© MAR 2026 | IRE Journals | Volume 9 Issue 9 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I9-1715408

Cybercrime In Nigeria: A Driving Force for Innovation or A Socio-Economic Plague?

OCHOLI, C.S
Department of Social Sciences and Humanities, The Federal Polytechnic, Idah, P.M.B,1037, Idah, Kogi State, Nigeria.

Abstract- ***This Article explores the dualistic role of digital activity in Nigeria, framed through the metaphor of a "Force" and a "Plague." While the digital economy acts as a driving force for financial inclusion and youth empowerment, the rise of cyber-malfeasance, colloquially termed Yahoo-Yahoo, presents a systemic plague threatening national security and international credibility. This study employs a qualitative, doctrinal research methodology. This approach is selected to critically analyze the intersection of legislative frameworks and the socio-economic realities of cyber-malfeasance. Through a critical lens, this paper examines the Cybercrimes (Prohibition, Prevention, etc.) Act 2015, the landmark 2024 Amendments, and the Evidence (Amendment) Act 2023. It evaluates the efficacy of Nigeria's evolving legal framework, concluding that while legislative updates are a step forward, the "plague" can only be contained through specialized judicial training and a rights-based approach to digital policing.***

Index Terms- ***Cybercrime, 2024 Amendment, Electronic Evidence, Section 24 Cyberstalking, Nigeria.***

I. INTRODUCTION

Cybercrime is a crime that involves computer and networks. The term cybercrime can be used to describe any criminal activity which involves the computer or the internet network (Okeshola & Adeta, 2013). The concept of cybercrime is historical. It was discovered that the first published report of cybercrime occurred on the mainframe computer in the 1960s (Maitanmi, 2013). The computer is a major source of evidence in cyberspace because either that it is used to commit a crime, a target of crime, or it is used to keep record of criminal log file.

Cybercrime has been on the increase for the immediate past years. A report from Federal Bureau Investigation of Information (FBI) that covered the period 2020-2024 shows that cybercrimes such as phishing, non-payment/non delivery, extortion, personal data breach and identity theft has been on the increase in the years surveyed.

(Maitanmi et el, 2013) highlights that cybercrime in Nigeria causes profound economic damage, damages the nation's international reputation, and poses security risks through activities like financial fraud. The prevalence of these crimes, often linked to youth involvement, has significantly impacted the banking sector, slowed economic growth, and fostered a "suspect" status for Nigerian business transactions globally.

Cybercrime in Nigeria began to come into the scene in the early 2,000's. (Stephen Ellis 2023) noted that cybercrime grew in Nigeria during the Obasanjo Administration in the early 2000s when the use of mobile phone was introduced. This is because those who could not afford computer could now do so in the comfort of their homes using their mobile phones to commit internet fraud.

Nigeria currently stands at a digital crossroads. On one hand, we are witnessing an unprecedented explosion in financial technology, making us a hub for global innovation. On the other, we are grappling with a persistent reputation as a sanctuary for digital fraud. As scholars, we must ask: is the internet a "Force" driving us toward a prosperous Fourth Industrial Revolution, or has it become a "Plague" eroding our socio-moral fabric?

The paradox is stark. While the Nigerian youth are arguably the most tech-savvy in Africa, a significant portion of this talent is being diverted into Business Email Compromise (BEC), identity theft, and phishing. This paper argues that cybercrime is not merely a criminal justice issue; it is a socio-economic

symptom that requires a more nuanced legislative response than simple incarceration.

II. LITERATURE REVIEW: ORIGIN OF THE INTERNET

Can you imagine your world without the internet? Probably the answer is 'NO'.

The invention of the internet is a contribution by many pioneering scientists, engineers, programmers, and researchers over some time. One of which was Lawrence Roberts, who proposed and led ARPANET and Tim Berners-Lee, who invented the World Wide Web. Each feature added by them contributed to the emergence of the internet.

The internet was created as a result of the cold war between the United States of America and the Soviet Union in the 1950s and 1960s, during that time each country was working towards increasing its science and technology capabilities in a bid to forestall or prevent nuclear attacks from one another. Mainframe computers at that time were expensive and could only do a specific task. They were so large that it can fit in an entire room. The Researchers who needed to use these computers to perform certain tasks had to travel long distance to do so. In order to erode these challenges, they had to find a solution to connect these computers so that they could interact with their colleagues and share various data in their Research work.

By the early 1960s computer manufacturers had begun to use technologies like timesharing systems, which allowed a computer's resources to be shared with multiple users, repeating through the queue of users so quickly that the computer appeared dedicated to each user's tasks despite the existence of many others accessing the system "simultaneously." This led to the notion of sharing computer resources called host computers over an entire network.

In 1991, CERN, the European Organization for Nuclear Research introduced the World Wide Web to the public.

Today, the Internet emphasizes social networking and user-generated content, and cloud computing is more prevalent. Social media services such as Facebook, Twitter, and Instagram have become some of the most popular Internet sites which allow users to share their content with their friends and the wider community. With the use of smartphones, there has been a rapid increase in Internet users worldwide.

The Digital Paradox in this highly digitalized World where everything is coming on an online platform and transaction is done online, some risks are increasing day by day with the advancement in technology.

Therefore, to protect users' rights, property rights, copyright, data protection, etc. It is paramount that we need some strict laws to protect the cyberspace. This is because every action and reaction that takes place in cyberspace has some legal aspects. Today there is so much rush on the internet traffic which leads to increase on legal issue of Cybercrime.

III. TYPES OF CYBERCRIME

Various cybercrimes like Credit card and ATM Fraud, theft, money laundering, identity theft, copyright, cyberstalking, distribution of viruses, plagiarism, Pornography, Hacking, Salami Attacks, Phishing and so many more are done using the computer or network.

EFCC alert site had enumerated some of the cybercrimes to include, romance scam, e-commerce/card, employment scam, wonder bank/Ponzi scheme, identity theft/phishing, contract scam/fund transfer, inheritance scam, charity scam, juju scam, crude oil/mineral, resources sales scam, scholarship scam, auction/scam, emergency scam, immigration/visa scam, and local purchase order scam.

National Cyber Security Policy and Strategy (2021) however, enumerated contents of cybercrime to include Phishing, Business Email Compromise (BEC), ransomware and malware, intellectual theft, and international property rights. Other emerging threats include machine learning poisoning, deep fakes, cloud hijacking, artificial intelligence fussing and crypto currency.

No doubt that technology is a very useful tool that can be used positively. It is becoming advanced for

helping us or for a better tomorrow, but some people use this in many dangerous ways for committing crimes. Hence, it should be the responsibility of the Government to make strict laws that must be enforced vehemently against these fraudsters, so that more security will be given to the users who adhere to the Law.

Cyberattacks have resulted in a large number of computer users having their privacy breached; this may include the disclosure of private photos, login passwords or medical details (Choo et al. 2007). In order to combat these cyber-malfeasances, the Nigerian government passed and put into effect the Cybercrimes (Prohibition, Prevention, etc) Act 2015 in 2015. Although the government recorded successes of these cybercriminals being detained, prosecuted by the Nigerian Police, The Economic Financial Crimes Commission (EFCC) and punished by the Law. Nevertheless, despite the efforts of the authorities, the ongoing modifications to strategies and advancements in approaches have consistently impeded the capture of a significant number of cybercriminals.

The Nigerian government in a quest to continuous protection of the cyberspace made an Amendment to the 2015 Act in 2024. However, there are still challenges as cyberattacks are still on the increase. It is important to point out that the 2015 Act and the Amended Act 2024 lack specific provisions for child and gender online protection, although the 2015 Act criminalizes child pornography and related offences, which aids in child protection. The Amended Act 2024 compliments and addresses some of the issues that were inadvertently omitted or not treated in the 2015 Act. Overall, while the 2015 Act and the Amended Act are largely aligned with the National Cybercrime Policy, further adjustments are needed to achieve full alignment.

The "Force": Innovation and Economic Necessity

The "Force" represents the immense potential of Nigeria's digital space. With the rise of unicorns like Flutterwave and Paystack, the digital economy is no longer a luxury, it is the backbone of our survival. The internet is acting as a primary driver of innovation by enabling digital entrepreneurship, transforming traditional sectors, and fostering a burgeoning tech ecosystem, with ICT contributing over 17% to the nation's GDP. As of late 2025, over 130 million Nigerians are connected online, with active broadband penetration exceeding 50%. The Nigeria Data Protection Act 2023 and the National Digital Economy Policy have provided the legislative scaffolding for this growth.

The government must be keen in establishing institutions bordering on Tech, to empower the youths in channeling their knowledge and talent to the right path. There should be sensitization among the youths on being creative, harnessing their talents-online businesses. The world is a global village and the government should see the need to create more Jobs that entails the use of technology like online schools, online registration, online services so that when these youths are more engaged there will be no forum to engage in these cyberattacks. This will help to foster a place where such innovations can aid in the economy and national development.

However, we must also acknowledge the "Necessity" argument that High unemployment, poverty, peer pressure, lack of sanctions and inflation have created a vacuum where the "Force" of technology is often the only accessible tool for survival. When traditional economic paths are blocked, the digital frontier becomes the only open market, leading many to cross the thin line between "hustle" and "crime."

The "Plague": The Erosion of National Integrity

Despite the economic gains, the "Plague" of cybercrime has deep-seated consequences. It isn't just about stolen funds; it is about the "Country Risk" branding that hampers Foreign Direct Investment (FDI). Today cybercrime is a direct threat to the global cyber space, which Nigeria as a country is part of. Worse still, Nigeria has a porous cyber security and so it's worse hit by cybercrime this is evident in the surge in cybercrime in Nigeria because due to the complexity of the organized cybercrime and weak cyber security system in Nigeria, being that Nigeria with its enormous natural and human resources, it is recorded that an estimate of 139 million Nigerians (roughly 61-62% of the population) live in poverty.(World Bank 2025) . This report shows that these youth are bound to look for other means of survival at all cost. Unemployed youth seeking for

survival, has found solace in various cyber security loop holes to perpetrate crimes against those companies and individuals that lack strong cyber security to protect themselves against eminent cybercrime. There is no doubt that these crimes have a lot of economic implications for the country. It has led to the scaring of foreign and local investors. It has also subjected individuals and organizations to huge financial losses, most especially in banking sector, where hacking is in constant reoccurrence. However, apart from economic effects, cybercrime also has many socio-cultural effects on the country. It makes the citizens to live in fear due to acts of killings of young girls and boys. The incorporation of fetishism and spiritual elements has incurred the name of such perpetrators as (Yahoo+), where in order to gain powers to manipulate their victims they must sleep with young virgins. These acts have spiraled into a lot of reported cases of kidnappings and rape, which has led to increase in insecurity and citizens leaving in fear.

Consider the landmark case of *FRN v. Hope Olusegun Aroke*. The defendant who was serving a 24 years sentence could still commit an international scam even from the confines of a maximum-security prison. It was later discovered he did so through the help of one of the staffs in the prison and a medical doctor. The defendant managed to coordinate a multi-million-dollar international scam. This demonstrates that the "Plague" is not just an external threat but a systemic one, thriving on the loopholes within our correctional and enforcement institutions. Furthermore, the social normalization of fraud among the youth suggests a long-term erosion of the national work ethic.

The Legal Framework: The 2024 Shift

For years, the Cybercrimes Act 2015 was a double-edged sword. While it provided a basis for prosecution, Section 24 (the "Cyberstalking" clause) was frequently weaponized against journalists and dissidents. Section 24 of the 2015 Act makes it an offence for any person to transmit a message via computer systems or networks that is grossly offensive, pornographic, indecent, obscene, or menacing, or knowingly send false information for the purpose of causing annoyance, inconvenience, danger, obstruction, insult criminal intimidation, enmity, hatred, ill will or needless anxiety to another or causes such a message to be sent.

This Section 24 of the 2015 Act has been a lightning rod for controversy since its inception. It has been criticized for its alleged role in curtailing and potentially undermining constitutionally guaranteed rights to freedom of the press and expression. This provision has been cited and used to justify alleged unlawful arrest of journalists and others based on their online activities.

The reason for this is the fact that the section was termed vague and overbroad. Terms

like "insult," "hatred," "inconvenience," "ill will," and "needless anxiety" were not clearly defined. What constitutes an insult, hatred, annoyance, or inconvenience under the section? Is there a limit to what may be classified under these terms? These ambiguities left the section open to interpretation, allowing law enforcement agencies to target individuals arbitrarily. When a statute is vague, it gives undue power to prosecutors, leading to arbitrary enforcement. The section was also criticized for its irreconcilability with sections 36(12) and 39(1) of the 1999 Constitution of the Federal Republic of Nigeria, 1999 (as amended).

In March 2024, reports emerged that the Economic Community of West African States (ECOWAS) Court of Justice ruled that Section 24 of the 2015 Act does not comply with Articles 9 of the African Charter on Human and People's Rights and the International Covenant on Civil and Political Rights. As a result, the ECOWAS Court of Justice ordered the Nigerian Government to amend section 24 of the 2015 Act. In reaction to the various criticisms, the Amended Act refined the language of Section 24 of the 2015 Act by limiting its parameters to pornographic or false information aimed at causing a breakdown of law and order or posing a threat to life. In effect, if a message is shown to be true and not pornographic, then no offence would have been committed under Section 24 of the 2015 Act as amended. This amendment is commendable; it represents a significant stride by the Nigerian Government in safeguarding the constitutionally guaranteed freedom of expression. Despite the

changes introduced by the Amended Act and the ECOWAS Court of Justice's decision in March 2024, it has been reported that journalists are still being arrested, with law enforcement officers citing Section 24 of the 2015 Act as their authority. This is likely because the Amended Act fails to clearly define what constitutes a breakdown of law and order. This ambiguity allows law enforcement officers to use the law as a pretext to target journalists, claiming their actions amount to a breakdown of law and order.

The 2024 Amendment is a welcome intervention. Following the ECOWAS Court ruling in *SERAP v. Nigeria*, the government finally narrowed the definition of cyberstalking to focus on pornography and misinformation that endangers public life. This shift is crucial; it ensures that the law remains a "Force" for order without becoming a "Plague" to free speech.

IV. EVIDENCE ACT

To emphasize, the greatest challenge in cyber-prosecution is the Evidence Act. Even with the 2023 Amendments, the "Certificate of Authentication" required under Section 84(4) remains a technical minefield. Many cases are lost not because the defendant is innocent, but because the prosecution cannot technically prove the "integrity" of the computer system that produced the evidence. We need a more pragmatic approach to digital forensics that accounts for the reality of cloud computing and decentralized data.

V. RESEARCH METHODOLOGY

To explore the dualistic nature of digital activity in Nigeria, this paper employs a qualitative, doctrinal research methodology. This approach is selected to critically analyze the intersection of legislative frameworks and the socio-economic realities of cyber-malfeasance. The methodology consists of the following components:

- Statutory Analysis: A primary examination of Nigeria's core digital legislation, specifically the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 and its 2024 Amendments, alongside the Evidence (Amendment)Act2023.
- Case Study Review: An analysis of landmark judicial precedents, such as FRN v. Hope Olusegun Aroke, to evaluate the systemic challenges within Nigerian correctional and enforcement institutions.
- Jurisprudential Review: A review of international rulings, notably the ECOWAS Court decision in SERAP v. Nigeria, to understand the shift in defining cyberstalking and the protection of civil liberties.
- Socio-Legal Synthesis: An interpretive approach that connects economic indicators—such as high unemployment and the rise of "unicorns" like Flutter wave—to the behavioral patterns of digital "hustle" versus "crime".

VI. FINDINGS

Based on the analysis of the legal landscape and socio-economic effect, the following findings are identified:

- Legislative Progress vs. Technical Barriers: While the 2024 Amendments narrowed the definition of cyberstalking to protect journalists, the prosecution of cybercriminals remains hindered by the technical "minefield" of Section 84 of the Evidence Act.
- The Necessity Argument: High unemployment and inflation create a vacuum where the digital space is often the only tool for survival, leading to the social normalization of fraud among the youth.
- Institutional Vulnerability: The "Plague" is not just an external threat but a systemic one that exploits loopholes within correctional and enforcement institutions.
- Admissibility Gaps: Many cases are lost because the prosecution cannot prove the "integrity" of the computer systems involved, highlighting a need for tech-literate judges.
- Economic Branding: Cyber-malfeasance carries a "Country Risk" that discourages Foreign Direct Investment (FDI), impacting the broader economy beyond the immediate financial theft.

VII. CONCLUSION

Cybercrime in Nigeria is a complex interplay of brilliance and desperation. The 2024 Amendments offer a more balanced path forward, but legislation alone cannot cure a plague. It requires a synergy of robust technology, ethical policing, and a judicial system that understands that the future of evidence is digital. The government must be proactive in reducing the rate of high unemployment and create policies that focuses on empowering the youth, embrace the more use of technology and sensitization on cybersecurity.

VIII. RECOMMENDATIONS

To ensure the "Force" of innovation triumphs over the "Plague" of crime, Nigeria must:

- Institutionalize Specialized Courts: General jurisdiction courts are often overwhelmed. We need judges who are as tech-literate as the criminals they are trying.
- Global Synergy: Cybercrime is borderless; our laws cannot be territorial. We must fully integrate with the Budapest Convention.
- Reform the Narrative: Legal education must move beyond the "thou shalt not" of the Act and focus on building an ethical digital citizenship.

REFERENCES

[1] Choo, K-K, Smith, R, & McCusker R. (2007). Future Directions in Technology Enabled crime.

[2] Research and public policy series no. 78 Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/rpp/rpp78

[3] Constitution of the Federal Republic of Nigeria (1999) As Amended. Evidence (Amendment) Act (2023).

[4] Economic and Financial Crime Commission (EFCC, 2022). Types of cybercrime. https://www.efccnigeria.org.

[5] Gbahabo E, kazeem L, Ufomba C. (2024) The Cybercrimes (Prohibiton, Protection, Etc) (Amendment) Act 2024: A Paradigm Shift for Individuals and Businesses https://www.templars-law.com/app/uploads/2024/08/cybercrimes.pdf

[6] FRN v. Hope Olusegun Aroke (2015) FHC/L/432C.

[7] Maitanmi O, Ogunlere S, Ayinde S, & Aekunle Y. (2013): Impact of Cybercrimes on Nigerian Economy. The International Journal of Engineering and Science (IJES) 2 (4), 45-51

[8] Nathan, Reuben, Abroad (2024) Relationship between Cybercrime and the Nigerian Economy: Causes, Implication and the Path Forward. Journal of Finance, Business and Management Studies Vol 4, No 1, pp.21-33, ISSN 2583-0503 published by RGN Publications. http://www.rgnpublications.com

[9] Okeshola B. and Adeta K. (2013) The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaira-Kaduna State, Nigeria. Ijrs. http:/www.ijrs.com

[10] Stephen Ellis (2023), “The Origin of Nigeria’s Notorious 419 Scams”, https://www.newsweek.com/origins-nigeria-notorious-419-scams-456701

[11] World Bank: (2025) Number of poor Nigerians increased by 35M from 2023. https://punchng.com/wbank-report-nigeria-needs-to-tackle-poverty

[12] SERAP v. Federal Republic of Nigeria (2024) ECW/CCJ/JUD/09/24.