Internet Fraud and Challenges of Redeeming Nigeria's International Image: Issues and Prospects 2015-2025

Onyia Ifeoma K, Assoc. Prof. Canice Esidene Erunke, Dr. Abdullahi Mohammed Abdul

Department Of Political Science, Faculty of Social Sciences, Nasarawa State University, Keffi, Nigeria

DOI: https://doi.org/10.47772/IJRISS.2026.100400394

Received: 15 April 2026; Accepted: 21 April 2026; Published: 25 May 2026

ABSTRACT

Recurrent Internet fraud in Nigeria has significantly damaged the country's international image, particularly through high-profile cases involving foreign victims. This negative perception has imposed various socio-economic costs on Nigerians, including heightened scrutiny during visa applications, restrictions on international financial transactions, reputational embarrassment at global entry points, and reduced trust in cross-border business engagements. This study examines the challenges undermining government efforts to combat internet fraud and restore Nigeria's global reputation. Anchored on Routine Activity Theory (RAT), the research adopts a mixed-method approach, utilizing interviews, questionnaires, and secondary data sources. Findings reveal that the problem extends beyond legislative inadequacy to include poor implementation of existing laws. Key issues identified include inconsistent enforcement mechanisms, infrastructural deficiencies, and insufficient training among law enforcement agencies. Additionally, weak inter-agency coordination creates operational gaps that cybercriminals exploit. Empirical evidence further highlights systemic challenges such as the absence of functional national databases, lack of standardized regulatory frameworks, weak institutional structures, and the erosion of rule of law institutions. The study concludes that addressing these challenges requires not only institutional reforms but also strict enforcement of existing legal provisions. It recommends that the Federal Government ensure effective implementation of the Cybercrime (Prevention, Prohibition, etc.) Act, 2015, particularly through the prompt prosecution of offenders. Such actions would serve as a deterrent, rebuild public trust, enhance Nigeria's international credibility, and improve its attractiveness to foreign direct investment (FDI).

Keywords: Internet fraud, Nigeria, international image, cybercrime, law enforcement, Routine Activity Theory, governance, foreign direct investment (FDI).

INTRODUCTION

The rapid advancement of the internet and digital technologies has revolutionized various aspects of human life, including communication, commerce, and social interactions. However, this digital revolution has also facilitated the proliferation of fraudulent activities, commonly known as internet fraud. Internet fraud, also known as cyber fraud or online fraud, has become a pervasive issue globally, with significant implications for individuals, businesses, and nations. Internet fraud encompasses a broad spectrum of deceptive practices conducted through online platforms with the aim of defrauding individuals, organizations, or governments. These fraudulent activities range from phishing scams and identity theft to more sophisticated schemes like Business Email Compromise (BEC) and advance fee fraud, commonly referred to as "419 scams".

Reep-van den Bergh and Junger (2023) conducted a systematic review and found that the yearly criminal incidence rates in Europe varied from 1 to 3% for online shopping fraud and 1 to 2% for online banking/payment fraud. Some forms of fraud affect less than 1% of the population, while online abuse, such as stalking and threats, affects no more than 3% of the population. Hacking affects 1-6% of people. Morgan (2021) reported that cybercrime remains a threat to every firm in the world and constitutes a serious problem to humanity. Internet frauds have significant global consequences. Internet fraud, for example, was said to have cost the global community $6 trillion per year by 2021, up from $3 trillion in 2015, signifying the largest transfer of economic wealth in history and more profitable than the worldwide trade in all major illegal

narcotics combined, according to Cyber security Ventures. In their analysis titled "2017 Crime Report," Cyber security Ventures, the world's premier researcher and publisher covering the global cyber market, recognized cyber-attacks as the fastest rising crime in the United States, adding that their scale, sophistication, and cost are all increasing.

Law enforcement agencies in seven African countries arrested over 300 suspected cybercriminals involved in mobile banking, investment and messaging app scams, according to Interpol (2025). In an international operation that stretched from November to February, authorities from Benin, Côte d'Ivoire, Nigeria, Rwanda, South Africa, Togo and Zambia uncovered cross-border criminal networks that defrauded more than 5,000 victims. In Nigeria alone, 130 individuals were arrested, including 113 foreign nationals, for their roles in scams such as online casino fraud and fraudulent investment schemes. These alleged criminals often used digital assets to conceal illicit proceeds, recruiting individuals from various countries to execute the schemes in multiple languages.

Since Nigeria became an independent state, the issue of fraud has always maintained a constant presence in Nigeria's socio-economic mainframe. Fueled by endemic socio-economic troubles ravaging the Nigeria society, Nigerians over time have been forced to dive into unscrupulous means of survival such as armed robbery, drug trafficking, money ritual, kidnapping and advanced fee fraud popularly known as '419'. Despite the assumed financial break-through by the practitioners, the act has devastating social and economic consequences for the country. According to Opaluwa (2024), cybercrime in Nigeria cost the country $9.3 billion. Sadly, the country's image has also suffered as we tend to lose global trust and integrity which is as a result of the illicit activities by some Nigerians, who have now turned cyberspace into an arena for committing criminal activities known as cybercrime.

Nigeria is one of the African countries that experience hundreds of millions of cyber attacks annually. For instance, in 2017, the country experienced a total loss of N198.6 billion, equivalent to $649 million (Adepetun, 2018), while in 2018, it was reported that the loss to cyber attacks in the country was $800 million (N288 billion) (Week, 2019). Similarly, in a 2019 report, cybercrime has cost Nigeria an average of N127 billion ($330 billion) (Sule et al., 2021). More broadly, according to a report in 2022, Nigeria loses an average of N200 billion yearly to cybercrime (Onuoha, 2022). These data indicate the considerable effect of internet fraud on the economy of Nigeria. A cause for even more significant concern is a report that states that if internet fraud continues to be unchecked or properly combated, the country is projected to lose about $6 trillion by 2030 (Adeniyi, 2021). In Nigeria and other African countries, financial institutions, governments, and industries are the primary targets for hackers.

In 2019 alone, the FBI received thousands of complaints related to Business Email Compromise (BEC) in the US. The total losses related to these complaints were up to $1.1 billion. Obviously, this became a national security threat to the country. Nigeria's name seems to have reechoed more than any other foreign country in these wire-related frauds. In fact, in the last 15 years, international law enforcement groups around the world, such as the FBI, Interpol, and Canadian and Italian agencies, have successfully indicted and arrested various Nigerian scammers. Though there are many Nigerians doing very well abroad, the relatively high numbers of internet crimes linked to Nigeria have resulted in a kind of national stereotyping. In fact, FBI's website has a section advising folks on how to avoid "The Nigerian Letter" or "419" Fraud (FBI, 2022).

Before the technological innovation which brought the Internet, the financial fraudsters known as "419-ners" that operated in popular cities in Nigeria such as in Lagos and Abuja, were mostly educated or illiterate adult men and women, who specialized in using fax machines to defraud unsuspected foreigners and Nigerians of their hard-earned money (Ezea, 2017). However, in the recent times, the tides have changed. The technological innovations in social media networks have popularized youths in the business of defrauding unsuspected foreigners and Nigerians today. Social media has made most Nigerian youths game players in the waters of financial frauds and cybercrimes in the country today. In Nigerian streets today, many youths are seen driving very expensive cars, building mansions and reveling in luxurious lifestyles which baffle most decent citizens, and which has raised a worrisome thought about the future of the country. However, this has put Nigeria under negative scrutiny and that is not good for our image in international relations. Nigeria continues to battle cyber fraud, as many youths turn to "get-rich-quick" schemes involving online theft. In response, the Economic and

Financial Crimes Commission (EFCC) has actively been on the lookout, arresting those identifying as "Yahoo boys." The National Drug Law Enforcement Agency (NDLEA) has also apprehended suspected fraudsters during their operations. According to Ojiego (2021), approximately 70-80% of the wealth of Nigerians is often traced to unverifiable sources.

Recently, internet fraud has emerged as a growing threat to national security in Nigeria. Recognizing the threat e- crimes pose to Nigeria's international image and to eradicate it, the Nigerian government has made several attempts to curb the phenomenon in the society, including the enactment of laws such as the comprehensive cyber security policy document adopted in 2015, which outlines the government's provisions and efforts to establish a safer digital environment. In addition, is the National Information Technology Development Agency (NITDA) established in 2015 to regulate and develop the country's information technology sector. NITDA has since developed cyber security guidelines and policies for government agencies and organizations in Nigeria to follow. The law also establishes a National Cyber security Fund to finance the country's cyber security efforts. Despite the laws and establishments aimed at curbing cybercrime in Nigeria, the country still faces cyber security challenges.

Statement of the Problem

The advent of the internet has undeniably transformed the world, connecting people across borders, enabling seamless communication and fostering economic growth. However, with this advancement, a darker side has emerged, internet fraud, "419 scams" or "advance fee fraud," in Nigeria. Unfortunately, it has gained notoriety as a hub for such fraudulent activities affecting Nigeria's international image especially from 2015 - 2025. Nigeria has gained notoriety for being a hotspot for various forms of internet fraud, posing significant challenges to its international image and reputation. Nigeria's international image crisis has been a contentious issue resulting from adverse effects created by stringent socio-economic and political conditions facing Nigerians.

According to the Federal Bureau of Investigation (FBI) report Nigeria ranks 16th in the world in terms of internet crimes. Unfortunately, the country's image has also suffered as a result of the unscripted activities of some Nigerians using the internet as a channel for the perpetration of criminal spamming activities. The quest for fast wealth acquisition through internet fraud among the Nigerian youth has become a common lifestyle. Majorly between 2015 - 2025, the reputation of Nigeria and Nigerians has suffered greatly as internet scams and fraud have taken on increasingly scary. On Nov. 3, 2024, the Nigeria Police Force executed a major operation leading to the arrest of 130 individuals suspected of internet fraud and hacking. Among those detained were 113 foreign nationals, predominantly Chinese and Malaysian, and 17 Nigerians. This operation took place in a building in Abuja. An INTERPOL initiative known as Operation Jackal III led to the arrest of 300 suspects and the seizure of $3 million in assets in a sting operation culminating in July 2024 (Eboh - Reuters News, 2025). According to the EFCC, the foreign nationals were allegedly involved in orchestrating large-scale internet fraud schemes and recruiting Nigerian youths into illicit cyber activities.

This issue has extended internationally, affecting Nigeria's reputation. Recurrent internet fraud and Nigeria's international image fraud cases involving foreign nationals have created a negative perception of Nigeria abroad. The cost of this stereotyping to Nigerians ranges from increased scrutiny during visa applications to offshore cash transactions, embarrassments at various airports around the world, lack of trust when dealing with foreign companies and restriction from using some international payment platforms. Many genuine Nigerian businesses seeking international partners cannot grow with this kind of stereotyping. Unfortunately, this image has impacted Nigerians, complicating international relations and travel. The unattractive and soiled image of Nigeria has been a result of the questionable attitude of some Nigerians who specialize in internet fraud, credit card manipulation, money laundering etc. Nigeria has picked up quite a reputation as the epicenter of international vice. Internet fraud brings down a nation and no doubt Nigeria has had its fair share.

Another, troubling fact is that various attempts and efforts have been done by Nigerian government in combating internet fraud; however, the outcomes leave much to be desired. Eze-Michael (2021) noted that although some laws regulate the activities of cyberspace, such as the Economic and Financial Crimes Commission Act, the Money Laundering Act and the Advance Fee Fraud Act, Yahoo business remains in

operation. In light of the foregoing, this study seeks to contribute to the existing body of knowledge on internet fraud and Nigeria's international image.

Research Questions

Based on the problem stated, the following research questions were raised;

i. What are the strategies put in place by the Nigeria government aimed at enhancing international image in the face of internet fraud?

ii. What are the challenges hindering Nigeria's government efforts to overcome internet fraud as it relates to redeeming Nigeria's international image?

Objectives of the Study

i. To examine strategies put in place by the Nigeria's government aimed at enhancing international image in the face of internet fraud?

ii. To evaluate challenges hindering Nigeria's government efforts to overcome internet fraud as it relates to redeeming Nigeria's international image?

Research Propositions

i. Successive Nigerian governments have made diverse attempts to curb the menace of cybercrime such as Nigerian Cybercrime Act in 2015.

ii. Porous nature of the internet, lack of infrastructure and national functional databases, lack of standards and national central control are the major challenges hindering Nigeria's government efforts to overcome internet fraud and redeeming Nigeria's international image.

Conceptual Framework

Internet Fraud

Due to its complex and constantly evolving nature, internet fraud can take various forms depending on the tactics and techniques employed by the offenders. As a result, multiple scholarly publications have previously sought to define internet fraud other wisely refer to cybercrime across different historical periods and under diverse conditions. Therefore, there is yet to be a generally accepted definition for the term. However, Idowu (2021) defined it as illegal activities committed via the internet and other digital networks, devices, and technologies. It involves using computers, software, and online platforms to conduct illicit activities such as hacking, financial fraud, publishing of disapproved electronic information, breach of confidentiality, data interference, system interference, illegal interception, and identity theft, among others. Analyzing this definition implies that internet fraud encompasses a range of offences in which computers play a significant role, including unauthorised access to private or company information, violation of network integrity, infringement of privacy, industrial espionage, and computer software piracy.

According to Bernik (2024), internet fraud can be defined as unlawful activities conducted through electronic means that aim to target computer systems and data processed by the devices. The implication of this study is that it regards internet fraud as a malicious activity conducted from a computer or against a computer or network. It is a computer-mediated act that is deemed illegal or illicit by certain institutions and can be carried out across global electronic networks.

International Image

Holsti (1996) clarifies this point when he defined image as an individual's perception of an object, fact or condition in terms of badness or goodness as well as the meaning ascribed to or deduced. If this definition is

extrapolated from that, it can be concluded that image-building must necessarily constitute a fundamental element of leadership character and a nation's foreign policy, suggesting that the way a country is perceived is a function of her national image. This is an internal psychological concept, the sum total of what penetrates our cognition and is organized into a rather complex structure of subjective knowledge. Anton, (2021) describes external image as the entirety of all perceptions, feelings, and judgments that people make about others. It is how we perceived others. This perception springs from earlier experiences or contacts with the person or organization and the outcome of these contacts and evaluation. The way we perceive and judge people modifies our interaction towards them.

The external image of a nation is like a mirror through which a nation is viewed by other countries as they relate among themselves. It is the perception of a country by other nations of the world.

EMPIRICAL REVIEW OF RELATED LITERATURE

Cyber Security Measures and Policies to Mitigate Internet Fraud in Redeeming International Image

Eluwah (2021) carried out a study on "Cyber awareness and education in Nigeria: An assessment. A quantitative approach was employed for data collection from 401 respondents using selected questions and statements assessing items in a self-structured questionnaire to assess respondents' awareness and education levels related to cybercrime; cyber security; and government cyber awareness initiatives; attitudinal and behavioural measures to forestall cyber security incidents; and the impact of government cyber awareness initiatives. The results showed that respondents had fair awareness of cybercrime and cyber security but very poor awareness of government initiatives aimed at achieving cyber security awareness. Attitudinal and behavioural measures to mitigate cyber security incidents were observed to be highly and moderately positive respectively.

A major highlight revealed from the research was the very poor impact of government initiatives on cyber security awareness and education. The study essentially reveals that the government should intensify the publicity and visibility of its cyber-security awareness and education initiatives. Both the reviewed study and the pioneering study are related, as both focus on cyber awareness. The area of divergence is related to the objectives, scope and methods. Also, the study did not proffer solutions to their findings, especially in addressing Nigeria's current cyber security measures and policies to mitigate internet fraud in redeeming Nigeria's international image.

Eke (2023) examined the awareness and perception of internet fraud among Nigerian youths. The theoretical framework Media technological determinism and technology-enabled crime theories underpinned the study as a theoretical framework. The study adopted a descriptive research design. A questionnaire was used for data collection and, percentages and weighted mean scores (WMSs) were used for data presentation. The findings of the study revealed that the level of awareness of the epidemic of internet fraud was very high and that there were more people associated with internet fraud among young people. The study recommended that, because the level of awareness of the epidemic of internet fraud is high, a massive awareness campaign should be undertaken to educate youths in Nigeria about the knowledge on the consequences of internet fraud.

Challenges Hindering Government Efforts to Overcome Internet Fraud and Redeeming International Image

Egbue (2019) studied globalization and transnational advance fee fraud: a study of perceptions of undergraduates in Southeastern Nigeria. The study used of a questionnaire, focus group discussions and interviews to examine the perception of undergraduates in southeastern Nigeria about certain aspects of this scam. This is because these youth are considered to be most predisposed, by virtue of their education, constant access to the internet, unsatisfied financial needs and the threat of imminent unemployment, to temptations to engage in advance fee fraud. The findings indicated that undergraduates were very familiar with advance fee fraud as a major economic activity. Furthermore, it was found that undergraduates generally viewed internet scam as less grievous than other irregular sources of income, largely because the victims were mainly foreigners, and also because there was usually no direct contact with victims. The study made

recommendations for improved enlightenment of youth, stricter overall anti-corruption law enforcement, and increased employment opportunities for undergraduates.

The study often gave clear indications as to the areas in which government was required to effect changes towards eradication of advance fee fraud. But did not explore the challenges hindering Nigeria's government efforts to overcome internet fraud and redeeming Nigeria's international image which is a gap in knowledge.

Further results of the secondary sources revealed related cybercrime to include; quest for wealth, Poor implementation of cybercrime laws, and corruption among others. With these alarming results, schools and National development would be at catastrophic in different ramifications of economy activities. The study suggests that; schools should form personality assessment committee to assess students attitudes toward cybercrimes, Personal Identification Number (PIN) should not be made known to unknown persons, and Government should enact stringent laws and prosecute perpetrators of such act without discrimination among others. What were not analyzed in the study are the challenges hindering Nigeria's government efforts to overcome internet fraud and redeeming Nigeria's international image which is a focus of this study.

Theoretical Framework: Routine Activity Theory (RAT)

Routine Activity Theory (RAT) was first formulated by Cohen and Felson (1979). Cohen and Felson's Routine Activity Theory applies to internet fraud by considering an attractive target, a motivated offender, and the absence of a capable guardian as criteria for a cyber attack, thereby shedding light on potential vulnerabilities within Nigeria's cyber security landscape. The focus of Routine Activity Theory is the study of crime as an event, highlighting its relation to space and time, emphasizing its ecological nature and implication. According to RAT, three factors or elements are required for a crime to be present. These elements include: the criminal must be motivated to commit a crime, a suitable target and the absence of a capable guardian who can prevent the crime from happening. These three elements must converge in time and space for a crime to occur. Cohen and Felson (1979) posit that the routine of activities people partake in day and night makes some individuals more susceptible to being viewed as suitable targets by a rationally calculating offender. Routine activities theory relates the pattern of offending to the everyday pattern of social interaction. Crime is therefore normal and is dependent on available opportunities to offend.

The theory is very relevant in that it has successfully and empirically demonstrate that a nation needs to increase it definitions for crime by campaigning rigorously against cyber-crime with the hope that the awareness being raised will form excess opinions as against the criminal minded persuasions that will sway the rational decisions of a citizens to be law keepers instead of becoming law breakers by associating with their folks. Similarly, the theory is relevant as it laid down the basic foundations for fighting crimes like cyber security by its three conditions. It required that three elements be present for a crime to occur: a motivated offender with criminal intentions and the ability to act on these inclinations, a suitable victim or target, and the absence of a capable guardian who can prevent the crime from happening. Therefore, a good crime fighter will just concentrate on denying citizens or would be criminals these three elements and society is successfully navigated away from crime.

METHODOLOGY

This study employed the mixed research design, which involves the use of questionnaire as main instrument of data collection and semi-structured interview. The target population of this study stand at two thousand, two hundred and seventeen (2,217) consisting of officials of the International Criminal Police Organization (INTERPOL), Economic and Financial Crimes Commission (EFCC), National Drug Law Enforcement Agency (NDLEA), Federal Ministry of Justice, National Information Technology Development Agency (NITDA), Federal Ministry for Foreign Affairs (MFA) and the National Bureau of Statistics (NBS). The sample size representative of the target population in this study is **327**. It is determined based on the Krejcie and Morgan sample size formula.

In terms of the sampling method to be applied, the snowballing method was mainly use for selection of participants for this study. Data for the research was collected using three main instruments: interview,

questionnaire and secondary sources. There are two different techniques of data analysis that were used by the researcher, namely qualitative and quantitative techniques. Under the qualitative technique, the study put emphasis on formulating themes of the objectives using content analysis, under this technique, the study commonly adopts thematic analysis that mainly supports in conducting in-depth examination. On the other hand, a quantitative technique was also adopted for analyzing the findings. Under this technique, descriptive statistics such as simple percentage, frequency and table were employed.

Data Analysis and Interpretation of Results

Three hundred and twenty-seven (327) copies of questionnaire were administered while three hundred and nineteen (319) copies of questionnaire representing 98% were duly completed and retrieved. Seven (07) copies of questionnaire representing 2% were not retrieved and all efforts to retrieve them proved abortive as some respondents could not be found on sit as a result of official assignment and leave. Therefore, the presentation and analysis was done based on the 319 retrieved copies of questionnaire.

Table 1: Responses on Nigeria's current cyber security measures and policies to mitigate internet fraud in redeeming Nigeria's international image

Responses	**Frequency**	**%**
Advance Fee Fraud and Other Fraud Related Offences Act 2006	34	11
Promulgation of the Cybercrime (Prohibition, Prevention, Etc.) Act, 2015	52	16
Money laundering Act and the Advance Fee fraud Act	43	13
Economic and Financial Crimes Commission Act 2004	50	16
Nigerian Financial Intelligence Unit (NFIU)	46	14
All of the above	37	12
	56	18
Total	**319**	**100**

Source: Field Work, August (2025).

The question in Table 1 aimed to determine whether participants are aware of any kind of mechanism and machineries deployed by Nigeria to mitigate internet fraud in redeeming Nigeria's international image. Table 1 indicates that Advance Fee Fraud and Other Fraud Related Offences Act 2006 (11%), Promulgation of the Cybercrime (Prohibition, Prevention, Etc.) Act, 2015 (16%), Money laundering Act and the Advance Fee fraud Act (13%), Economic and Financial Crimes Commission Act 2004 (16%), Nigerian Financial Intelligence Unit (NFIU) (12%) while 18% which is the majority indicated all of the above mentioned options.

However, the respondents have contradictory views on Nigeria's current cyber security measures and policies to mitigate internet fraud in redeeming Nigeria's international image. Successive Nigerian governments have made diverse attempts to curb the menace of cybercrime. Such attempts recorded debatable degrees of success. Huge sums of money are often budgeted annually to give the anti-cybercrime and other forms of criminality fight the necessary fillip as part of government's drive to encourage local and foreign investors/investments. By far the most significant push in the battle against cybercrime is the promulgation of the Cybercrime (Prohibition, Prevention, Etc.) Act, 2015. The provisions of the Act are meant to curb the notorious activities of cybercriminals vis-à-vis their implication on the country's local and international image. The Act has eight

major parts including objectives and application of the law, protection of critical national information infrastructure, offences and penalties, duties of financial institutions, administration and enforcement, arrest, search, seizure and prosecution, jurisdiction and international co-operation and miscellaneous.

While the Act contains eight major parts, part three which isolated offences and penalties is particularly relevant. Offences covered by this section include those against critical national information infrastructure, computer-related forgery and fraud, cyber terrorism, identity theft and impersonation, child pornography and related offences, cyber stalking, cyber squatting, among others. Like many pieces of legislation, the implementation of the Act has been confronted with some challenges which are narrowed down to lack of harmonized global cybercrime laws, weak access to internet evidence and an increase in the number of internet users (Suleiman et al, 2017).

Nigeria as a country currently has some laws that regulate the activities of the cyberspace. Such as the Economic and Financial Crime Commission (EFCC) Act, Money laundering Act and the Advance Fee fraud Act. A ricochet of an adverse effect caused by internet fraud is that Nigerian ISPs and email providers are being black-listed in e-mail blocking systems across the Internet. The implication of this is that some countries websites like eBay do not receive materials from Nigerian ISPs. All the above can be very detrimental to Nigeria's image in the international system causing numerous strain on its political, economic and diplomatic relations with other states. This, therefore, has necessitated Nigeria to take a stance in combating the issue of internet fraud and reform its image in the international system (KII/Abuja/Male/51/August/2025).

Aside the Cybercrime (Prohibition, Prevention, Etc.) Act, 2015, Nigeria's former National Security Adviser (NSA), Retired Major- General Babagana Mungonu, also revealed that the government has established a National Cyber Security Policy and Strategy Roadmap to address emerging threats in the cyber domain and enhance progressive use of cyberspace in Nigeria. According to the Guardian (2021) the NSA made the disclosure in Lagos at the Cyber Secure Nigeria Conference 2021, with the theme "The Future of Cyber Security in Nigeria's Digital Transformation".

The fundamental aim of the National Cyber Security and Strategy Roadmap is to have a harmonized security strategy that would respond to the dynamism of the national security threat landscape. The document listed five key national cyber security threats which pose significant challenges to the country and are inimical to Nigeria's national growth and security. These include cybercrime, cyberespionage, cyber conflict, cyber terrorism and child online abuse and exploitation. However, despite the existence of government-induced cybercrime mitigation interventions, cybercriminal activities in Nigeria have not shown any significant sign of abatement (KII/Abuja/Male/48/August/2025).

Ebem et al. (2017) averred that the BVN project was introduced to enhance financial security which was already failing to arrest password and pin theft. Accordingly, during the heat of registration for BVN, customers' bank accounts were suspended to enable them obtain the BVN within the stipulated timeframe. However, during the interval, cybercriminals were reported to have impersonated legitimate bank staff by contacting unsuspecting bank customers, requesting their bank details, and promising to unlock their suspended bank accounts. This resulted in the loss of a substantial amount of money after the accounts have been activated by the bank when the customer eventually registered and obtained the BVN. To date, cyber fraudsters are known to be visiting sites like 'harvest' phone numbers and truecaller.com, to access registered phone numbers. Text messages are sent to such phone numbers, telling the owners that their BVN registration was incomplete and therefore, request for the first or last names of the owners. The financial information (ATM pin, account number, etc.) of the owners of these numbers is required to rectify the issue observed and to which correct response eventually results in their being defrauded.

Nigerian government has made several attempts to curb the phenomenon in the society, including the enactment of laws such as the comprehensive cybersecurity policy document adopted in 2015, which outlines the government's provisions and efforts to establish a safer digital environment. In addition, is the National Information Technology Development Agency (NITDA) established in 2015 to regulate and develop the country's information technology sector. NITDA has since developed cyber security guidelines and policies for government agencies and organisations in Nigeria to follow. The law also establishes a National Cyber

security Fund to finance the country's cyber security efforts. Despite the laws and establishments aimed at curbing cybercrime in Nigeria, the country still faces cyber security challenges, including inadequate cyber security infrastructure, lack of awareness and education about cyber security, and the prevalence of cybercrime that still poses a significant challenge (KII/Abuja/Male/41/August/2025).

The Office of the Nigerian National Security Adviser (2014) defined the National Cyber Security Strategy (NCSS) "as a road map that seeks to provide cohesive measures and strategic actions for stakeholders to ensure a safe, secure and resilient of the country's presence in cyberspace, building and nurturing trusted cyber- community" (Osho & Onoja, 2015). With the rise of cyber threats such as malware, phishing, ransomware, and other malicious activity targeting Nigerian citizens and businesses alike, a firm cyber security policy must be implemented to protect individuals and organisations from potential harm. Nigeria has several cyber security policies and frameworks that guide its efforts to combat the growing cyber-attacks in the country. These policies and frameworks aim to create secure cyberspace in Nigeria, protect critical information infrastructure, and promote cyber security awareness.

Before 2015, Nigeria did not have dedicated legislation on cybercrime; instead, existing laws whose provisions were deemed relevant to preventing cyber-related crimes were utilised by law enforcement agencies (Awhefeada & Bernice, 2020). Presently, Cybercrime (Prohibition, Prevention, etc.) Act of 2015 is Nigeria's primary legislation governing cybercrime, making the country more legally equipped to combat cybercrime. Although, before the implementation of this Act, other legislation existed to address cybercrimes (Adeniyi, 2021). As a result, it is essential to acknowledge the enabling laws to address cybercrime before enacting the 2015 Cybercrime Act.

The Economic and Financial Crimes Commission (Establishment) Act of 2004 established the Economic and Financial Crimes Commission (EFCC), which is an agency tasked with investigating and prosecuting economic and financial crimes, which includes advance fee fraud (commonly known as 419), computer credit card fraud, illegal charge transfers, contract scam, fraudulent encashment of negotiable instruments, among others (Adeniyi, 2021). The EFCC has played a crucial role in Nigeria's fight against cybercrime by investigating and prosecuting cybercriminals.

The Advanced Fee Fraud and Other Related Offences Act of 2006 criminalises various forms of fraud, including advance fee fraud (commonly known as 419), a prevalent form of cybercrime in Nigeria. The act makes it an offence to commit fraud by false pretence. The act also stipulates that inducing another person to confer a benefit under the front that the benefit will be paid for is also an offence (Adeniyi, 2021). The Act criminalises financial transactions that involve proceeds from unlawful activities (Awhefeada & Bernice, 2020). These provisions in the Advanced Fee Fraud and Other Related Offences Act serve as legal measures to prevent and prosecute fraudulent activities, including those carried out electronically in Nigeria.

Additionally, the National Identity Management Commission Act 2007 established the National Identity Management Commission (NIMC), responsible for maintaining a national database of citizens' biometric data. This database is essential for combating cybercrime, particularly crimes involving identity theft, as it identifies and tracks cyber criminals. Despite the existence of the National Identity Management Commission (NIMC) Act, its provisions may not be entirely effective in prosecuting cybercriminals. Cybercriminals can evade detection by falsely claiming they have lost their National Identity cards or using modern photographic techniques to alter their appearance. Such tactics enable them to conceal their true identity and avoid being caught, thus rendering the provisions of the NIMC Act insufficient in combating cybercrime in Nigeria (KII/Abuja/Male/35/August/2025).

Table 2: Responses on the major challenges hindering Nigeria's government efforts to overcome internet fraud and redeeming Nigeria's international image

Responses	**Frequency**	**%**
Porous nature of the internet	82	26

Lack of infrastructure and national functional databases	56	18
Lack of standards and national central control	55	17
Lack of defined structures by security agencies	64	20
Collapse of Rule of Law Institutions	62	19
Total	**319**	**100**

Source: Field Work, August (2025).

Table 2's question seeks to understand the major challenges hindering Nigeria's government efforts to overcome internet fraud and redeeming Nigeria's international image. Statistically 82; 26% indicated porous nature of the internet, 56; 18% indicated lack of infrastructure and national functional databases, 55; 17% indicated lack of standards and national central control, 64; 20% indicated lack of defined structures by security agencies while 62 respondents accounting for 19% indicated collapse of rule of law institutions as the major challenges hindering Nigeria's government efforts to overcome internet fraud and redeeming Nigeria's international image. This is supported by the following information from both interview and secondary sources:

While the enactment of the legislation is commendable, the complexities of internet fraud often make them elusive to legislative frameworks. The challenges faced in Nigeria revolve not merely around legislation but its effective implementation. There are discernible issues, such as inconsistent enforcement, which might be attributed to both infrastructural inadequacies and a potential lack of adequate training for the enforcing bodies. Moreover, coordination failures among various law enforcement agencies further exacerbate the problem ,leading to scenarios where cybercriminals might find lacunae to exploit (KII/Abuja/Female/45/ August/2025).

In the context of the digital era, having the right human resources is paramount in tackling cyber security threats. Like many countries, Nigeria faces significant challenges in acquiring specialised personnel to manage cyber threats' intricate dynamics. Shackelford et al. (2016) emphasise that even the most fortified cyber defences can be rendered obsolete without tailored technological tools that adapt to region-specific challenges. Lastly, it's not only technical specialists who need to be in the loop. The broader populace, spanning various sectors, needs a foundational understanding of cyber risks.

The spate of unemployment in Nigeria is alarming and growing by the day. Companies are folding up and financial institutions are going bankrupt. Companies are also embarking on mass sacks of staff. Financial institutions have put unreasonable age barriers on who is eligible to apply for jobs and embarked on mass lay-offs of staff based on ad-hoc decisions. The rich are getting richer and the poor are getting poorer. Insufficient basic amenities and an epileptic power supply have grounded small scale industries. The Internet is free for all with no central control. Hence, the state of anarchy presently experienced. A hostile party using an internet connected computer thousands of miles away can attack internet- connected computers in Nigeria as easily as if he were next door. It is often difficult to identify the perpetrator of such an attack, and even when a perpetrator is identified, criminal prosecution across national boundaries is problematic (KII/Abuja/Female/36/August/2025).

According to Anozie (2023), in Nigeria, due to the limited private sector investment, low industrialization and economic growth as well as the economy's inability to absorb the 4 to 5 million new entrants into the Nigerian labour market each year, unemployment is predicted to remain a significant challenge in 2023 and beyond. The national unemployment rate rose from 23.1% in 2018 to 33.3% in 2020, according to the National Bureau of Statistics. This rate rose to 37.7% in 2022 and will increase even more to 40.6 percent in 2023. Cyber security in Nigeria is currently at a critical juncture due to the increasing prevalence and sophistication of cyber threats and the country's growing dependence on technology. Nigerian citizens and businesses are increasingly vulnerable to malicious attacks. With an estimated population of over 200 million, Nigeria has become one of

the most prominent targets for cybercriminals (Sule et al., 2021). Cyber security threats such as malware, phishing scams, ransomware attacks, and data breaches are becoming increasingly common in this West African nation. While there have been some significant strides in cyber security awareness and capability in recent years, such as the establishment of the National Cyber security Policy and Strategy in 2014 and the Cybercrime Prohibition Act 2015, the reality is that Nigeria remains vulnerable to cyber-attacks.

A cornerstone of Nigeria's legislative response to this challenge is the Nigerian Cybercrimes Act of 2015. This act was introduced as a landmark initiative to criminalise cyber offences, symbolising a significant step toward creating a safer digital environment in the country. Yet, despite its ambition, the Act has faced criticism and challenges. There are noticeable inconsistencies in its enforcement, highlighting the struggle of translating policy into practice. Furthermore, the rapidly evolving nature of cyber threats has sometimes outpaced the adaptability of this legislative framework, emphasising the necessity for periodic revisions and updates. Moreover, while Nigeria has endeavoured to foster international collaborations to tackle cybercrime, there's also a palpable need to look inward. The evident lack of synergy among national agencies has sometimes hindered a cohesive and unified response. For the legislative and regulatory measures to be effective, it's recommended to strengthen the enforcement mechanisms and enhance inter-agency coordination. Moreover, the dynamic nature of cyber threats demands that the legal framework undergo continuous revisions to remain relevant and practical (KII/Abuja/Female/48/August/2025).

DISCUSSION OF FINDINGS

i. The result for objective one reveals that Nigerian governments have attempted to combat internet fraud through the promulgation and deployment of the Cybercrimes (Prohibition, Prevention, etc.) Act 2015. The Nigerian police and the Economic and Financial Crimes Commission (EFCC) have waged continuous war against cybercriminals by arresting and prosecuting many suspects. However, despite government's efforts, consistent tactic updates and changes in strategies have frustrated the apprehension of many cybercriminals. The findings from examining government documents paint a picture of a nation that has made significant strides in establishing a legal and strategic framework for cyber security.

ii. The result for objective two reveals that the challenges faced in Nigeria revolve not merely around legislation but its effective implementation. There are discernible issues, such as inconsistent enforcement, which might be attributed to both infrastructural inadequacies and a potential lack of adequate training for the enforcing bodies. Moreover, coordination failures among various law enforcement agencies further exacerbate the problem, leading to scenarios where cybercriminals might find lacunae to exploit. This is supported by result from table 2 which reveals that porous nature of the internet, lack of infrastructure and national functional databases, lack of standards and national central control, lack of defined structures by security agencies and collapse of rule of law institutions are the challenges hindering Nigeria's government efforts to overcome internet fraud and redeeming Nigeria's international image.

CONCLUSION

The core of this work delves into understanding the dimensions of internet fraud within Nigeria and its implications on Nigeria's international image. Given the broad digital landscape and Nigeria's place in it, the results of this research shed light on the intricate relationship between cybercriminal internet fraud and Nigeria's international image. Nigeria's international image crisis is enveloped in the poor international perception of the Nigerian business environment, poor perception of Nigeria within the diplomatic circle and the international perception of corruption in Nigeria. This is seen in the withdrawal of Foreign Direct Investments (FDI), ill-treatment/unwarranted suspicion of Nigerian nationals abroad, the deportation of Nigerian nationals, visa ban, and the corruption perception index of Nigeria by Transparency International, World Bank, and other related reports.

Therefore, it is concluded that internet fraud is no doubt an image trauma for Nigeria; it is a source of concern and embarrassment for the nation.

RECOMMENDATIONS

i. More cyber security management such as data encryption and careful management of personal information in the internet were also identified as a way of keeping fraudsters from gaining access to personal information of people. There's a pressing need to revisit and update the Nigerian Cybercrimes Act of 2015. While it stands as a testament to the nation's early recognition of digital threats, the evolving nature of cybercrime demands regular policy revisions. Updated regulations should address current challenges and anticipate future threats.

ii. The Federal Government should ensure the due enforcement of the relevant sections of the Cybercrime (Prevention, Prohibition, etc.), Act of 2015 by ensuring that apprehended cybercriminals are promptly prosecuted to serve as deterrent to other potential internet fraudsters. The prosecution of such criminals will also serve to restore public confidence in the fight against cybercriminals as well as attract foreign direct investment (FDI) in the country.

REFERENCES

1. Adeniyi, I.A. (2021). Cyber security in Nigeria: appraising cybercrime, the existing legal framework, the challenges and the way forward. SSRN Electronic Journal, 2(4): 43-46.
2. Adepetun, A. (June 7, 2018). Financial losses to cybercrimes on steady rise to N198b. The Guardian Nigeria News - Nigeria and World News.
3. Alghamdi, M. (2020). A Descriptive study on the impact of cybercrime and possible measures to curtail its spread worldwide. International Journal of Engineering Research and Technology, 9(3): 43-54.
4. Antons, K. (2021). Praxis der gruppendynamik: übungen und techniken' practice of group dynamics: exercises and techniques in german' (ed.). göttingen: hogrefe verlag gmbh & co. kg.
5. Awhefeada, u.v., & bernice, O.O. (2020). Appraising the laws governing the control of cybercrime in nigeria. journal of law and criminal justice, 8(1): 52-63.
6. Bernik, I. (2024). Cybercrime. Cybercrime and Cyberwarfare, 1–56.
7. Cohen, L.E., and Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 588 – 608
8. Ebem, D.U., Onyeagba, J.C., & Ugwuonah, G.E. (2017). Internet Banking: Identity Theft and Solutions - The Nigerian Perspective. Journal of Internet Banking and Commerce, 22(2), 1-15.
9. Eboh, C. (January 10, 2025). Economic and Financial Crimes Commission (EFCC) on Friday arraigned a group of individuals from the 792 alleged internet and cryptocurrency fraud suspects apprehended last december in Lagos. Reuters News.
10. Egbue, N.G. (2019). Globalization and transnational advance fee fraud: A study of perceptions of undergraduates in Southeastern Nigeria. The Nigerian Journal of Sociology and Anthropolo, 7(1): 61-78.
11. Eke, C. (2023). Awareness and perception of internet fraud epidemics among Nigerian youths. African Journal of Social and Behavioural Sciences (AJSBS), 14(3): 1370-1383.
12. Eluwah, D. (2021). Cyber awareness and education in Nigeria: An assessment. Research Gate.
13. Eze-Michael, E. (2021). Internet fraud and its effect on Nigeria's image in international relation. Covenant Journal of Business and Social Sciences (CJBSS), 12 (1): 20 – 26.
14. Federal Bureau of Investigation. (2022). Internet Fraud. Available at: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/internet-fraud.
15. Garba, A., & Bade, A. (2021). The current state of cybersecurity readiness in nigeria organizations. international journal of multidisciplinary and current educational research, 3(1):154–162.
16. Holsti, K. J. (1996). International politics: a framework for analysis. englewood cliffs.
17. Holt, J.T. (2021). Low self-control, Deviant peer association and juvenile cybercrime. American Journal of Criminal Justice, 12(3), 209-221.
18. Ibrahim, U. (2019). The impact of cybercrime on the Nigerian economy and banking system. NDIC Quarterly, 34(12):1–20.
19. Idowu, O.A. (2021). Cybercrimes and challenges of cyber-security in nigeria. 3:1–12.

20. Moga, E., Galle, S.A., and Abdulkarim, R. (2021). A historical assessment of cybercrime in nigeria: implication for schools and national development. journal of research in humanities and social science, 9(9): 84-94.
21. Morgan, S. (2021). cybercrime report. available at: https://www.cybersecurity.com.
22. Ogwu, J. (October 20, 2015). National reputation and logic of rebuilding nigeria's foreign image. the guardian.
23. Ojiego, N. (October 14, 2021). The audacity of the 'yahoo boys'. vanguard newspaper.
24. Onuoha, S. (2022). Cyber crimes: nigeria loses n200bn every year. daily business update.
25. Onwunyi, U.M., and Okonkwo K.J. (2021). Youth and cybercrime in nigeria: implications of the nationwide covid 19 lockdown. international journal of legal studies, 2(10): 209 – 232.
26. Opaluwa, T. (February 27, 2024). Cybercrime in nigeria: the fight rages on. the leadership.
27. Osho, O., and Onoja, A. (2015). National cyber security policy and strategy of nigeria: a qualitative analysis. international journal of cyber criminology, 9(1): 120–143.
28. Reep-van den Bergh, C. M., and Junger, M. (2023). Victims of cybercrime in europe: a review of victims surveys. crime science, 7(5), 2 – 15.
29. Shackelford, S.J., Timothy, L.F., & Danuvasin, C. (2016). Sustainable cybersecurity: applying lessons from the green movement to managing cyber attacks. u. ill. l. rev: 19-28.
30. Soeze, C.I. (2024). Laundering nigeria's international image. Retrieved from www.ndokwareporters.com/laundering-nigerias-image-international-pub
31. Sule, B., Yahaya, M., Sambo, U., and Mat, B. (2021). Cyber security and cybercrime in nigeria: the implications on national security and digital economy. 4:27–61.
32. Suleiman, I.M., M.A. Ishaq, M.A., & Rabiu, B.I (2017). The nigerian cybercrime (prohibition, prevention, etc.) act 2015" in p.n. ndubueze (ed.). cyber criminology & technology assisted crime control: a reader. zaria: ahmadu bello university press.
33. The Guardian (October 7, 2021). 80% of EFCC's 978 Convictions cybercrime related. www.guardian.ng.
34. Week, C. (2019). Nigeria lost $800m to cybercrimes in 2018 – Report.