African Journal of Social and Behavioural Sciences (AJSBS)
Volume 15, Number 2 (2025) ISSN: 2141-209X

CYBERCRIME AND ECONOMIC DEVELOPMENT IN NIGERIA: CHALLENGES, OPPORTUNITIES, AND STRATEGIC POLICY INTERVENTIONS

Ann Kuro John-Williams

Department of Sociology, Ignatius Ajuru University of Education, Rumuolumeni, Port Harcourt. Rivers State, Nigeria

anniesco33@gmail.com

ABSTRACT: This study examined the implications of cybercrime and economic development in Nigeria. Three research questions and three objectives were formulated to aid the study. The study is anchored on differential association theory propounded by Edwin Sutherland. The study adopted a qualitative research method with the use of desk research methodology; as such data was elicited through Secondary sources such as journals, periodicals, newspaper publications, textbooks and reviews. Our analysis revealed that cybercrime has become a huge menace threatening the socio-economic and technological advancement of Nigeria as the attention of many youths have been diverted from embarking on productive activities to flamboyant life styles. Also, that the financial losses accrued by consumers and business resulting from the theft of information and money or extortion impedes economic growth. The study concluded that widespread cybercrime has negative impact on the economic development in Nigeria as it tarnishes the image of the country at the global scale. The paper recommends that government should pursue vigorous enlightenment campaigns for the citizens on basic preventive and protective measures against cybercrime.

Keywords: Cybercrime, Economic Development, Differential Association Theory, Nigeria

INTRODUCTION

Cybercrime has emerged as a significant global challenge, expanding in scope and complexity alongside the rapid advancement of internet technologies (Singh et al., 2024). The internet has fundamentally transformed contemporary society, driving economic growth in both developed and developing nations while facilitating seamless communication and fostering globalisation. However, this digital revolution has also given rise to sophisticated cyber threats. In Nigeria, internet penetration has increased significantly since the early 21st century, reaching over 40% of the population (Eze, 2023) and contributing to economic opportunities but also exposing the country to cybercriminal activities. Nigeria is now considered the epicentre of cybercrime in sub-Saharan Africa, with annual economic losses estimated at $649 million (Kovacs, 2024). The proliferation of digital platforms has created vulnerabilities that criminals exploit, posing serious socio-economic risks. As societies become more interconnected through cyberspace, the security of digital transactions and information remains a critical concern, necessitating robust cybersecurity measures to mitigate potential threats.

Recent reports from experts in Information and Technology indicate that the internet offers numerous advantages, including access to vast information resources, opportunities for online education, platforms for research, avenues for commerce, enhanced communication, and its pivotal role as a catalyst for innovation. However, it is important to acknowledge that the internet also hosts content that many users may deem objectionable, thereby raising concerns about the exposure of themselves, their children, and society at large to such material. Despite these apprehensions, the number of GSM users and internet subscribers continues to rise monthly. This leads to a pertinent question: Are these subscribers adequately secured within cyberspace? Currently, a significant portion of activities are conducted via the internet, which is increasingly relied upon as a medium for service-oriented operations. Nevertheless, it must be emphasized that this over-reliance on cyberspace can render individuals and businesses susceptible to various cyber-attacks and threats.

Spruyt (2021) posits that, owing to several significant technological advancements, Nigeria may emerge as the preeminent hub for information technology expertise in Africa. Regrettably, this exceptional proficiency has been appropriated for nefarious purposes such as cybercrime. Furthermore, the World Bank (2022) indicates that Nigeria constitutes approximately half of West Africa's demographic landscape, comprising around 202 million inhabitants and an impressive total of 312,955,143 Mobile GSM users as of August 2022. The Nigerian Communications Commission (NCC, 2022) disclosed that roughly 210 million individuals are subscribed to the internet. Notably, despite Nigeria's ranking of 150th among global nations concerning internet speed, it reported a fixed broadband download speed registering at 9.70 megabits per second (Mbps) (Premium Times, 2022). Additionally, Nigeria was positioned 47th worldwide regarding the volume of internet subscribers. In this context, the International Telecommunication Union's (ITU) Connect 2030 initiative anticipates that by 2023, global internet penetration will reach 70 percent, thereby underscoring the imperative for a secure cyberspace (GCI, 2018).

Cyberspace has significantly contributed to the economic growth and sustainability of both developing and developed nations. However, these advantages are accompanied by various challenges, particularly cyber-attacks. Countries renowned for their stringent cybersecurity measures, such as the United Kingdom, the United States, and Russia, have experienced setbacks due to attacks and fraudulent activities, which have adversely affected their citizens, businesses, and governmental institutions. This has necessitated a cautious approach within the cyberspace community (Olusola et al., 2014). The primary objective of these fraudulent activities is financial gain, often executed through the unauthorized access of bank accounts belonging to individuals, businesses, and governments. Ogbonnaya (2020) reported that Nigerian commercial banks incurred losses amounting to ₦15 billion ($39 million) in 2018, a significant increase from ₦2.37 billion in 2017. Furthermore, Information Technology (IT) plays a vital role in bolstering the Nigerian economy, as well as in other developed nations such as the United Kingdom. However, the proliferation of IT also exposes individuals, corporations, and states to various risks often perpetuated in cyberspace.

The prevalence of cybercriminals, both in Nigeria and globally, is escalating due to the increase in interconnectivity and communication mediums facilitated by cyberspace. This surge has significantly hindered the ability to apprehend and prosecute individuals engaging in cybercrime,

with their targets frequently comprising information technology (IT) systems and related devices or services. Mbanaso, Chukwudebe, and Atimati (2015) argue that the socio-economic, political, and cultural frameworks of contemporary states are increasingly reliant on cyberspace, and any disruption to this domain could result in severe repercussions. They further contend that the internet has evolved into a battleground for warfare, a medium for novelty and networking, as well as a conduit for criminal activity.

While the internet offers boundless opportunities for commercial, social, and educational endeavours, it simultaneously introduces unique risks that threaten the economy. These risks have the potential to impact multiple sectors adversely, jeopardizing national development. Among the potential challenges are the erosion of the nation's reputation both domestically and internationally, threats to personal safety and property security, apprehension regarding business interactions with Nigerian entities, and substantial economic losses incurred through investments in the prevention and control of cybercrime (Chade, 2018).

Shehu (2014) asserts that the convergence of computing and communication technologies, coupled with the rapid proliferation of digital innovations, has yielded significant benefits for society. However, these advancements are accompanied by heightened risks on both national and international fronts. Our society is increasingly embroiled in criminal activities, while the public mandates that law enforcement agencies adapt to modern technological advancements that impact the processes of investigation and prosecution, thereby enhancing their capacity to combat crime effectively. In a related observation, Jackson and Robert (2016) highlight that the escalating incidence of cybercrime in Nigeria poses a significant concern not only for the citizenry but also for the government, as it tarnishes the nation's international image. This issue is a contributing factor to the reluctance of foreign investors to engage with Nigeria and its populace. Folashade and Abimbola (2013) contend that the information technology revolution, particularly associated with the internet, has engendered a dual-edged phenomenon: while it has imparted positive contributions to global society, it has also spawned numerous challenges that jeopardize societal order and foster a new wave of criminality on a global scale.

Similarly, Sesan (2019), Vladimir (2005) and Olumoye (2013) argue that the internet, a global network connecting millions of computers across different countries, offers broad opportunities for obtaining and exchanging information, but is now being used for criminal purposes to achieve economic gains. Cybercrime is a global phenomenon perpetrated by syndicates with regional and international networks. Supporting this, Guillane (2009), Herselman et al. (2005) and Gordon (2002) assert that, due to its lack of borders or physical boundaries and absence of any form of importation, customs, or forex constraints, coupled with the absence of rules and codes from a central governing authority, cybercrime can be committed by anyone from anywhere in the world. According to crime-research.org, as early as 2003, the United States was already leading the world in the percentage of cyber-attacks at 35.4 percent, followed by South Korea at 12.8 percent (Hassan, Lass & Makinde, 2012). In agreement with Frank and Asirifi (2015), a similar study by Norton revealed that a staggering 65% of internet users globally and 73% of internet users in the U.S.A. have fallen victim to cybercrime.

Based on the preceding analysis, it is evident that research on cybercrime is increasing; however, the challenges confronting citizens and the broader Nigerian economy stemming from these cyber thefts remain significantly underexplored. Consequently, this study seeks to address this knowledge gap by investigating the perceptions of cybercrime in relation to economic development in Nigeria, focusing on both prospects and challenges.

Research Questions

The following research questions were raised to guide the study;

1. What is the effect of cybercrime activities on economic development in Nigeria?
2. What are the challenges of cybercrime on economic development in Nigeria?
3. What measures could be taken to curb cybercrime to enhance economic development in Nigeria?

Deducing from research questions, the main objective of this study is to examine the prospects of cybercrimes and economic development in Nigeria. The specific objectives are:

1. To investigate the effect of cybercrime activities on economic development in Nigeria
2. To analyse the challenges of cybercrime on economic development in Nigeria
3. To examine these measures currently in place to curb cybercrime and their effects on economic development in Nigeria.

Clarification of Concepts

Cyber: The term relates to the characteristics of the culture of computer, information technology and virtual reality.

Crime: Crime is an action which constitutes an offense and punishable by law.

Cybercrime: Cybercrime refers to any computer related crime which is considered as illegal, unethical or unauthorized behaviour relating to the processing and the transmission of data.

Economic development is the process of improving economic welfare in an economy. It involves an increase in real incomes, higher life expectancy, lower poverty rate and a greater provision of basic amenities (Samuel 2019). Economic development can also involve a stronger economy enabling a greater range of social services that improve a nation's welfare. For instance, an undeveloped economy will be primarily based on agriculture and very limited social services such as health care and education. Economic development is a multifaceted process embracing economic growth, structural changes in the economy, improving the conditions, and quality of life of the population. Various models of economic development are known but for all their diversity and national characteristics, there are general parameters characterizing this process (Mary, 2017). Economic development is a broader concept than economic growth. Development reflects social and economic progress and requires economic growth. Growth is a vital and necessary condition for development, but it is not a sufficient condition as it cannot guarantee development. According

to Amartya (2001), development is about creating freedom for people and removing obstacles to greater freedom. Greater freedom enables people to choose their own destiny. Obstacles to freedom, and hence to development, include poverty, lack of economic opportunities, corruption, poor governance, lack of education and lack of health.

Cyberspace: Cyberspace is an international and unstable domain which is identified by the use of electrons and electromagnetic spectrum whose aim is to create, modify, store, exchange, extract, use and delete information without a sole administrator (Mayer, 2014). Nigeria, being on the international domain, benefits from the existence of cyberspace. As a developing country with a growing economy, Nigeria stands a greater chance of benefiting from this space because of her population, which is fast growing and also serves as a market hub for Africa (Ukwuoma, 2019).

Theoretical Foundation

This study theoretically synthesized the differential association theory propounded by Edwin Sutherland, an American Sociologist. This Differential association theory proposed that through interaction with others, individuals learn the values, attributes, techniques and motives for criminal behaviours. This implies that the environment plays a major role in deciding which norms people learn to violate (Onodugo, 2016). The principle of differential association asserts that a person becomes delinquent because of an excess of definitions favourable to violation of law over definitions unfavourable to violation of law. In other words, an individual will become a criminal if they are exposed to more favourable criminal influences rather than legal influences. Simply put, an individual will break a law if they see/have more reasons to break it than to stay in compliance with that law. This can be seen in environments with poor socio-economic conditions, which may encourage negative views towards the law and authority governing the place.

According to Sutherland (1939, in Onodugo, 2016), criminal behaviours are learnt. It is learned through interaction with other people in a process of communication. This would mean a peer group influence where an individual is incorporated to learn/participate in criminal activities just by watching and interacting with a person with these criminal tendencies or engrossed with criminal behaviour within an intimate personal group. The learning includes techniques on how to commit crime, which are sometimes very complicated, sometimes simple, and they learn the specific directions of motives, drives, rational and attitudes for committing a crime. This means that an individual will be brain-washed into believing that the behaviour which they may have previously believed was wrong can now be seen as right through rationalization of their action.

Furthermore, an individual will be pushed into deviant behaviour depending on their view of the legal code as being favourable or unfavourable. Interestingly, differential association may vary in frequency, duration, priority, and intensity. Hence, the theory states that criminal behaviour is an expression of general needs and values; it is not necessarily the fulfilment of these needs and values that causes deviant behaviour since non-criminal behaviour is an expression of these same needs and values.

Differential Association is a theory with a number of postulations which help to explain the reasons why cybercrime is on the rise in our society. The main premise of applying the theory of

Differential Association as it pertains to cybercrime posits that criminal behaviour is acquired through social interactions. The archetype of a cybercriminal is often characterized by high intelligence, extensive knowledge, and proficiency in computer technology. Such individuals typically engage in social interactions via electronic communications with others who possess similar technological interests. This theory, originally developed to elucidate white-collar crimes, is particularly relevant for understanding the motivations and actions of individuals who engage in cybercrime.

METHODS AND MATERIALS

This study employs a qualitative research design utilizing desk research methodology. Data were gathered from secondary sources including the internet, academic journals, periodicals, textbooks, and review articles. A thematic analysis approach was implemented to interpret the qualitative data, presenting it in a structured and accessible manner.

RESULTS/DISCUSSIONS

Understanding the concept of Cybercrime and economic development

The concept of cybercrime was first articulated by Peter Cassidy, the Secretary General of the Anti-Phishing Working Group, to differentiate between computer programs specifically designed to facilitate financial crimes and other types of malicious software (Shehu, 2014). Cybercrime has emerged as a significant subject of discourse across various academic and professional fields (Ibikunle & Eweniyi, 2013). Halder and Jaishankar (2011) define cybercrime as an offense characterized by a criminal motive, perpetrated against individuals or groups connected to the internet through computers or mobile devices. This form of crime not only seeks to harm the reputation of the victim but can also inflict irreversible damage on critical infrastructure and hardware.

According to Symantec Corporation, the foremost global authority in computer security, cybercrime encompasses any criminal act executed via a computer, network, or hardware device (Theohary & Finklea, 2015). Maitanmi, Ogunlere, and Ayinde (2013) further elaborate on this definition, positing that cybercrime involves offenses committed by individuals utilizing computers as instruments and the internet as a conduit to achieve various illicit objectives, including but not limited to illegal downloading of music and film, piracy, and spam dissemination.

Alarmingly, Allen (2021) estimates that the African business sector incurred losses amounting to approximately $3.5 billion due to online scams and theft in the year 2017, categorizing cybercrime as a principal threat to the economies of Nigeria, the African continent, and the global market at large. This underscores the urgent need for enhanced cybersecurity measures and comprehensive policy frameworks to mitigate the risks associated with cybercriminal activities.

Causes of Cybercrime in Nigeria

Several scholars have sought to provide answers to the undying question of the causes of cybercrime and why cybercrime continues to flourish in our society. Dashora (2011) has adduced the following reasons in this regard:

i. Human negligence on cyber security, which creates easy access for cybercriminals;
ii. Capacity to store mega-sized data in comparatively small space;
iii. Cybercrime is associated with loss of evidence as data are routinely destroyed, making it difficult to apprehend offenders;
iv. Complexities of the computer software and program engender human errors.

Likewise, Swanson et al. (1988, cited in Iwarimie-Jaja, 2012) opined that computer crimes flourish due to the following factors.

i. Insufficient caution in hiring, training and assigning personnel;
ii. Unusual situations can be identified as errors rather than crimes;
iii. Computer security is lax;
iv. Managers disassociate themselves from operations.
v. Obtaining necessary evidence may be difficult;
vi. Certain types of computer crimes are easily accomplished by people with few skills.

In addition, Udeson et al (2023) identified the following causes of cybercrime in Nigeria:

i. Desperation for quick wealth, values for materialism and negative role models;
ii. Increasing youth unrest and Unemployment;
iii. Weak enforcement of cybercrime laws and inadequately equipped agencies;
iv. Rapid urbanization.
v. Peer culture and family pressure.
vi. Impunity.

Various Cybercrimes in Nigeria

The following are some of the cybercrimes most prevalent in Nigeria.

i. ***Yahoo Attack:*** This is also called 419 because section 419 of the Nigerian criminal code has a law against such offenders. It is characterized by using e-mail addresses obtained from Internet access points using e-mail address harvesting applications (web spiders or e-mail extractors). These tools can automatically retrieve e-mail addresses from web pages. Nigerian fraud letters join the warning of impersonation scams with a variation of an advance fee technique in which an e-mail from Nigeria offers the recipient the chance to share a percentage of a huge amount of money that the author, a self-proclaimed government official, is trying to siphon out of the country.
ii. ***Hacking:*** Here, Nigerian hackers are engaged in brainstorming sessions at trying to break security codes for ecommerce, funds point cards and e-marketing product sites.

iii. ***Software Piracy:*** Piracy involves the unlawful reproduction and sharing of applications software, games, movies/videos and audios.

iv. **Pornography:** Pornography covers all types of‟ photography, films and videotapes with varying degrees of sexual contents. The Internet has provided a free market for this crime as so many pornographic sites are now all over the net. This is one of the most popular cybercrimes in Nigerian academic institutions

v. ***Credit Card or ATM Fraud:*** Hackers can steal credit card or ATM numbers when users type the credit card number into the seller's Internet page for an online transaction or when withdrawing money using an ATM card. The hackers can abuse this card by impersonating the credit card holder.

vi. ***Denial of Service Attack:*** This is an act by the fraudster who floods the bandwidth of the victim's system or fills his email inbox with junk mail, depriving him of the services he is entitled to access or supply.

vii. ***Internet Relay Chat (IRC):*** Crime IRC servers have chat rooms in which people from anywhere in the world can come together and chat with each other. Criminals use it to meet co-conspirators, and hackers use it to discuss their exploits and share techniques.

viii. ***Virus Dissemination:*** A virus is a computer program that infects files, frequently executable programs, by inserting a duplication of itself into the file. There are different types of viruses, and each type requires human participation (usually unaware) of their spread.

ix. ***Phishing:*** Phishing refers to cloning product and e-commerce web pages in order to dupe unsuspecting users. This is a technologically advanced scam that often uses spontaneous emails to trick people into disclosing their financial and/or personal data.

x. ***Cyber Plagiarism:*** This is the act of stealing peoples‟ ideas through the Internet public domains. This is very common in academic institutions as students and lecturers alike use it to steal other people's ideas and publish them as their own original work.

xi. ***Spoofing:*** To have one computer on a network to act like another computer, usually one with exceptional access rights, so as to gain access to the other systems on the network.

xii. ***Cyber Stalking:*** The fraudster follows the victim by distributing mails and entering the chat rooms frequently.

xiii. ***Cyber Defamation:*** The fraudster sends e-mails containing defamatory content to people related to the victim or posts it on a website.

xiv. ***Salami Attack:*** Salami assaults are flamboyant economic scams or exploits against confidentiality by comprehensive data gathering.

xv. ***Cyber Terrorism:*** According to the U.S. Federal Bureau of Investigation, cyber terrorism is any premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents. It means that any act intended to instil fear by accessing and distorting any useful information in organizations or Government bodies using computer and internet is generally referred to as cyber terrorism.

Implications of Cybercrime and Economic Development in Nigeria

The proliferation of cybercrime has proven increasingly resilient to the countermeasures implemented by crime prevention agencies, resulting in significant detrimental effects on both local and global economies. In Nigeria, cybercrimes are predominantly executed by young male individuals colloquially referred to as "yahoo-boys" or "yahoo-zee millionaires." A substantial number of these perpetrators are either undergraduates at various Nigerian universities or recent graduates engaged in illicit activities such as hacking, cloning, and defrauding unsuspecting victims. They utilize a range of sophisticated tools, including password crackers, key loggers, network sniffers, port scanners, and vulnerability scanners (Folashade & Abimbola, 2013). Furthermore, there has been a notable increase in corporate internet fraud, wherein unethical banking officials collude with external parties to misappropriate depositor funds. As a clandestine criminal enterprise, cybercriminals in Nigeria meticulously plan their operations, as the selection of their victims—specific systems or networks—is carried out intentionally rather than at random. Their targets predominantly consist of individuals characterized by gullibility, greed, inexperience, and a fervent desire for expedited financial gain or romantic relationships.

The prevalence of these cybercrimes has created a poor image for Nigeria among the committee of nations, branding it as one of the most corrupt countries in the world. As a result, information flowing from the country is characterised as questionable due to the criminal elements that render it inaccurate and unreliable (Iwarimie-Jaja, 2010). This tarnished national image affects how Nigerians are treated abroad, often viewed with suspicion and extreme caution, as they are stereotyped as 419ers (conmen) and therefore deemed untrustworthy. Private companies worldwide are starting to take steps to block emails originating from the country, and financial instruments are accepted with extreme caution. Foreign investors are wary of the country, considering it a risky and unattractive business environment.

In examining the ramifications of cybercrime in Nigeria, Folashade and Abimbola (2013) assert that such criminal activities significantly impede the socio-economic progress of the nation. They argue that cybercrime fosters an environment of mistrust and scepticism in profitable transactions, deprives innocent Nigerians of opportunities abroad, and results in considerable job losses and diminished revenue. Similarly, Sesan, Soremi, and Oluwafemi (2012) report that in 2012 alone, the financial impact of cybercrime amounted to an estimated customer loss of N2,146,666,345,014.75 ($13,547,910,034.80) in Nigeria. Furthermore, findings from the study conducted by Maitanmi et al. (2013) indicate that cybercrime hinders socio-economic development by discouraging foreign investment, largely due to the erosion of confidence in the Nigerian economy that it engenders. The research also highlights the role of cybercrime in facilitating various illicit activities in Nigeria, including intellectual property theft, disruption of public services, drug trafficking, and terrorism. Ultimately, the impact of cybercrime remains pervasive, presenting numerous potential challenges to the economic development of the country.

Perception of challenges associated with the various types of cybercrime evident in Nigeria

The prevalence of internet-based cybercrime has emerged as a significant threat to the socioeconomic and technological progression of Nigeria. According to Shehu (2014), cybercrime

activities, including cyberstalking, harassment, blackmail, and cyber terrorism, pose a substantial risk to individuals' rights to privacy and fundamental freedoms. Furthermore, forms of cybercrime such as pornography, child predation, online gambling, and online prostitution erode moral standards within society and place it at risk of a breakdown in social norms and values. This criminal activity has diverted the attention of many Nigerian youths from engaging in productive endeavours—such as manufacturing, construction, and large-scale agriculture—that would contribute to economic growth, instead luring them towards criminal pursuits due to the allure of the ostentatious lifestyles it promises (Folashade & Abimbola, 2013). In conclusion, the challenges faced by Nigerians are largely attributable to inadequate infrastructure, low levels of digital literacy, and insufficient information dissemination.

Unsuccessful Measures of Curbing Cybercrime in Nigeria

In pursuit of eradicating cybercrime in Nigeria, the government has implemented several measures, including the enactment of key legislative acts such as the Cybercrime (Prohibition, Prevention, etc.) Act 2015, the Constitution of the Federal Republic of Nigeria (1999, as amended), the Nigerian Communications Act 2003, the Economic and Financial Crimes Commission (Establishment) Act 2004, the Advanced Fee Fraud and Other Fraud Related Offences Act 2006, the Money Laundering (Prohibition) (Amendment) Act 2012, the Evidence Act 2011, and the National Information Technology Development Agency (NITDA) Act 2007, among others. Despite the establishment of these laws and agencies, the prevalence of cybercrime in Nigeria remains alarmingly high. Furthermore, the impact of cybercrime on per capita income is significantly detrimental, suggesting that these illicit activities have adversely affected the economic development of Nigeria. This phenomenon poses severe threats to the nation’s technological, educational, political, security, and socio-economic advancement.

Conclusion

This study conducts a comprehensive analysis of the economic implications of cybercrime in Nigeria. It reveals that the pervasive nature of cybercrime adversely affects the country's economic development by undermining its global image, deterring foreign investment, and eroding trust in the digital economy, resulting in substantial financial losses for individuals, businesses, organizations, and the government.

The proliferation of cybercrime in Nigeria can be attributed to several critical factors, primarily the insufficiency of specific legislation aimed at mitigating this issue. Numerous traditional crimes are being facilitated through the utilization of computers and networks, leading to the emergence of previously unimaginable forms of wrongdoing, owing to the remarkable capabilities of information systems. Furthermore, corporate internet fraud has escalated, as unscrupulous banking officials collude with external parties to misappropriate depositor funds, contributing to the rise of numerous 419 perpetrators within the economic landscape. The prevalence of fraudulent practices associated with cybercrime has engendered the rapid accumulation of wealth by certain individuals within the economic framework. However, these illegally acquired funds are often not utilized productively to foster economic growth, thereby posing a significant threat to overall economic development.

Recommendations

Following these submissions, the paper, amongst others recommends that:

i. The government should provide jobs and entrepreneurial development opportunities to engage young people to keep them away from crime, while pursuing vigorous enlightenment campaigns for the citizens on basic preventive and protective measures against cybercrime.
ii. Telecommunication service consumers should protect their devices from loss as they can become tools in the hands of cyber criminals who often steal them. Such theft are inevitable therefore consumers should be proactive by reporting any loss of device to service providers for immediate deactivation or report suspected cyber criminals and their activities to NCC or the police and other members of the nation's security community.
iii. The Nigerian government should enact comprehensive laws to curb cybercrime, while building the capacity of the law enforcement agencies in tackling contemporary cyber technology.

REFERENCES

Allen, N. (2021), Africa's evolving cyber threats. *African Center for Strategic Studies.*

CSIS (2014) "Net Losses: Estimating the global cost of cybercrime", Economic impact of cybercrime II. *Center for Strategic and International Studies* (CSIS)

Cybercrime Act (2012). Nigerian Cybercrime (Prohibition, Prevention Etc.) *Act* 2015.

Dashora, D. (2011). Cybercrime in the society: problems and preventions. *Journal of Alternative Perspectives in the Social Sciences, 3*(1), 240-259.

Eze, B. O. (2023). Cybercrime: legal protection and liabilities for nigerian internet users. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4605510

Folashade, B.O. & Abimbola, K.A.(2013). The nature, causes and consequences of cybercrime in tertiary Institutions in Zaria-Kaduna State, Nigeria. *American International Journal of Contemporary Research,* 3.

Frank, A.D. & Asirifi, M.K. (2015). The impact of cybercrime on the development of electronic business in Ghana. *European journal of business and social sciences,* 4.

Halder, D. & Jaishankar, k. (2011). Cybercrime and the victimization of women: Laws, Rights, and Regulations. IGI Global.

Hassan, A.B. Lass, F.D. & Makinde, J. (2012). Cybercrime in Nigeria: Causes, effects and way out. *ARPN Journal of Science and Technology, 2.*

Henry C. U. (2021). Cybercrime: An emerging threat to economic development in Nigeria. National Institute for policy and Strategic Studies Kuru, Nigeria. *An International Journal of Cyber Education, 3*.

Herselman, M. & Warren, M. (2003). Cybercrime influencing businesses in South Africa, issues in information science and information technology.

Ibikunle, F. and Eweniyi, O. (2013). Approach to cyber security issues in Nigeia: Challenges and Solutions. *International Journal of cognitive Research in science Engineering and Education (IJCRSEE), 1*.

Iwarimie-Jaja (2012). Criminology: The study of crime. Springfield Publishers.

Iwarimie-Jaja, D. (2010). Criminology; crime and delinquency in Nigeria. Pearl Publishers.

Kovacs, A. M. (2024). Here there be Dragons: Evolution, Potentials and Mitigation Opportunities of Cybercrime in Nigeria: A Review, Analysis, and Evaluation. *Journal of Central and Eastern European African Studies*, *2*(1). https://doi.org/10.59569/jceeas.2022.2.1.55

Lakshmi P. & Ishwarya, M., (2015). Cybercrime: Prevention and Detection". *International Journal of Advanced Research in computer and Communication Engineering,* 4(3).

Lewis, J. (2018). Economic impact of cybercrime-no slowing down. *Center for Strategic and International Studies* (CSIS). McAfee.

Maitanmi O., Ogunlere S. & Ayinde S. (2013) Impact of cybercrimes on Nigerian economy, *International Journal of Engineering and Science* (IJES, 2(4),

Meke, E.S.N. (2012). An article Urbanization and cybercrime in Nigeria: Causes and Consequences".

NCC (2022) subscribers Data – Nigerian Communications Commission https://www.ncc.gov.ng>subscribers

Nigeria Criminal Code Act, (2004), Cap c38 LFN,

Ogbonnaya, M. (2020), Cybercrime in Nigeria demands public – private action. *Institute for Security Studies Africa.*

Olumoye, M. Y. (2013). Cybercrime and technology misuse: Overview, impact and preventive measures. *European Journal of Computer Science and Information Technology,* 1.

Premium times (2022) Nigeria ranks 150th in global internet speed –survey https://www.premiumtimesng.com

Punch Nigeria (2022) Nigeria's active Mobile subscribers hit 210M. https://punchng.com>Nigerias.action

Ribadu, (2007), Cybercrime and commercial fraud: *A Nigerian perspective. A paper presented at the Modern Law for Global commerce*.

Sesan, (2019), Youth and cybercrime in Nigeria'. The Punch Nigeria. https://punchnig.com/youth-and-cybercrime-in-Nigeria/

Shehu, A.Y. (2014), Emerging issues in cybercrime: Causes, implications and effects for the legal profession, *Online Journal of Social Sciences Research,* 3.

Spruyt, E. (2021), African software developers: Best countries for sourcing in 2021. https://tunga.io/african-software-developers-best-countries-for-sourcing/

Singh, O. A., Tiwari, A., & Chauhan, D. (2024). Cybercrime: Trends, challenges, and mitigation strategies. *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), 4*(3), 140–142. https://doi.org/10.48175/IJARSCT-22824

The World Bank (2022), Nigeria: development news, research, data / World bank Nigeria. https://www.worldbank.org>country

Theohary, C.A & Finklea, K. (2015), Cybercrime: conceptual issues for congress and U.S law enforcement. *Congressional Research Service Report*.

Udosen, J.I, Olarinde, E.S, Anwana, E.O, & Adiodun, T.O. (2023), Prosecution of cybercrimes in Nigeria: challenges and prospects. *International Conference on Cyber Management and Engineering.*

Vanguard News (2019) NCC move to secure Nigeria's cyber-space

Vladimir, G. (2005). International cooperation in fighting cybercrime. www.crimeresearch.org.