
	Analytical	0.163	0.112	0.087	1.459	0.048
	Communication	0.225	0.134	0.101	1.684	0.096

a. Dependent Variable: Cybercrime Deterrence

Source: SPSS output, 2026

a. Dependent Variable: Cybercrime Deterrence
Source: SPSS output, 2026
The table of coefficients above demonstrated how investigative skills, analytical skills, and communication skills influence cybercrime deterrence.
Table 2 shows that every increase in investigative skills, and analytical skills, results in 88.0%, and 8.7%, reduces in cybercrime prevention, respectively. Also, for every decrease in communication skills, results in a 10.1% increase in cybercrime deterrence. Furthermore, the probability and [t-statistics] values of.000 and [16.127], .000 and [1.459], and .096 and [-1.684] indicate that the association between investigative skills, analytical skills, and communication skills is significant, since the alpha level of 0.05 is smaller than the p-value except for communication skills.

Hypotheses Two: Digital forensic accounting has no significant impact on digital transformation in Africa.

Table 3: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.775	0.600	0.586	2.29847

Predictors: (Constant), Connectivity, Infrastructure, and Energy.
Source: SPSS output, 2026
Table 3 demonstrates that the R-square value of 0.600 indicates that 60.0% of the variability in digital transformation is accounted for by these digital forensic accounting skills. The Adjusted R-square of 0.586, which adjusts for the number of predictors in the model, is very close to the R-square value, suggesting that the model is well-fitted and the predictors included are highly relevant.

Table 4: Coefficientsa

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	T	Sig.
1	(Constant)		3.610	2.764	1.306	0.000
	Connectivity	0.688	0.126	0.458	5.474	0.000
	Infrastructure	0.356	0.332	0.093	1.073	0.006
	Energy	2.320	0.329	0.541	7.057	0.000

a. Dependent Variable: Digital Transformation

Source: SPSS output, 2026

Table 4 above reveal the individual contributions of each predictor to the model. Analytical skills emerges as the most influential predictor, with a standardized beta coefficient of 0.541 and a highly significant p-value ($p < 0.000$). This indicates that connectivity has a strong and positive impact on digital transformation. In contrast, infrastructure has a much smaller but still statistically significant positive effect on digital transformation ($\beta = 0.093$, $p = 0.006$), suggesting that while energy plays a role, it is less impactful than connectivity. Connectivity, more so, significantly predict digital transformation ($p = 0.000$), as indicated by its positive beta value and sufficient statistical significance.

Discussion of Findings

There were 90 copies of structures questionnaire administered to the targeted respondents and all questionnaires were dully filled and returned by the respondents and also all of these were used for computation. The findings from the first hypothesis reveal that digital forensic accounting plays a significant role in cybercrime deterrence in Africa. The R-value of 86.8% indicates a strong positive relationship between digital forensic accounting and cybercrime deterrence, with the R-square value showing that 75.3% of the variance in cybercrime deterrence is explained by digital forensic accounting initiatives. This aligns with the study of Asah and Obiora (2022), which shows that the empirical analysis of the study indicated that there is a significant and positive relationship between forensic assurance services and fraud detection and prevention at 1% significant level. (see also Mvunabandi & Nomlala, 2022; Okoye & Mbanugo, 2020). The second hypothesis examines the influence of digital forensic accounting on the digital transformation in Africa. The model summary indicated that digital forensic accounting components; Investigative skills, communication skills, and analytical skills explain 60.0% of the variance in digital transformation, demonstrating a very strong model fit. This finding is consistent with studies of Ikpe (2024), which revealed that there is a significant positive effect on the efficiency of forensic accounting skills and fraud prevention in the deposit money banks in Nigeria. (see also Esonwune & Ogiri, 2024; Ogunleye & Fanimokun, 2025; Inweregbu, Ikwudinma & Obiah, 2026).

Conclusion

The study concludes that digital forensic accounting plays a significant role in cybercrime deterrence and digital transformation in Africa. The findings demonstrate a strong positive relationship between digital forensic accounting and cybercrime deterrence, with digital forensic accounting initiatives explaining 75.3% of the variation in cybercrime deterrence. This indicates

that the application of digital forensic accounting techniques can substantially contribute to identifying fraudulent activities, strengthening internal controls, detecting financial irregularities, and preventing cyber-enabled fraud.

The study also concludes that digital forensic accounting skills contribute significantly to digital transformation. In particular, investigative skills, communication skills, and analytical skills jointly explained 60.0% of the variation in digital transformation. This suggests that strengthening digital forensic accounting competencies can enhance the capacity of entities to detect and prevent financial and cyber-related crimes, thereby reducing potential financial losses and supporting a more secure and efficient economic environment. Therefore, the findings establish that forensic accounting is not only an investigative mechanism for responding to fraud after its occurrence but also an important deterrent tool for addressing cybercrime and protecting economic resources in Africa.

Recommendations

1. Financial institutions, government agencies, and other establishments should strengthen digital forensic accounting capacity and skills improvement and provide continuous training and professional development in investigative, analytical, communication, digital-forensic, and data-analysis skills. This would enhance the ability of digital forensic accountants to identify emerging cybercrime techniques, investigate suspicious transactions, and provide reliable evidence for fraud deterrence.

2. Relevant regulatory institutions should integrate digital forensic accounting with stronger digital control and monitoring systems. Such measures would improve the early detection and deterrence of cybercrime, reduce financial losses, and contribute to a safer environment for digital transformation in Africa.

References

Adekunle, A. (2024). Fraud prevention and internal control mechanisms in selected banks in Nigeria. *International Journal of Research and Innovation in Social Science, 8*(7), 287-298 https://dx.doi.org/10.47772/IJRISS.2024.807023

Agbo, A., Idimoasho, M.G., & Kwanum, I. (2023). The role of forensic accounting techniques in preventing fraud in deposit money banks in Nigeria. *European Journal of Accounting, Finance and Investment, 9*(6), 15-23

Akeke, M. N., & Atah, C. A. (2023). Forensic accounting techniques on fraud prevention in tertiary institutions in Cross River State, Nigeria. *Mediterranean Journal of Social Sciences, 14*(1), 46-59

Ali, H.R., & Hafidh, A.H. (2024). Literature review on forensic auditing. *International Journal of Management and Economics, 6*(1), 134-138

Ali, P.I., Ukaegbule, O.H. Obiah, M.E. Akpelu, A.E. (2025). Forensic Accounting in Easing of Entity Fraud in Deposit Money Banks of Nigerian. *Journal of Accounting and Financial Management, 11*(4), 21 – 30

Anowu, D.N., Nyor, T., Agbi, S.E., Nelson, A.I., & Saliu, A.N. (2021). Financial forensic analysis and fraud deterrence in listed deposit money banks in Nigeria. *Gusau Journal of Accounting and Finance, 2*(4), 18-18

Asah, I.M., & Obiora, F.C. (2022). Forensic assurance services and its effect on fraud detection and prevention in manufacturing firms in Nigeria. *Journal of Accounting and Financial Management, 8*(3), 1-12

Awodiran, M.A., Ogundele, A.T., Idem, U.I., & Anwana, E.O. (2023). Digital forensic accounting and cyber fraud in Nigeria. *2023 International Conference on Cyber Management and Engineering (CyMaEn).* Pp. 321 – 326

Bukar, B.A., Adebisi, J.F., & Abdulrahman, S.B. (2025). Forensic investigation and litigation support efficacy on fraud prevention in public agricultural sector in Nigeria. *Global Scientific and Academic Research Journal of Economics, Business and Management, 4*(2), 10-19 https://gsarpublishers.com/journals-gsarjebm-home/

Chima, C.C., & Obiah, M.E. (2021). Forensic Accounting in Mitigation of Corporate Fraud in Nigerian Banks. *International Journal of Financial Research and Management Science, 7*(7), 1 – 35

Chukwuka, O.U. (2022). Internet fraud: the menace of 'yahoo boys' and the deceitfulness of riches 87 internet fraud: The menace of 'yahoo boys' and the deceitfulness of riches. *Sapientia Global Journal of Arts, Humanities and Development Studies, 5*(2), 87 – 97

Cybercrime (Prohibition, Prevention, Etc.) Act, 2015. (2015). Federal Republic of Nigeria Official Gazette.

Dan'azumi, B.E., Yonla, M.N., Gani, B.J., Maram, M.I., & Ahmed, A.G. (2020). The contribution effect of anti-fraud policy mechanism on the financial performance of a selected bank in Nigeria. *African Journal of Research and Management Science, 1*(1), 174-188

Daraojimba, R.E., Farayola, O.A., Olatoye, F.O., Mhlongo, N., & Oke, T.T. (2023). Forensic accounting in the digital age: A U.S. perspective: Scrutinizing methods and challenges in digital financial fraud prevention. *Finance & Accounting Research Journal, 5*(11), 342-360 DOI:10.51594/farj.v5i11.614

El-Yaqub, A.B., & Yahaya, I. (2025). Impact of digital currency on deposit money bank in Nigeria. *International Journal of Research and Innovation in Social Science, IX*(I), 1363 – 1377 https://dx.doi.org/10.47772/IJRISS.2025.9010114

Eneisik, G.E., & Ogbonna, F.I. (2021). Forensic accountants as an expert witness in Nigeria: A literature reflection. *International Journal of Economics and Financial Management, 6*(2), 64 – 78

Ewa, U.E., Adesola, W.A., & Eseneyen, J.M. (2020). Evaluation of forensic accounting techniques in fraud prevention/detection in the banking sector in Nigeria. *International Journal of Finance and Accounting, 9*(3), 56-66

Eze, A., & Osuji, I. (2023). The importance of forensic accounting in fraud prevention. *Journal of Accounting Research, 12*(2), 34-47.

FATF (2020). Financial action task force global standards. Retrieved from https://www.fatf-gafi.org.

Hansa, P. (2022). A descriptive study on frauds in forensic accounting. *St. Joseph's Journal of Business Research, 1*(01), 12-22

Ibukunoluwa, A.A. (2024). Fraud detection and prevention in the Nigerian financial industry. *Walden Dissertations and Doctoral Studies Collection at Scholar Works.* https://scholarworks.waldenu.edu/dissertations

Ikpe, E.O. (2024). Effect of forensic accounting skills and fraud prevention infrastructures on the prevention of fraud in the deposit money banks in Nigeria: Professional accountant perspective. *Journal of Human Resources & Management Science, 6*(7), 217-238

Inweregbu, O.A., Ikwudinma, A.E., & Obiah, M.E. (2026). The Study on The Effect of Tax Fraud on Per Capita Income in 21st Century Nigeria. *Journal of Accounting and Financial Management, 12*(7), 312 – 325 DOI: 10.56201/jafm.vol.12.no7.2026.p312.325

Jaishankar, K. (2008). Space transition theory of cyber crimes. In F. Schmalleger & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 283–301). Prentice Hall.

John-Oti, E., & John-Oti, S.G. (2025). Financial crimes: A comparative study of Nigeria and Chinese approaches to combating the scourge. *IRJEMS International Research Journal of Economics and Management Studies, 4*(5), 59-64 Doi: 10.56472/25835238/IRJEMS-V4I5P108

Kankpang, A.K., Ogar-Abang, J.O., & Animpuye, C. (2024). Forensic accounting and fraud prevention and detection in commercial banks in Nigeria. *AKSU Journal of Management Sciences, 9*(1), 106 – 128

Kazaure, A.A., Yusoff, M.N., & Jantan, A. (2023). Digital forensics investigation approaches in mitigating cybercrimes: A Review. *Journal of Information Science Theory & Practice, 11*(4), 14-39.

Lazarus, S., Button, M., Adogame, A. (2022). Advantageous comparison: Using Twitter responses to understand similarities between cybercriminals ("Yahoo Boys") and politicians ("Yahoo men"). *Heliyon 8: e11142 https://doi.org/10.1016/j.heliyon.2022.e11142*

Muideen, A.A., Abiodun, T.O., Udosen, J.I., & Anwana, E.O. (2023). Digital forensic accounting and cyber fraud in Nigeria. *International Conference on Cyber Management and Engineering (CyMaEn).* DOI: 10.1109/CyMaEn57228.2023.10050992

Mvunabandi, J.D., & Nomlala, B. (2022). The role of forensic auditing techniques in preventing nongovernment organisations' financial statement fraud in South Africa using a proactive approach. *ACRN Journal of Finance and Risk Perspectives, 11:* 105-119 https://doi.org/10.35944/jofrp.2022.11.1.006

Nwankwo, E.P. (2020). The role of information technology in curbing the challenges of internet and cybercrime in Nigeria. *International Journal of Social Sciences and Humanities Reviews, 10*(1), 66 – 76

Nwokoro, C.V., Chima, F.O., Ndom, D.A., & Iheonu, O.M. (2022). Youth's engagement in cybercrime (yahoo-yahoo) in Owerri Municipal of Imo State Nigeria. *Journal of Education & Social Policy, 9*(4), 117 – 128 doi:10.30845/jesp.v9n4p13

Obiah, M.E.; Ukaegbule, O.H.; Okere, O.C.; Eke, F., & Igwe, C.F. (2023). Scientific application in accounting: The fundamentals of forensic accounting and neuroaccounting research. *Journal of Social Sciences & Interdisciplinary Research, 1*(2-1), 17 – 27

Obideyi, O.A. (n.d.). Cybercrime and digital evidence: The Nigeria police force in perspective. *Resource Material Series No. 114:* 157 – 160

Ogunleye, R.O. & Fanimokun, I. O. (2025). Impact of forensic accounting practices and fraud detection and prevention in listed deposit money banks in Nigeria. *International Journal of Applied and Advanced Multidisciplinary Research, 3*(6), 427-442

Ojo-Agbodu, A., Abiola, J., & Ndubusi, E.I. (2022). Effect of forensic accounting on fraud detection and prevention in selected quoted deposit money banks in Nigeria. *Fuoye Journal of Finance and Contemporary Issues, 3*(2), 36-48

Okafor, O.G., Obiora, F. & Onuora, J.K.J. (2022). Impact of forensic audit and financial statement fraud of deposit money bank in Nigeria. *International Academy Journal of Management, Marketing and Entrepreneurial Studies, 9*(1), 88-98

Okeke, E.U. & Okoye, E.I. (2025). Forensic data analytical skills and fraud management in ministries, departments and agencies in south-east Nigeria. *Journal of Contemporary Issues in Accounting, 6*(2), 29 – 53. https://journals.unizik.edu.ng/index.php/jocia/index

Okoye, E.I., Nwoye, U.J., Akuchi, B.N., & Onyema, A.C. (2020). Effect of forensic investigation techniques in detecting occupational fraud in the public sector: A study of ministry of finance, Anambra State. *International Journal of Innovative Finance and Economics Research 8*(1), 117-124

Okoye, K.R.E., & Mbanugo, C.I. (2020). Forensic Accounting a tool for fraud detection and prevention in the public tertiary institutions in South East Nigeria. *European Journal of Education Studies, 7*(6).

Okpa, M.M., Gwambeka, E.J., Waziri, M., & Mamman, S. (2025). Cybercrimes and bank performance: A study of financial technology literacy interventions in Cross River State. *East African Scholars Journal of Education, Humanities and Literature, 8*(10), 576-591 https://doi.org/10.36349/easjehl.2025.v08i10.006

Olagunju O.J., Otu, G.J., & Zamani, A.E. (2025). Protecting Nigeria's sovereignty in the digital age: A review of security measures in e-governance. *British American University Journal of Terminology and Administrative Management, 1*(1), 169 – 186

Oluwamuye, A.D., & Adedipe, O. (2025). The effect of fraud on financial performance of tier 1 deposit money banks in Nigeria. *ICONIC Research and Engineering Journals, 9*(5), 1538 – 1550 DOI: https://doi.org/10.64388/IREV9I5-1712128

Oni, E.O. (2021). Contextualizing corruption in anti-corruption: The perspectives of the independent corrupt practices and other related offences commission (ICPC), Nigeria. *Global Journal of Political Science and Administration, 9*(4), 16-43

Onyema, C.C., Ojo-Agbodu, A.A., & Adebayo, A.M. (2024). Impact of forensic accounting on fraud management: An examination of some selected deposit money banks in Nigeria. *International Journal of Research and Innovation in Social Science, VIII*(IV), 1648 – 1661 DOI: https://dx.doi.org/10.47772/IJRISS.2024.804119

Raji, Y., Igbekoyi, O.E., Ogungbade, O.I., & Nana, O.S. (2023). Forensic audit technology and audit report quality of selected audit firms in Nigeria. *International Journal of Economics,*

Business and Management Research, 7(04), 45 – 64 https://doi.org/10.51505/IJEBMR.2023.7404

Smith, T. (2021). *Prosecution support in financial crimes: A forensic accounting approach*. London: Routledge.

Sutherland, E. H. (1940). White-collar criminality. *American Sociological Review, 5*(1), 1–12.

Ugochukwu, N.J., & Okenwa, O.C. (2021). Effective deploy of digital forensic techniques and the sustenance of material misstatement-free financial reporting in Nigeria. *Journal of Academic Research in Economics, 13*(3), 442-470.

Ukangwa, V.O., et al. (2023). Improving the use of forensic accounting for fraud detection in Nigerian banks. *Journal of Accounting and Auditing, 7*(4), 56-69.

Ukpabi, J.F., et al. (2021). Enhancing financial transparency through forensic accounting in Nigerian banks. *Journal of Financial Governance, 10*(3), 45-58.

Veledar, B., Bašić, M., & Čolpa, A. (2022). State and perspectives of forensic accounting development in Bosnia and Herzegovina. *Journal of Forensic Accounting Profession, 2*(1), 1-18. https://doi.org/10.2478/jfap-2022-0001

Wigwe & Partners. (2025). Nigeria: Cybercrimes (Prohibition, Prevention, Etc.) (Amendment) Act, 2024—Key highlights. *Retrieved from https://www.wigweandpartners.com/news/cybercrimes-act-amendment-2024*