Journal of Research in Education and Society, Volume 15, Number 1, April 2024
ISSN(p): 2141-6753 ISSN(e): 2795-3033
Published By
International Centre for Integrated Development Research, Nigeria
In collaboration with
Copperstone University, Luanshya, Zambia

The Threats of Cyber Crimes in Nigeria: Causative factors in Society and Development

Phillips Olubiyi
Department of General Studies
The Federal Polytechnic, Ilaro, Ogun State, Nigeria
E-mail: olubiyi.philips@federalpolyilaro.edu.ng

ABSTRACT

This review interrogated some causative factors that have influence on the increasing incidences of cybercrimes in Nigeria. It adopted an analytical, theoretical and textual methodological approach to undertake an inventory of the degree of cybercrimes in Nigeria. By adopting an analytical, theoretical and textual methodological approach, it argued that there exist various gaps in Nigeria's cyber security architecture including the absence of scientific data base and adequate research agencies needed for stemming the erosion of Nigeria's path to progress due largely to the spectra of cybercrime.

***Keywords**: Cybercrime, National Security and Development*

INTRODUCTION

Phenomenal innovations in information communication technology (ICT) has have opened up the infinite technological space called the internet. Representing one the rapidly growing frontiers of technological advancement the internet through the cyberspace is able to give solutions and answers to unquantifiable volume of questions daily. From government to industry, business and non-governmental bodies, agencies and organizations, the internet has unbundled transactional and business procedures through customized report generation sorting and coding on real time basis. Ironically, the incursion of the internet into human existential affairs has equally led to unintended development of cyber-criminal activities including phishing, credit card frauds, identity theft and a variety of automated teller machines frauds (ATM's). Odinma (2010) observed that cybercrime in Nigeria has transcended traditional criminality and is currently posing serious danger in various forms to the security architecture of many countries beyond Nigerian boarders. According to the European, Middle East and Africa group (EMEA, 2003), an acronym used by institutions, governments and global spheres of marketing, media and business when referring to this region,. Nigeria currently occupies the 43rd position and is also the 3rd amongst the ten countries in the world that is acknowledged to be involved in cyber-criminality globally. Olumide and Victor (2010) argued that the erosion of standard of the Nigerian Educational System derives from cybercrime activities traceable to the adoption of immoral and anti-social behavioural patterns amongst teeming Nigerian students desiring to become rich quickly without being ready to embrace the virtue of hard work and contentment. Bhawna (2016) noted that “the cyberspace in general has morphed into an environment for cyber related crimes and allied offences although the benefits that the internet has impacted on mankind remain indelible”.

Objectives of Study

Essentially, this paper attempted to

1. Review some of the causative factors responsible for the high incidences of cyber criminality especially amongst the Nigeria youth.
2. Identify and explain the different types of cybercrime in Nigeria.
3. Recommend strategies for combating cybercrimes in Nigeria to fostering national development.

LITERATURE REVIEW

Igwe (2021) argued that “cyber criminality has continue to be on the increase in Nigeria even as the number of it perpetrators and victims has equally been on the rise”. Accordingly, many of these cyber fraudsters are half baked school dropouts while some are university, polytechnic and colleges of Education graduates without jobs, known as “Yahoo boys” a phrase popularized in Nigeria and applicable to cyber fraudsters (Azeez, and Osunade, 2009).

The Federal Bureau of Investigation; (FBI) recently identified Nigeria as the 16th country that is mostly recognized for cyber criminality globally (FBI, 2020). The factor responsible for the increasing perpetrators in Nigeria is traceable to the erosion of ethical and societal moral values occasioned by destructive and negative influences of the members of the political class many of which did not requires special knowledge nor academic qualifications to enter the national political arena with a view of becoming stupendously wealthy overnight (FBI, 2020).

Ribadu (2007) observed that the predominant types of cyber criminalities operational in Nigeria includes amongst others internet fraudulent purchases; cloning of websites and impersonation with the internet to defraud victims online with continued expansion usage of and accessibility to the internet globally, millions of young adults of both sexes have the tendency to be attracted to engaging in cybercrimes blended with activities related to occultism and ritualism that may involve murdering of targets of such occultism activities.

Figure 1: Suspected Cybercriminals in EFCC Custody

Source: EFCC 2022

Nigeria's Solicitor-General, Beatrice Jedy-Agba (2023), argued that "in the post-covid era in Nigeria, digital revolution has basically re-shaped life and although its boast some positives yet there are associated problems including increase in the percentage of cyber criminality". According to her, "The global context of cybercrime that has been dubbed as a "Phenomenon without boundary" that requires governments at various levels in Nigeria to put in place institutions and agencies with the appropriate capacities to confront it and ensure that "awareness creation its priority". According to the Economic and Financial Crime Commission (EFCC) who claimed to have secured about 1,084 cyber related crime convictions in 2023. The Director, Legal and Prosecution, Department of EFCC, Sylvanus Tahir, argued "that it is easier, cheaper and faster to commit cybercrimes than other forms of traditional crimes" Still on the downside, the Senate in Nigeria lamented the annual loss of about $500 million (five hundred million dollars) by Nigeria's digital annual economy to cybercrime (EFCC, 2023).

The President of the Senate in Nigeria, Senator Godswill Akpabio (2023) argued that "there is an urgent need to institutionalize a broad-based legal structure to pursue, deter, investigate and punish cybercrimes in Nigeria as the phenomenon of cybercrime has come to symbolize a major threat to the Nigeria State, personal security and economy.

Internet penetration in Nigeria in the 21st century has reportedly grown exponentially, meaning that the usage of the internet by Nigerian's especially in relation to her demography has also increased tremendously from 3.45 percent in 2005 to 47.4 percent in 2014 (WDI, 2016). The increased level of use of the internet by Nigerians has attracted both positive and negative consequences. Cybercrime has become a daunting national problem regardless of the current level of awareness and attention extended to curbing it threat in Nigeria.

Shafic and Adamu (2011) observed that cyber criminality was estimated to have cost countries including Japan, United Kingdom U.S.A, Australia and Brazil between USD $4.3 Million and USD $17.3 Million annually. The report added that cybercrime has continued to worsen different countries relationship with others by way of tarnishing the national image of the countries where there is predominance of cybercrime since such countries are seen as haven for cybercrime activities which make investors more cautious in investing their funds thereby directly injuring the stability of many national economies.

Ogai (2007) has described "National Development", as a well-rounded growth of the different areas and aspect of a country whether economic, political, cultural, social and scientific. For a country like Nigeria, the consequences of cybercrime include profit pilferage, welfare losses, revenue losses and disruption of business activities. The Financial Derivative Company (FDC, 2020) reported that the loss of revenue by Nigeria as a result of cybercrime stood at N250 billion or ($649 million) as at 2017 and N288 billion or ($800 million) as at 2018 respectively.

A critical consequence of cybercrime on Nigeria's national growth and development is that cyber espionage is also making an in-road and gaining a fast traction in the Nigerian social and economic space as the cyberspace is now being deployed to attract funds and swell the ranks of terrorist groups. Akinyetun (2021) argued that the Boko Haram terrorist organization in Nigeria penetrated the Department of State Security (DSS) servers in 2013; exposed confidential information include the names of members of families and private addresses of these family members online thus straining national security. Ogunjobi (2020) equally observed that the coming of the internet has also beamed awareness on the high degree of cybercrime amongst the Nigerian youth with many of these youth dropping out of schools to register with coalitions of cybercrime thus negating the positive values that Nigeria's educational institutions are expected to impact on Nigerian youth.

CONCLUSION AND RECOMMENDATIONS

Cybercrime has become a major threat and concern to the Nigerian people, national development and national security. This paper has attempted to show that the continuous abuse of the internet exposes public safely and national security to cybercriminals. Nigeria showcases ineffective legal institutions and frameworks in the vital area of cyber regulations and enforcement of relevant cyber laws. There is the need for various stakeholders including governments across all levels in Nigeria and non-governmental agencies to not only create a cyber-security awareness culture that would involve the public, security agencies and cybercafés operators, but that would also address issues that relates to enforcement of laws as one of the strategies for stemming the scourge of cybercrime.

In addition, cyber education needed to be introduced into Nigerian academic curricular as a compulsory course domiciled in the department of crime management to re-educate the Nigerian youth on the negative consequences of cybercrime. Finally, The Economic and Financial Crime Commission (EFCC) should endeavour to partner other law enforcement agencies including the Nigerian cyber forensic department and the Nigerian police to monitor and investigate suspected cyber activities across the 36 States as well as establish a scientific data base for prosecuted cases which would help serve as a quick point of reference and future retrieval of valuable cyber information.

REFERENCES

Akinyetun, T.S. (2021). "Poverty, Cybercrime and National Security in Nigeria" Journal of contemporary sociological issues, Volume 1, issue 2, pp. 1-23. DOI: 10.19184/csi.vli2.24188.

Beatrice Jedy-Agba (2023), EFFC "FG decries rising cybercrimes, EFCC secures 1084

EFFC (2023). "FG decries rising cybercrimes, EFCC secures 1084 convictions" www.Punch Newspaper. Online, November 8th

FDC (2020); Federal Derivatives Company report 2020 National reports. http://pdf/DerivativescompanyofNigerian.com

FBI (2020) Internet crime report on Nigeria *on cybercrime in Nigeria.*

Azeez N. A. and Osunade O. (2009). Towards ameliorating cybercrime and Cyber security International Journal of Computer Science and Information Security, Vol. 3, No. 1,

Odinma, A. C. (2010): Cybercrime & Cert: issues & Probable policies of Nigeria, DBI Presentation, November 1-2.

Ogai, J.O. (2007). "An Analysis of the Concepts of Development and Underdevelopment" in O. Uwake, Communication National Development, (2nd Edition); London, Cecta Books Publisher, 25-31

Ogunjobi, O., (2020) "The Impact of Cybercrime of Nigeria Youth" Research Gate Publication. http://www.researchgate.net/publication/347436728

Olumide, O.O. and Victor, F.B. (2010): E-crime in Nigeria: trends, Tricks, and Treatment. The Pacific Journal of Science and Technology, Volume 11, Number 1 (spring)

Ribadu, E. (2007). "Cyber Crime and Commercial Fraud: A Nigeria Perspective". A Paper Presented at Conference of the Modern Law for Global Commerce, Vienna 9th – 12th July.

Shafic C. & Adamu (2011) Cybercrimes and the Nigeria Academic Institution Networks Cybercrime, its impact on government, society and the prosecutor

WDI (2016). World Development indicator (WDI), International Bank for reconstruction and Development/ The World Bank; Washington D.C, U.S.A. http;//diplomatie.gouv.fr/IMG/pdf/paris call cyber cle443433.pdf.