DIGITAL ECONOMY AND THE MENACE OF CYBER CRIME IN NIGERIA

[1]Igbinomwanhia, Osasere Greg and [2]Sulaiman, Adeyinka Ibrahim

Department of Sociology and Anthropology
Faculty of Social Sciences,
University of Benin, Benin City, Nigeria
osasere.igbinomwanhia@uniben.edu
08133798888; 08135624850
adeyinka.sulaiman@uniben.edu
https://orcid.org/0009-0001-4047-9314

https://doi.org/10.60787/aasd.vol4no1.92

Abstract
Cyber crime has emerged as a significant threat to Nigeria's socio-economic development, with its impact felt most strongly among the youth population. The rapid expansion of internet access and digital technologies, while beneficial for economic growth and communication, has also created new avenues for criminal activities. This study examines the underlying causes, major forms, and far-reaching effects of cybercrime in Nigeria, alongside an evaluation of existing legal frameworks and strategies aimed at curbing the menace. Adopting a qualitative, non-empirical research design, the study relies on secondary data drawn from academic literature, government reports, and institutional publications. Through thematic analysis, the study identifies key drivers of cybercrime, including unemployment, urbanization, weak law enforcement mechanisms, and the influence of societal value systems that increasingly normalize illicit wealth acquisition. The findings further reveal that cybercrime manifests in various forms such as online fraud, identity theft, hacking, and phishing, all of which pose serious risks to economic stability, national security, and youth development. The study concludes that although legislative measures, particularly the Cybercrime Act, have been established to address cyber-related offences, their effectiveness is significantly undermined by poor implementation, inadequate institutional capacity, and persistent socio-economic challenges. Consequently, the paper advocates for a holistic and multi-stakeholder approach involving government agencies, private sector actors, educational institutions, and the general public in order to effectively combat cybercrime and promote a secure digital environment in Nigeria.

Keywords: *Cybercrime, Youth Involvement, Socio-Economic Impact, Digital Crime Prevention, Online Fraud*

Introduction

In recent years, society has become increasingly dependent on the internet and other information and communication technologies (ICTs) for business transactions, communication, and social interaction. While these technological advancements have significantly enhanced productivity, efficiency, and global connectivity, they have also created new opportunities for criminal activities. One of the major challenges associated with this digital transformation is cybercrime. Cybercrime broadly refers to any illegal activity carried out using computers or internet networks, including offenses such as fraud, theft, blackmail, forgery, and embezzlement (Okeshola, 2013).

Maitanmi (2013) further conceptualizes cybercrime as criminal activities in which computers serve as tools and the internet acts as a medium for executing various illicit acts, including software piracy, unauthorized downloads, spamming, and online fraud. The evolution of cybercrime can be traced back to the 1960s when early forms of computer-related crimes were recorded on standalone mainframe

systems. At that time, such acts were largely internal (committed by insiders) and were referred to as "*computer crimes*" rather than cybercrimes due to the absence of interconnected networks (Maitanmi, 2013).

In the Nigerian context, cybercrime has become increasingly prevalent and is perpetrated by individuals across different age groups, though it is most common among the youth. The growing involvement of young people in cybercrime is largely driven by the availability of inexpensive digital tools and widespread internet access. As noted by Mbaskei in *Cybercrimes: Impact on Youth Development*, large-scale fraud cases have been uncovered in Nigeria, including a notable operation in Lagos involving fraudulent financial instruments valued at approximately $2.1 billion. Such incidents highlight the sophistication and scale of cybercriminal activities, as well as the increasing normalization of cybercrime as a means of livelihood among some youths.

The proliferation of cybercrime in Nigeria is closely linked to prevailing socio-economic challenges, including high levels of poverty, unemployment, and systemic corruption. These conditions create a conducive environment for cybercriminal activities, as many individuals resort to illicit means of income generation in the absence of legitimate opportunities. Furthermore, weak regulatory frameworks and inadequate enforcement mechanisms have contributed to the persistence of cybercrime, allowing it to thrive as a subculture among certain segments of the population.

Globally, cybercrime is a growing concern. Lakshmi (2015) reports that countries such as the United States and South Korea accounted for significant proportions of cyberattacks in the early 2000s, underscoring the transnational nature of the problem. In Nigeria, the rapid expansion of internet usage has further intensified the challenge. According to the Nigerian Communications Commission (NCC, 2022), a substantial proportion of the population now has access to the internet, thereby increasing both the opportunities for digital engagement and the risks of cybercrime. Consequently, cybercrime continues to pose a serious threat to Nigeria's economic development, national security, and global reputation.

Research Methodology

This study adopts a qualitative, non-empirical research design, relying exclusively on secondary data sources to examine the growing menace of cybercrime in Nigeria. The choice of this design is informed by the exploratory nature of the study, which seeks to synthesize existing knowledge, identify patterns, and provide a comprehensive understanding of cybercrime without generating primary data.

Data for the study were systematically collected from a wide range of credible and relevant sources, including:

1) Peer-reviewed journal articles
2) Government publications (e.g., reports from the Nigerian Communications Commission and other regulatory bodies)
3) Institutional and policy reports
4) Books and academic textbooks
5) Media reports and reputable online publications

These sources were selected based on their relevance, credibility, and contribution to the discourse on cybercrime, particularly within the Nigerian context. Emphasis was placed on both classical and contemporary studies to ensure a balanced and comprehensive perspective. A thematic analytical approach was employed to organize and interpret the data. This involved a careful review of the

selected materials, followed by coding and categorization of recurring ideas and patterns. The data were subsequently grouped into key thematic areas, including the causes, forms, effects, and control measures of cybercrime in Nigeria. To enhance the rigor and reliability of the study, information from multiple sources was compared and cross-validated, ensuring consistency and minimizing bias. This methodological approach enabled the study to provide a coherent synthesis of existing literature while offering insights into the dynamics and implications of cybercrime in Nigeria.

Results

a. **Causes of Cybercrime in Nigeria:** Through careful examination of data the study identifies several interrelated socio-economic and institutional factors that drive the proliferation of cybercrime in Nigeria. These factors not only create enabling conditions but also sustain the continuous involvement of individuals, particularly youths, in cybercriminal activities. However the the validity of these result can be subjected to further investigation to determine if there are varying patterns and trends.

b. **Unemployment, Poverty and Urbanization**: From the data gathered, it was found that high levels of unemployment and widespread poverty remain primary drivers of cybercrime in Nigeria. With limited access to legitimate income-generating opportunities, many youths resort to cybercrime as an alternative means of survival and financial stability. The absence of gainful employment, coupled with rising living costs, creates economic pressure that pushes individuals toward illicit online activities, which are often perceived as lucrative and low-risk.

   Another factor that was found while analyzing the data is Rapid urbanization and rural-to-urban migration. These have significantly contributed to the rise of cybercrime. As individuals move to urban centers in search of better opportunities, they often encounter intense competition, limited job prospects, and increased exposure to criminal networks. Urban environments also provide the technological infrastructure—such as internet access and cybercafés—that facilitate cybercriminal activity. Consequently, cities become hotspots for the recruitment and operation of cybercrime syndicates.

c. **Weak Legal Enforcement**: From the data, it was also found that weak legal framework is key to explaining the rise in cybercrime in the area of study. Although legal frameworks such as cybercrime laws exist, their implementation remains weak and inconsistent. Inadequate law enforcement capacity, lack of technical expertise, and limited resources hinder effective detection, investigation, and prosecution of cybercriminals. This enforcement gap creates a sense of impunity, where offenders operate with minimal fear of arrest or punishment, thereby encouraging the persistence and expansion of cybercrime.

d. **Quest for Wealth and Materialism**: The increasing desire for rapid financial success and material accumulation is another significant factor. In a society where wealth is often highly celebrated regardless of its source, many individuals are motivated to pursue quick and easy means of acquiring money. Cybercrime, particularly online fraud, is perceived as requiring minimal investment while offering substantial financial returns, making it attractive to young people seeking upward social mobility.

e. **Negative Socialization and Cultural Influence**: Social and cultural factors also play a critical role in the spread of cybercrime. Peer influence, media representation, and societal attitudes that

glamorize illicit wealth contribute to the normalization of cybercriminal behavior. In some cases, cybercriminals are admired for their perceived success, thereby influencing others to emulate such behavior. Additionally, weak parental supervision and the erosion of traditional value systems further reinforce deviant behaviors among youths.

Forms of Cybercrime

The data also show the various forms of cybercrime that is prevalent in the area of study. Cybercrime in Nigeria manifests in diverse and increasingly sophisticated forms, reflecting both technological advancements and the adaptability of cybercriminals. The most common forms identified in this study include:

i. **Advance Fee Fraud (Yahoo-Yahoo/419 Scams**: Advance Fee Fraud is one of the most prevalent forms of cybercrime in Nigeria as found from the data. It involves deceiving victims into paying upfront fees with the promise of receiving a larger financial reward later. These scams are typically executed through emails, social media platforms, and fake websites, often involving impersonation and fabricated business or romantic relationships.

ii. **Hacking and Unauthorized Access**: Hacking and unauthorized access was another form of cybercrime that was found. It involves gaining illegal access to computer systems, networks, or databases with the intent to steal, manipulate, or destroy information. Cybercriminals exploit security vulnerabilities in systems to access sensitive data, including financial records, personal information, and organizational secrets.

iii. **Software Piracy and Cyber Pornography**: The study also found that Software Piracy and Cyber pornography are common forms of cyber malfeasance in the area. Software piracy refers to the unauthorized copying, distribution, or use of copyrighted software, movies, music, and other digital content. Software piracy is widespread due to the high cost of licensed products and weak enforcement of intellectual property laws from what was found. Also it was discovered that Cyber pornography is a common form of the crime in the area. The internet has facilitated the production, distribution, and consumption of pornographic materials. In Nigeria, cyber pornography has become increasingly accessible, particularly among youths, raising concerns about moral standards, exploitation, and exposure to inappropriate content.

iv. **Credit Card and ATM Fraud:** This involves the theft and misuse of credit card or ATM details to carry out unauthorized financial transactions. Cybercriminals obtain such information through skimming devices, phishing schemes, or database breaches, leading to significant financial losses for victims.

v. **Phishing Attacks and Denial of Service (DoS) Attacks:** The data also show that Phishing Attacks are a regular form of cybercrime in the area. Phishing is a deceptive practice where attackers impersonate legitimate institutions, such as banks or online services—to trick individuals into revealing sensitive information like passwords, PINs, and account details. These attacks are often carried out through fake emails, messages, or websites that appear authentic. DoS attacks were also found to be a prevalent form of cybercrime practiced by my people in the area of study. DoS attacks are aimed at disrupting access to online services

by overwhelming a system, server, or network with excessive traffic. This renders the service unavailable to legitimate users and can significantly affect businesses and institutions that rely on digital platforms.

vi. **Cyber Plagiarism and Virus Dissemination:** It was found from the data that was examined that Cyber plagiarism was a common form of cyber crime in the area. Cyber plagiarism involves the unauthorized use or reproduction of another person's intellectual work obtained online, presenting it as one's own. This is particularly common in academic environments, where students and even researchers copy materials without proper credit to the original owner of the intellectual material. Another form of cyber crime that was found to be often practiced in the area is Virus dissemination. This involves the creation and spread of malicious software (malware), such as viruses, worms, and Trojan horses, designed to damage, disrupt, or gain unauthorized access to computer systems. These programs can corrupt data, steal information, or compromise system functionality.

Effects of Cybercrime on Youth Development

From the data that was used, it was found that cybercrime has the potential to generally impact young people negatively in various ways. Cybercrime has far-reaching consequences on both youth development and the broader socio-economic landscape of Nigeria. Its impact extends beyond immediate financial gains for perpetrators, contributing to long-term developmental challenges and social disorientation. Some specific effects are put below.

Promoting School Drop Out and Undermining Skill Acquisition and Entrepreneurship

It was found that cybercrime has the tendency to promote out of school syndrome among young people in Nigeria. The involvement of youths in cybercrime often leads to a decline in academic commitment. Many students become distracted by the quick financial rewards associated with online fraud, resulting in poor academic performance and, in some cases, complete withdrawal from formal education. This undermines the development of a skilled and educated workforce necessary for national growth. It was also found that Cybercrime discourages youths from pursuing legitimate skill acquisition and entrepreneurial ventures. This also has great implication for the national progress of the country especially as it will seriously affect the productive capacity of the nation.

Discussion

The findings of this study underscore that cybercrime in Nigeria extends beyond a purely technological challenge and should be understood as a multi-dimensional socio-economic problem. Structural factors such as poverty, high unemployment rates, inequality, and weak institutional capacity collectively create an enabling environment for the proliferation of cybercriminal activities. These conditions not only push individuals—particularly youths—toward cybercrime as a means of survival, but also sustain its growth as an alternative economic system within certain social groups.

Furthermore, the study reveals that the rapid expansion of internet access and digital technologies, while beneficial for development, has inadvertently increased exposure to cybercrime opportunities. In the absence of strong regulatory oversight and effective monitoring systems, technological advancement has outpaced institutional capacity, thereby creating gaps that cybercriminals exploit. This aligns with broader scholarly arguments that cybercrime thrives in environments where technological growth is not matched by adequate governance and control mechanisms.

Although the enactment of the Cybercrime Act represents a significant policy response by the Nigerian government, its effectiveness remains constrained by several challenges. These include weak enforcement mechanisms, inadequate technical expertise among law enforcement agencies, insufficient funding, and poor inter-agency coordination. As a result, many cybercriminal activities go undetected or unpunished, reinforcing a culture of impunity.

In addition, societal attitudes play a critical role in the persistence of cybercrime. The growing normalization and, in some cases, glorification of cybercriminal behavior—particularly among youths—pose serious obstacles to intervention efforts. The celebration of illicit wealth in popular culture and peer networks contributes to the erosion of ethical standards, making cybercrime appear socially acceptable or even desirable.

Given these complexities, addressing cybercrime in Nigeria requires a holistic and multi-stakeholder approach that goes beyond punitive measures. Effective strategies should integrate socio-economic reforms, institutional strengthening, and value reorientation. Key measures include:

a) **Strengthening legal and institutional frameworks:** Enhancing the capacity of law enforcement agencies through training, funding, and technological support to improve detection, investigation, and prosecution of cybercrimes.

b) **Improving cyber security infrastructure:** Investing in advanced security systems, data protection mechanisms, and digital monitoring tools across both public and private sectors.

c) **Creating employment opportunities:** Addressing youth unemployment through job creation, entrepreneurship support, and vocational training to reduce economic incentives for cybercrime.

d) **Promoting ethical reorientation:** Implementing value-based education and public campaigns aimed at discouraging illicit wealth acquisition and promoting integrity among young people.

e) **Enhancing public awareness and digital literacy:** Educating citizens on cyber risks, safe online practices, and methods of identifying fraudulent activities.

f) In sum, the fight against cybercrime in Nigeria must be comprehensive, combining legal, economic, technological, and socio-cultural interventions to achieve sustainable results.

Conclusion

Cybercrime continues to pose a significant and evolving threat to Nigeria's socio-economic development, particularly in the context of increasing digitalization and internet penetration. As this study has demonstrated, the persistence of cybercrime is not solely a function of technological advancement, but is deeply rooted in underlying socio-economic challenges such as poverty, unemployment, inequality, and weak institutional capacity. These factors collectively create an enabling environment in which cybercriminal activities can thrive, especially among the youth population.

Although Nigeria has made notable progress through the establishment of legal frameworks such as the Cybercrime Act, the effectiveness of these measures remains limited due to enforcement deficiencies, inadequate technical expertise, and poor coordination among relevant agencies. Consequently,

cybercrime continues to undermine national development by damaging the country's global reputation, discouraging foreign investment, and eroding ethical standards among young people.

Addressing the menace of cybercrime therefore requires a comprehensive and collaborative approach that goes beyond legislative provisions. It demands the active involvement of government institutions, the private sector, civil society, and individual citizens. Efforts must focus not only on strengthening legal and technological mechanisms but also on tackling the socio-economic drivers of cybercrime and promoting ethical reorientation within society.

In conclusion, building a secure and resilient digital environment in Nigeria will depend on sustained commitment to institutional reform, economic empowerment, public awareness, and value reorientation. Only through such a holistic strategy can the country effectively curb cybercrime and harness the full benefits of the digital economy for sustainable development.

Recommendations

In light of the findings of this study, a multi-dimensional and collaborative approach is essential to effectively address the growing menace of cybercrime in Nigeria. The following recommendations are proposed:

1. **Strengthening Enforcement of Cybercrime Laws:** Existing legal frameworks should be rigorously enforced to ensure that offenders are promptly investigated, prosecuted, and sanctioned. This requires eliminating loopholes in the justice system and ensuring consistency in the application of cybercrime laws.

2. **Capacity Building for Law Enforcement Agencies:** There is a need to enhance the technical and operational capacity of law enforcement agencies through continuous training, recruitment of cybercrime experts, and provision of modern digital forensic tools. This will improve the detection, investigation, and prosecution of cybercriminal activities.

3. **Promotion of Public-Private Partnerships in Cyber security:** Effective collaboration between government institutions, financial organizations, telecommunication companies, and technology firms is critical. Such partnerships can facilitate information sharing, threat intelligence, and the development of innovative solutions to combat cybercrime.

4. **Job Creation and Economic Empowerment for Youths:** Addressing youth unemployment should be prioritized through the creation of sustainable job opportunities, entrepreneurship development programs, and vocational training initiatives. This will reduce the economic incentives that drive many youths into cybercrime.

5. **Public Sensitization and Awareness Campaigns:** Nationwide awareness campaigns should be intensified to educate citizens on the risks, consequences, and prevention of cybercrime. Digital literacy programs should also be introduced to equip individuals with the knowledge to identify and avoid online fraud schemes.

6. **Promotion of Ethical Values and Value Reorientation:** Educational institutions, religious bodies, and community leaders should actively promote integrity, accountability, and responsible digital behavior among young people. Efforts should be made to discourage the glorification of illicit wealth and reinforce positive societal values.

7. **Investment in Cyber security Infrastructure:** Both government and private organizations should invest in advanced cybersecurity systems, including firewalls, encryption technologies, and intrusion detection systems. Strengthening digital infrastructure will reduce vulnerabilities that cyber criminals exploit.

8. **Parental and Institutional Monitoring of Internet Use:** Parents, guardians, and educational institutions should play a more active role in monitoring and guiding the online activities of young people. This includes promoting responsible internet use and preventing early exposure to cybercriminal practices.

9. **Enhancing International Cooperation:** Given the transnational nature of cybercrime, Nigeria should strengthen collaboration with international organizations and foreign governments. This includes intelligence sharing, joint investigations, and adherence to global cyber security standards and conventions.

References

Ajaero, C. K. and Onokala,P. C. (2013). The Effects of Rural-Urban Migration on Rural Communities of Southeastern Nigeria, International Journal of Population Research, vol. 2013, Article ID 610193, 10 pages, 2013. doi:10.1155/2013/610193

Awe, J. (2009), Fighting Cyber Crime in Nigeria.http://www.jidaw.com/itsolutions /security3.html.

Ayantokun, O. (2006). Fighting Cybercrime in Nigeria: Information-system.www.tribuneonlineng.com/cbn-licences-n100bn-development-bank-nigeria/

Ehimen, O.R. and Bola, A, (2010).Cybercrime in Nigeria. Business Intelligence Journal, January 2010, Vol.3.No.1.

Ekeji, E. (2014). Cyber Crime in Nigeria. Retrieved from https://www.academia.edu/ 4818858/Cyber_Crime_in_Nigeria

Hassan, A. B. Lass F. D. and Makinde J. (2012) Cybercrime in Nigeria: Causes, Effects and the Way Out, ARPN Journal of Science and Technology, vol. VOL. 2(7), 626 – 631.

Kumar, K. (2003). Cyber Laws, International Property and e-commerce Security.Dominant Publishers and Distributors, New Delhi. Legislative and Government Relations Unit,

Lakshmi P. andIshwarya M. (2015), Cyber Crime: Prevention & Detection," International Journal of Advanced Research in Computer and Communication Engineering, vol. Vol. 4(3).

Maitanmi, O. Ogunlere, S. andAyinde S. (2013), Impact of Cyber Crimes on Nigerian Economy, The International Journal of Engineering and Science (IJES, vol. vol 2(4), 45–51.

Maitanmi, O., Ogunlere, S., Ayinde, O., and Adekunle, Y. (2013).Impact of Cyber Crimes on Nigerian Economy. The International Journal Of Engineering and Science (IJES), 2(4), 45-51. Retrieved from http://www.theijes.com/papers/v2-i4/part.%20(4)/H0244045051 .pdf Monday Editorial. (2016). Curbing Cybercrime in Nigeria. Thisday Newspapers Ltd [Lagos]. Retrieved from https://www.thisdaylive.com/index.php/2016/11/07/curbing-cybercrime -in-nigeria/

Nweke, O. J. (2014). The rapid growth of internet fraud in Nigeria, Cause, Effect and Solution. Retrieved from https://innertempleoou.wordpress.com/2017/03/07/the-rapidgrowth-of-internet-fraud-in-nigeria-cause-effect-and-solution-by-nweke-oluchi-jacinta/

Okeshola, F. B., &Adeta, A. K. (2013).The Nature, Causes and Consequences of CyberCrime in Tertiary Institutions in Zaria - Kaduna State, Nigeria. American International Journal of Contemporary Research, 3(9), 98-114.

Okonigene, R. E., &Adekanle, B. (2010).Cybercrime in Nigeria. Business Intelligence Journal, 3(1), 93-98.

Olaide and Adewole (2004), Cyber Crime Embarrassing for Victims. Retrieved September 2011 from http//www.heraldsun.com.au

Olugbodi, K. (2010), Fighting Cyber Crime in Nigeria. Retrieved September 10,2011 from http//www.guide2nigeria,com/news_articles_About_ Nigeria

Olusola, M., Samson, O., Ayinde, S., & Adekunle, Y. (2013).Impact of Cyber Crimes on Nigerian Economy. Retrieved from http://www.theijes.com/papers/v2- i4/part.%20(4)/H0244045051.pdf

Oni, M. J. (2013). Cyber-crime in Nigeria: The implication on our economy and social image. Retrieved from http://acta-pac.org/pac-article/cyber-crime-nigeria-implication-oureconomy-and-social-image

Oyewole and Obeta (2002), An Introduction to Cyber Crime. Retrieved September 2011 from http//www.crime- research.org/articules/cyber-crime.

Public Affairs Department.(2015). A Summary of the Legislation on Cybercrime in Nigeria. Retrieved from http://www.ncc.gov.ng/thecommunicator/index.php?option=com_content&view=article&id=899:a-summary-of-the-legislation-on-cybercrime-in-nigeria

Ribadu, E. (2007), Cyber Crime and Commercial Fraud; A Nigerian Perspective. A paper presented at the Modern Law for Global Commerce, Vienna 9th – 12th July.

Sesan, G. (2010), The New Security War. http://www.pcworld.com/article/122492/the_new_security_war.htm#tk.mod-rel. Shinder, D.L.(2002), Scene of the Cybercrime: Computer Forensics Handbook. Syngress Publishing Inc. 88 Hingham Street, USA.

Thisday Newspaper (2012): Growing menace of Cyber crime, 20th September, 2012.

Tyendezwa, T. G. (2015). Legislation on cybercrime in Nigeria: Imperatives and challenges. Retrieved from http://www.ncc.gov.ng/documents/233-legislation-on-cybercrime-innigeria-imperatives-and-challenges/file

Umoru, H. (2017). $450m lost to cyber-crime in Nigeria —Senate. Vanguard Media Limited [Nigeria]. Retrieved from https://www.vanguardngr.com/2017/05/450m-lost-cybercrime-nigeria-senate/

Vladimir, G. (2005), International Cooperation in Fighting Cyber Crime. www.crimeresearch.org. Retrieved from http://www.crime-research.org/articles/ Golubev0405/

Zero Tolerance (2006), Retiree in Trouble over Internet Fraud. Economic and Financial Crime Commission, Vol.1, No. 2 Zhudifeng. (2016). Cybercrime in Africa: Facts and figures - SciDev.Net Sub-Saharan Africa. Retrieved from http://www.scidev.net/sub-saharan-africa/icts/feature/cybercrime-africafacts-figures.html