PLASU Law Journal (PLASULJ) Vol. 1, No. 1, 2024
A Publication of Faculty of Law, Plateau State University, Bokkos –Nigeria
EISSN 1596-0625(Online)https://journals.plasu.edu.ng ISSN: 2695-2661 (Print)

EVALUATION OF NIGERIA'S LEGAL FRAMEWORK FOR COMBATING CYBERCRIMES

Chakaam N. Dalan[1] **Sarah R. Garba**[2] **Rinyen M. Donglong**[3]

Correspondent email: rinyenm@gmail.com

Abstract

With the advent of modern technology and the internet, we have moved from the slow analog style of sourcing for information to the fast, efficient and reliable digital style of gathering information. Imagine getting answers to complex questions just with the click of a button! Unfortunately, unscrupulous elements have turned the internet space into a haven for the commission of cybercrimes. This crime is prevalent not only in Nigeria but also worldwide. The connection between organized crimes and the internet has increased the insecurity of the digital world especially as it relates to cyber security in Nigeria. This article aimed at examining the existing laws on cybercrime in Nigeria as well as the legal and institutional framework for combating cybercrime. It was found that Nigeria's ineffective system of regulating the use of internet has led some persons to be able to hack into personal information systems of individuals, corporate organizations and government agencies alike thus, leading to huge data and financial losses. It has also found that poor sensitization about the use of the internet and the insufficient tools and trainings for government officials has also contributed to the ever rising spate of cybercrimes in Nigeria. This article recommended a review of the existing Cybercrime Prevention Act 2015 to meet with the existing realities on cybercrime in Nigeria, prevent ambiguity in its application in order for it to compete adequately with the legal framework of cybercrimes globally. There is also the need for stringent punitive actions to deter would be cybercrime perpetrators.

Key words: Cybercrime, Legal Framework, Internet, Technology

[1] Lecturer, Faculty of Law, Plateau State University, Bokkos, Plateau State, Nigeria
[2] Lecturer, Faculty of Law, Plateau State University, Bokkos, Plateau State, Nigeria
[3] Lecturer, Faculty of Law, Plateau State University, Bokkos, Plateau State, Nigeria

Introduction

With the advent of development especially in the technology aspect, it can be said that Nigeria, indeed the whole worlds have metamorphosed into one giant global village. Different nations have been brought together under the wide umbrella of technology and this has in turn made the world advanced as we can now access the economies of the world via the internet [1]. There are approximately two billion users of internet and over five billion mobile phone networks users across the world[2].According to a report given by the International Telecommunications Union (ITU), as at 2011, there were over forty-five million users of internet in Nigeria, which is 26.5% of the population[3]. As at 2022, Nigeria has nearly 84 million internet users and this figure has been projected to rise to 117 million users in 2027 with internet penetration percentage of about 38% in 2022 alone [2]. In 2023, there are about 90.48 million internet users [3] and about 97.13 in the year 2024[6] (the year has not ended and as such, we might record even higher numbers).

It is without gainsaying that the internet has become an indispensable tool to education, law, engineering, medicine and the society at large. The internet has become the pillar of legal practice as we can now access law reports, journals, judicial decisions, laws and all the likes with the click of a button. The internet has also created opportunities to provide new and better service delivery to clients[4]. Ilobinso[5] opined that invention of electronic technology and the internet has changed how we communicate, learn, work and do business and has also brought the world's people closer in time and space with businesses working efficiently as both suppliers and consumers now have greater choice and shop from the comfort of their homes, offices or even while travelling.

---

[1] Nnamdi K. Akanni,Agu C. Queeneth, 'Information and Communication Technology : An Evaluation of Cybercrimes Laws in Nigeria' *Journal of International Trade Law and Contemporary Issues (2023)* (3) (3) 2.

[2] International Telecommunucation Union. Understanding Cybercrime: Phenomena, Challenges and Legal Response. http//www.itu.int/ITU-D/cybersecurity/legislation. Accessed 10 July, 2024.

[3] J Herhalt, 'Cyber Crime- A Growing Challenge for Governments' <https://www.kpmg.com/Global/en/IssuesandInsights/ArticlesPublications/Documents/cyber-crime.pdf> Accessed 10 July 2024

[4] https://www.statistica.com. Nigeria: number of internet users in Nigeria from 2018 to 2022, with forecasts from 2023 to 2027.

6 Ibid.

[6] Ibid.

[7] M. Olushola, 'Cybercrimes and Cyber Laws' *International Journal of Engineering and Sciences* (2013) (2) (3) 3.

[8] Ilobinso I., 'Formation of Electronic Contracts :Moulding the Traditional Contracts with Contemporary Electronic Commerce' *The Commercial and Industrial Law Review* (2016)

(2) 50.

With advancement in information technology comes the proliferation of fraudulent activities and crimes on unsuspecting internet users who are the grieving victims. There have been instances where they are defrauded of their hard earned money by ordering goods or services online[1]. The use of computer systems to perpetrate crimes and attacks, have birthed a new kind of terrorism hence the need to combat the threat as a global challenge, seeing that the cyberspace is not safe due to sophisticated cyber terrorists hacking computers, equipment to endangering millions of lives and the nation's security [2] . As a result of the horrors' of cybercrimes highlighted above, a high percentage of Nigerian businesses and consumers, are still very wary about doing extensive business over the internet. This is primarily because of the risk associated with concluding a commercial transaction from a distance with an anonymous party due to frauds, cybercrimes and the absence of a legal framework governing electronic transactions in Nigeria and uncertainty surrounding the ability of the parties to form valid and enforceable contracts via internet or paperless mode of communication. There is an urgent need to address this menace and restore pride and glory to the image of Nigeria (both at home and abroad).

Conceptual Clarifications

Cybercrime

There is no universal definition of cybercrime as both scholars and jurists alike have different perspectives of cybercrime. Consequently, cybercrime can be defined as any online wrongdoing ranging but not limited to spam emails and denial of service attacks to malware[3] Cybercrime can be defined as any criminal activity that involves a computer or networked device[4] . McQsuade,[5] in his book, defined cybercrime as the use of electronic devices or computers via information systems to facilitate illegal activities. The grouse with this blanket' definition of cybercrime lies in the fact that it is too broad and can be ambiguous. For example, if one uses a keyboard to commit battery, it does not mean that a cybercrime act has been committed. Another author defined cybercrime as computer- mediated activities which are either illegal or considered illicit by certain parties and

---

[9] Olujobi O. Joshua, 'Analysis of the Legal Framework for Combating Cybercrimes: A Tool for Economic Development in Nigeria' *Kwasu Law Journal* (2021) (2) (1) 116.

[10] Oyinde O, Omidoyin T.J, 'The Crime of Cyber Terrorism: Myth or Reality?' *AfeBabalola University Ado-Ekiti Law Journal* (2017) (1) (5) 101-120.

[11] R. McCusker, 'Transitional Organized Cybercrime: Distinguishing Threat from Reality' *Crime, Law and Social Change Journal* (2006) (45) (5) 257-273.

[12] https://www.techtarget.com. What is Cybercrime. Accessed 10 July 2024.

[13] S. C. McQuade, *Understanding and Managing Cybercrime* (New York: Allyn and Bacon, 2006) 2.

which can be conducted through global electronic networks[6]. This definition is quite flawed in the sense that cybercrimes are not always conducted through global electronic networks. Cybercrimes, like hacking, do not require global electronic networks for them to be perpetrated[15].

There have been arguments by scholars that cybercrimes can either be defined in either narrow or broad terms. During the 10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders, two definitions in terms of narrow and broad sense were developed. Cybercrime in its narrow sense, was defined as any illegal behaviour directed by means of electronic operations that target the security of computer systems and the data processed by them[7]. While cybercrime in a broader sense (computer-related crimes) is any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network[8].

Whatever definition is given to cybercrime, one factor still remains that it is a crime committed through the use of a computer to carry out any illegal activity.

Classification Of Cybercrime: There are three main categories of cybercrime:

a) Property cybercrime

Here, the cybercriminal or hacker, illegally obtains a person's bank details in order to gain access to funds and make purchases online or transfer such funds to another bank account. They can even run phising scams to get people to give access to their personal information while pretending to be someone that those innocent victims know [9]. This is most common in Nigeria and the hackers use online chat platforms like Facebook, WhatsApp, X, Instagram e.t.c.

b) Individual Cybercrime

This category of cybercrime involves an individual distributing malicious or illegal information online. It includes cyber stalking, pornography distribution and trafficking[10].

c) Government Cybercrime

---

[14] Loader B, Douglas T., *Cybercrime: Security and Surveillance in the Information Age* (Routledge Press, 2020). [15] Babafemi T., *An Appraisal of the Legal Framework of Cybercrime in Nigeria* (Being a published LL.B Project, Faculty of Law AfeBabalola University Ekiti,2015) 39.

[15] Ibid.

[16] Ibid.

[17] https://www.pandasecurity.com. Types of cybercrime. Accessed 12 July, 2024.

[18] Ibid.

This form of cybercrime, is not as rampant as the two listed above but it has the most devastating effect on the economy of any government. Thus, a crime against the government is known as cyberterrorism. This involves hacking government websites or military websites, getting access to government sensitive information and distributing same to enemy nations[11].

Other categories of cyber related crimes include:

i. Cyberstalking

This involves online harassment where the victim is subjected to a barrage of online messages or emails. Cyberstalkers use social media platforms, search engines and websites to instill fear in their victims and thus making them feel afraid for their lives and their safety. This has played out a lot of times in Nigeria. One prominent figure that was cyberstalked and bullied is Alex Iwobi, a Nigerian international football star, who was harassed online after Nigeria lost the final match in the AFCON 2023 against Ivory Coast[12]. He was bullied to the point he had to lock his social media pages and take down all his pictures. It took the intervention of his colleagues and some prominent members of the Nigerian government for the cyberbullies to leave him alone. Another instance of cyberbullying, is the case of Nigerian Actress, Toyin Abraham

Ajeyemi, who arrested an X user who goes by the name #YVRLO for making harsh comments about her and also threatening to harm her family, including her son. She was bullied for her support towards the government of President Bola Ahmed Tinubu. She faced a backlash of vitriol for daring to arrest the cyberbully and people even made moves to report her movies to the online streaming platform NETFLIX for her movies to be taken down. She was forced to secure the release of the cyberbully because of the insults targeted at her [13].

ii. **Phising**

This involves hackers sending malicious email attachment or URLS to internet users to gain access to their computers. These criminals have mastered the art of phising that most of these emails are not flagged as spam and users are tricked into changing their passwords or updating their billing information thereby, unknowingly giving access to these criminals. A lot of Nigerians have fallen victim to this scam and have had their monies wiped out of their account. The case of Nigerian actress, Shan George, comes to mind. She disclosed on the internet that some fraudulent persons pretending to be officials of Zenith Bank, sent a link to her to rectify issues she had with her bank account. After filling in her personal details, she was locked out of her bank app by these criminals and had the

---

[11] Ibid.

[12] Httpss://www.aljazeera.com. Nigerian Star Iwobi faces cyberbullying after AFCON loss to Ivory Coast. Accessed 10 July 2024.

[13] Adekunle Sulaimon, ' Toyin Abraham faces Backlash for action against trolls who cursed her over Tinubu'ssuport' *Punch Newspaper* (Lagos, 10 July 2024). https://www.punchng.com

sum of 3.6 million naira, transferred from her account[14]. It took the help of her bank and the efforts of spirited Nigerians before she could recover the money.

iii. Prohibited/ Illegal Content

This category of cybercrime involves criminals sharing and distributing inappropriate content that can be considered highly disturbing and offensive. The contents distributed include but are not limited to sexual activities between adults, videos with intense violence and videos of criminal activities, materials advocating terrorism related acts and child exploitation [15].

iv. Online Scams

These are usually in the form of ads or spam emails that come with promises of rewards or unrealistic amounts of money. These scams include offers that seem too good to be true and when clicked on, can cause malware to interfere and compromise the user's information[16].

v. Cyber Squatting

This refers to the unauthorized registration and use of internet domain names that are identical or similar to trademarks, service marks, personal or company names[17]. It occurs when an individual or a corporation registers a domain name that is spelled the same as a preexisting trademark, and demands money from the trademark owner before the registrant will release the domain name. Cyber squatters obtain and use the domain name in bad faith with intent to profit from the goodwill of the original trademark owner.

Emerging Cyber Tricks In Nigeria

The following are the main emerging cyber tricks in this 21st century, used by cybercriminals to lure and ultimately defraud unsuspecting computer users.

---

[14] KhadijatLawal, ' Actress, Shan George retrieves N3.6 m stolen from her account' https://www.channelstv.com. Accessed 12 July 2024.

[15] Yasin M, 'Global Nature of Computer Crimes and the Convention on Cybercrime'*Ankara Law Review* (2016) (3) (2) 135.

[16] https://www.techopedia.com. What is cybercrime? Accessed 12 July, 2024.

[17] https://www.winston.com. What is the definition of cyber squatting? Accessed 12 July 2024.

"Breaking News" Videos/Articles: This nefarious tactics involve the use of catchy headlines that tackle hot global news and current events will always be viable bait for cybercriminals to use against unknowing users. This social engineering technique can easily trick users to click the malicious link and even share it with their friends on social media.[18]

Government Notices And Summons

This nefarious tactics is similar to "breaking News" scam. Here, the cyber criminal, uses fake notices from the government to alarm users and trick them into opening a malicious email.[19]

Facebook Chat Termination: This spammed notification asks verify their account or else their chat account will be terminated. When the user follows the attacker's instructions, the attacker will end up with access to the user's account.

Banking Related Schemes: This scam tactics, include calls or emails to inform users about banking-related updates or notifications like card suspension and suspicious transactions. The scare tactic then leads to fake banking pages that are designed to steal information. In some cases, users get a call from a fake customer service representative who tries to fish banking details from the victim.

Virus Scare: Cybercriminals play on the fear of online users by using news items— such as the Ebola virus—as bait for phishing scams. The tactic then involves a link that supposedly goes to a guide on safety measures, but is actually a lure for users to click on malicious links, which can lead to the user's account being hacked or important data stolen.

Online Charity: Another dubious method used by internet fraudsters to defraud unsuspecting online users, involves the use of websites of charity organizations soliciting monetary donations and materials to these organizations that do not actually exist. Unfortunately, many unsuspecting people, have been exploited through this means.[20]

Lottery Scam: This scheme involves the use of online platforms to announce winning tickets in Lottery which people never entered.

---

[18] '10 Scary Tricks cybercriminals use to Lure Unsuspecting Users', https://www.trendmicro.com, accessed 15th July 2024.

[19] I bid

[20] Yakubu Ajiji Makeri, 'Cyber Security in Nigeria and Challenges', *International journal of Advanced Researched in Computer science and Software Engineering* (2017) (7)(4) https://www.
Kiu.ac.ug>assets>publications>accessed 15th July 2024

These scams lately, include the State Department of the United States green card lottery.[21]

Will Scam: This involves the use of various online platforms such as instagram, X (formerly known as twitter), Facebook, LinkedIn, snapchat, TikToK, email, etc to dubiously inform an innocent online user or estranged relative that the person stands to inherit an estate worth millions.

Examination Of Prior Legal Regime

The Cybercrimes (Prohibition, Prevention, etc) (Amendment) Act, 2024 ("the Cybercrimes (Amendment) Act") is the current legal framework regulating electronic transactions, and combating cybercrimes in Nigeria. This current piece of legislation amended the Cybercrimes (Prohibition, Prevention, etc) Act, 2015.

However, before the enactment of the Act, computer generatedevidence was not recognized in Nigeria's evidential law. The reason being that it was not clear whether computer generated evidence should be treated as primary or secondary evidence under the old Evidence Act (i.e prior to the enactment of the Evidence Act 2011), and the current Evidence (Amendment) Act 2023. Under the Old Evidence Act, the procedure for roving or authenticating the sealing of a document required actual writing on a tangible medium by the person alleged to have executed such document, so as to examine his signature or finger impression.[22] This legislation, did not contemplate the current use of electronic signature in email transactions, cryptographic codes on internet platforms and biometric system in financial institutions, such as the current use of Bank Verification Number in the banking system.[23]

However, the coming into force of the New Evidence Act 2011 and the Evidence (Amendment) Act, 2023 resulted in great improvements on the Old Evidence Act. Sections 84 and 93 of the New Evidence Act, provide for the admissibility of computer generated documents[24] , the recognition of electronic signature and waiver of its proof by means of writing on a tangible medium. These substantial improvements were a major boost to electronic transactions before the enactment of the Cybercrimes Act, 2015, and the current Cybercrimes Amendment Act, 2024.

---

[21] Ibid

[22] See sections 100, 102 and 108 of the Old Evidence Act.

[23] Okoro Jude Okwoma, 'Cybercrime and E-Crime in Nigeria: A Review of Legal Framework' *Journal of Public& Constitutional Practice* (2017) (10)192.

[24] See sections 84 and 93 of the Evidence Act 2011

Despite these significant improvements on the evidential value on electronic generated documents, many cybercrimes which undermine the integrity of parties to online transactions still went unchecked. This was due to the following factors:

i) The fact that fraudulent activities such as hacking, black mailing scam, identity theft, website cloning, PIN theft, cyber squatting, cyber attack, scamming , phishing, etc were not clearly defined by the New Evidence Act, thereby becoming unknown to the Nigerian legal system. It is a notorious fact that for any action to constitute a crime in Nigeria, it must be clearly defined in a written legislation.[25]

ii) The fact that there was no designated or specialized court or institution with competent jurisdiction to prosecute matters relating to cybercrimes in Nigeria aside the Economic and Financial Crimes Commission (EFCC) and the Nigeria Police Force who are train to generally handle conventional criminal matters.[31]

Evaluation Of Current Legal Framework For Combating Cybercrimes In Nigeria

The current legal framework for combating cybercrimes in Nigeria is the Cybercrimes (Amendment Act) Act 2024. This important piece of legislation was signed into law by President Bola Ahmed Tinubu sometime in February, 2024.

The Cybercrimes (Amendment) Act has thirteen (13) sections, amending 11 sections of the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015. According to the Explanatory cemorandum of the Cybercrimes (Amendment) Act, it aims to insert some consequential words that were inadvertently omitted in the Cybercrimes Act.

However, a critical look at the Cybercrimes (Amendment) Act reveals that it does more than inserting omitted words; it introduces some new provisions that are significant to Nigeria's cyber security landscape. We shall therefore examine the key amendments made by the Cybercrimes (Amendment) Act.

Introduction of Certified True Copies of Valid Electronic Signature

[25] See section 36(12), Constitution of the Federal Republic of Nigeria 1999 (as amended).

[31] Ekwoma (see n 32 above)

Section 2(b) of the Cybercrimes (Amendment) Act [26]amends Section 17(2) of the Cybercrimes Act [27]to provide an exception to transactions that would be excluded from the categories of contractual transactions or declarations that are valid by virtue of electronic signature, with the exception being "where they are legally verified in Certified True Copies".

Similarly, Section 2(a) of the Cybercrimes (Amendment) Act[28] amends Section 17(1)(b) of the Cybercrimes Act [29]by substituting the word "geniuses" with the word "genuineness".

Consequently, with this amendment, Section 17(1)(b) of the Principal Act[30] now reads as follows "where the genuineness or otherwise of such signatures is in question, the burden of proof, that the signature does not belong to the purported originator of such electronic signatures, shall be on the contender".

Establishment of Sectoral National Computer Emergency Response Team (CERTs)

Section 3 of the Cybercrimes (Amendment) Act[31] amends Section 21(1) of the Cybercrimes Act[32] by establishing the Sectoral National Computer Emergency Response Team (CERTs) and Sectoral Security Operations Centers (SOC) which shall be under the administration and control of CERT Coordination Center.

CERT Coordination Center is a centre where any person or institution, who operates a computer system or a network, whether public or private can report any attacks, intrusions and other disruptions liable to hinder the functioning of another computer system or network, so that necessary measures may be taken by the Centre to tackle the issue. By this amendment, there is hopefully going to be more efficiency in managing reports of cyber threats by the Centre.[33]

Resolving the issues of Section 24 of the Cybercrimes Act Section 24(1) of the Cybercrimes Act[34] criminalizes sending a message via a computer system which is hgrossly

---

[26] See section 2(b) of the Cybercrimes(Amendment) Act.

[27] See section 17(2) of the Cybercrimes Act.

[28] See section 2(a) of the Cybercrimes (Amendment) Act

[29] See section 17(1)(b) of the Cybercrimes Act

[30] Ibid

[31] See section 3 of the Cybercrimes (Amendment Act).

[32] See section 21(1) of the Cybercrimes Act.

[33] FOLEGAL, 'A Review of the Cybercrimes Amendment Act, 2024.' LinkedIn, accessed 30th July 2024.

[34] See section 24 of the Cybercrimes Act.

offensive, pornographic, or of an indecent, obscene, or menacing character', or to send a message knowing it to be false for the purpose of "causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will, or needless anxiety to another", or to cause such a message to be sent.

The words used in this provision are quite vague, nebulous and ambiguous. In fact, the civil society organizations are of the opinion that this provision was used by state authorities to prosecute journalists, bloggers and media practitioners.[35]

Thankfully, Section 5 of the Cybercrimes (Amendment) Act[36] has deleted the vague, nebulous and ambiguous words used in Section 24(1) of the Principal Act and amended the provision with clarity and certainty. Now, Section 24 of the Cybercrimes Act[37] simply criminalizes messages that are hpornographic' or sent by a person knowing them to be false, for the breakdown of law and order, posing a threat to life, or causing such a message to be sent.

National Identification Number (NIN) as requirement for Electronic Financial Transactions.

Section 8 of the Cybercrimes (Amendment) Act[38] amends Section 37 (1) of the Cybercrimes Act.[39] By this amendment, financial institutions shall verify the identity of their customers by requiring them to present their 'National Identification Number issued by the National Identity canagement Commission and other valid' documents bearing their names, addresses, and other relevant information before issuance of ATc cards, credit cards, debit cards, and other related electronic devices.[49]

Recognition of Nigeria Data Protection Act

---

[35] FOLEGAL(note 43)

[36] See section 5 of the Cybercrimes (Amendment) Act.

[37] See section 24 of the Cybercrimes Act.

[38] See section 8 of the Cybercrimes(Amendment) Act [49] See section 37(1) of the Cybercrimes Act.

[39] FOLEGAL(note 43).

Section 9 of the Cybercrimes (Amendment) Act [40]amends Section 38(1) of the Cybercrimes Act [41] by providing that a service provider must keep and protect specific traffic data and subscriber information in accordance with the provisions of the Nigeria Data Protection Act, which the principal act had only prescribed as "relevant authority".

Cyber Security Levy and Punishment for defaulting

Section 11(a) of the Cybercrimes (Amendment) Act [42] amends Section 44(2)(a) of the Cybercrimes Act[43] to provide a levy of 0.5% (0.005), equivalent to half a percent of all electronic transaction values by the businesses specified in the second schedule of the Act, which include GSc service providers and all telecommunication companies; Internet service providers; banks and other financial institutions; insurance companies; and the Nigerian Stock Exchange. Under the old provision, it required "a levy of 0.005 of all electronic transaction by the businesses specified in the second schedule of this Act"[44]

However, as it stands, President Tinubu had directed the Central bank of Nigeria to suspend the Cyber Security Levy implementation to ease economic hardship in Nigeria.

Section 11(b) of the Cybercrimes (Amendment) Act[45]further provides for the punishment for defaulting to pay the levy which is "on conviction, to a fine of not less than 2% of the annual turnover of the defaulting business" and failure to comply with payment of fine shall lead to closure or withdrawal of the business operational license.

Removal of Section 48(4) of the Cybercrimes Act

Section 12 of the Cybercrimes (Amendment) Act[46]deletes Section 48(4) of the Cybercrimes Act[47], which provides that any person convicted of an offence under this Act shall have their international passport cancelled, and in the case of a foreigner, their passport shall be withheld and only returned to them after they have served the sentence or paid the fines imposed on them.

---

[40] See section 9 of the Cybercrimes (Amendment) Act.

[41] See section 38(1) of the Cybercrimes Act.

[42] See section 11(a) of the Cybercrimes(Amendment) Act.

[43] See section 44(2)(a) of the Cybercrimes Act.

[44] Ibid.

[45] See section 11(b) of the Cybercrimes (Amendment) Act.

[46] See section 12 of the Cybercrimes(Amendment) Act.

[47] See section 48(4) of the Cybercrimes Act.

In the case of the Cybercrimes (Prohibition, Prevention, etc) Act 2015, the Act is divided into Eight (8) different parts. Part 1 spells out the objectives and applications of the Act; Part II deals with protection of critical National Information Infrastructure; Part III centers on offences and penalties; Part IV contains Duties of Financial Institutions; Part V relates to Administration and Enforcement; Part VI deals with Arrest, Search, Seizure and Prosecution; Part VII captures issues relating to Jurisdiction and International Cooperation and Part VIII deals with miscellaneous matters.[48] Part I which relates to objectives and application declares the objectives of the Act as follows: To provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria [49] ; To ensure the protection of critical national information infrastructure[50]; and to promote cyber security and the protection of computer, systems and networks, electronic communications, data and computer program, intellectual property and privacy rights.[51]

From the general reading of the Act, it is clear that the Act fails to provide the definition of the term "cybercrime", which incidentally is the subject matter of the legislation itself.[52] This, it is submitted, is not unconnected with the inconsistencies in the cybercrime vocabulary engendered by the lack of a unanimous perception that would sufficiently represent cybercrime as an umbrella term for the technology induced types of offences. For instance, Wall defines cybercrime thus:

> Cybercrimes are criminal or harmful activities that are informational, global and networked and are to be distinguished" from crimes that involve simple use computers. They are the product of networked technologies that have transformed the division of criminal labour to provide entirely new opportunities and new forms of crime which typically involve the acquisition or manipulation of information and its values across global networks for gain. They can be broken down into crimes that are related to the integrity of the system, crimes in which networked computers are used to assist in perpetration of crime, and crimes which relate to the content of computers.[53]

---

[48] Abayome B Sogunle, 'Cybercrimes (Prohibition, Prevention etc) Act 2015: Challenges and Enforcement', *Journal of Law and Judicial System* (21) (4) (1) 2.

[49] Ibid

[50] Ibid

[51] Ibid

[52] Ibid

[53] D. Wall, 'Cybercrime: The Transformation of Crime in the Information Age' https://sryawahpublications.com> accessed 15th July 2024.

As broad as this definition is, the difficulty with the definition is that it would not cover traditional crimes such as murder and some other offences. [54]For example, an offender, using a keyboard to hit and kill a victim, is not covered here. Those cases where physical hardware is used to commit regular crimes are excluded.[55] However, the Stanford Draft International Convention to Enhance Protection from Cybercrime and Terrorism defines cybercrime to mean "conduct, with respect to cyber systems that is classified as an offence punishable by the Act"[56]This definition, no doubt, would include cases where physical hardware is used to commit regular crime. Considering the fact that there is no simple definition of cybercrime, the draftsmen of the Act, adopted the approach found in the Convention on Cybercrime which distinguishes four different types of offences namely: offences against the confidentiality, integrity and availability of computer data and system; computer related offences; content related offences and copyright related offences (this last one is not captured in the Act).[57] Suffice it to say however that this typology is not wholly consistent as it is not based on a sole criterion to differentiate between categories.[58] Thus, first three categories focus on the object of legal protection, offences against confidentiality, integrity and availability of computer data and systems, content related-offences and copyright related offences.[59]

Offenses Against Confidentiality, Integrity And Availability Of Computer Systems

Reliance on digital technology, particularly networked communication, is now so pervasive that it is regarded as part of the critical infrastructure. The volume of sensitive government and commercial information stored and transmitted electronically, raises the potential for espionage.[60] Under the Act[61] , offences included in this category, are unlawful access to a computer.[73] Unlawful interceptions [62] and system interference. [63] Of course, given the ubiquitous presence of computers in modern life and the dependency of modern commerce on computer networks, such offences have potentially serious consequences. Unlawful access to

---

[54] Chang E, Chung W, Chan H., Chou S., 'An International Perspective on Fighting Cybercrime' https://sryawahpublications.com> accessed 15th July 2024.

[55] Ibid

[56] Article 1: 1 Draft International Convention to Enhance Protection from Cybercrime and Terrorism, 1999, available at http://media accessed 16th July 2024.

[57] Sogunle(n 36)3

[58] Ibid

[59] Ibid

[60] Jonathan Clough, "Cybercrime", *Commonwealth Law Bulletin* (2011) https://sryawahpublications.com> accessed 17th July 2024.

[61] Cybercrimes (Prohibitio]n, Prevention, etc) Act, 2015. [73] Section 6 of the Act.

[62] Section 12 of the Act

[63] Section 8 of the Act

a computer is analogous to illegal access to a building and is recognized as a criminal offence under the Act.[64]

Illegal access to computer systems hinders computers operators in managing, operating and controlling their systems in an undisturbed and uninhibited manner. The aim of course is the maintenance of the integrity of computer systems. However, the question that may arise here has to do with whether unlawful access is the end goal here or the unlawful access envisaged by the provisions of section 6, extends to further crimes committed after the initial access such as modifying or obtaining stored data (where law seeks to protect integrity and confidentiality of the data).[77]In other words, does the Act criminalize the act of illegal access in addition to subsequent offences?

The above question is relevant because, enacted provisions sometimes confuse illegal access with subsequent offences. However, it is submitted here that a conjunctive reading of the provisions of section 6 of the Act, shows that the provisions criminalize both illegal access and subsequent offence.[78] Section 6 (i) talks about the issue of access "in whole or in part". Furthermore, section 6 (2) goes on to provide a stiffer penalty where the illegal access indicated in subsection 1 is committed with the intent of obtaining computer data etc.[79]Also, the section requires that the act of unlawful access must have been committed with the requisite intention. [80]

It has been submitted that another element of the offence created by section 6 of the Act is that the "access to a computer" can only be committed if it takes place without authorization.[65] In the light of this, it is submitted that the section explicitly aims to incorporate the notion of self-defence. However, the provisions of section 6 can run into difficulties where a computer system was not accessed unlawfully, but the user continues to use the system after permission had expired.[66] It is therefore, suggested that a provision similar to section 5 of the "Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedure Cybercrime Legislative text" be included in the Act to clear doubts in this regard.

Section 5 of the Enhancing Competitiveness in the Caribbean ICT Policies, Legislation Regulation Procedure provides: Illegal Remaining A person who intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, remains logged in a computer system or part of a computer system or continues to use a computer system commits

---

[64] Section 6 (i) provides in part: "Any person, who, without authorization, intentionally accesses, in whole or in part, a computer system or network for fraudulent purpose and

[65] Ibid

obtain data that are vital to national security, commits an offence….." Section 6 (2) says: "where the offence provided in subsection (1) of this section is committed with the intent of obtaining computer data, securing access to any program commercial or industrial secrets or classified information……

[66] Ibid

an offence punishable in conviction, by imprisonment for a period of not exceeding (period), or a fine not exceeding (amount) or both. [67]

Unlawful Interception

The provision of section 12[84] of the Act, underscores the importance of computer data to private users, businesses and administrators. Lack of data, can cause considerable damage in terms of finance to users. A careful reading of the section shows that its applicability is limited to the interception of data by technical means. Also, the section talks about interception of "nonpublic transmissions". First, it must be realized the "transmission" covers all data transfers, whether by telephone, fax, e-mail or file transfer.

A transmission is "non-public" if the transmission process is confidential. According to Gercke, the "vital element to differentiate between public and non-public transmission is not the nature of the data transmitted but the nature of the transmission process. Even the transfer of publicly available information, can be considered criminal, if the parties involved in the transfer intend to keep the content of their communication secrete."[85]

System Interference

The Act also criminalizes the intentional hindering of lawful use of computer system.[86]No doubt, the application of this section is limited to cases where hindering is "serious" and is carried out by one of the acts mentioned thereunder. Also the offender must be carrying out the offences "intentionally" or for fraudulent purposes and the act must have been done without lawful authority. Also criminalized are acts that render computer data inaccessible. However, the requirements that the particular section can be invoked only where the hindering is a serious one is likely to cause confusion as legal arguments here may center on the criteria to be fulfilled for determining whether the hindering of the functioning of the computer system is serious or not. It is submitted that, to obviate unnecessary arguments here, a provision similar to section

---

[67] Section 12 (i) of the Act "Any person who intentionally and without authorization, intercepts by technical means, non-public transmissions of computer data, content, or traffic data, including electromagnetic emissions or signals from a computer, computer system or network carrying or emitting signals, to or from a computer, computer system or connected system or network; commits an offence and shall be liable on conviction to imprisonment for a term of not more than 2 years or to a five of not more that N5,000,000:00 or to both such fine and imprisonment. Cf with Article 3 of the European Convention on Cybercrime, 2000, which provides: "Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmission of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be

7 of the 1999 Stanford Draft International Convention be adopted to replace section 8 of the Act. The section in question provides[87]:

> (1) A person who intentionally or recklessly without lawful excuse or justification: (a) hinders or interferes with the functions of a computer system; or (b) hinders or interferes with a person who is lawfully using or operating a computer system; commits an offence punishable, on conviction for a period not exceeding (period), or a fine not exceeding (amount) or both in subsection (i) "hinder," in relation to a computer system, includes but is not limit to:
>
> (a) cutting the electricity supply to a computer system, and
>
> (b) causing electromagnetic interference to a computer system by any means; and
>
> (c) corrupting a computer system by any means; and
>
> (d) inputting deleting or altering computer data"
>
> The incorporation of the definition of the word "hinder" in the above section in our section 8 is necessary to widen the list of the acts by which the functioning of a computer system may be affected adversely.

---

committed with dishonest intent, or in relation to a computer system that is connected to another computer system,

http://conventions.co.int accessed 18th July , 2024.

[68] See section 12 of the

Act [85] Gercke(n 54)

[69] Section 8 of the Act provides "Any person who, without lawful authority, intentionally or for fraudulent purposes does an act which causes directly or indirectly the serious hindering of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating; altering or suppressing computer data or any other form of interference with the computer system, which prevents the computer system or any part thereof, from functioning in accordance with its intended purpose, commits an offence and shall be liable on conviction to imprisonment for a term of not more than 2 years or to a fine of not more than N5,000,000.00 to both fine and imprisonment. Contrast with Art 5. Of the European Convention on Cybercrime, 2000 and section 7 of the 2002 Commonwealth codel Law, available at www.thecommonwealth.org/shared asp files/uploaded files/%7BDA109CD2-5204- 4FABAA77=86970A639805%7 Computer%20Crime.pdf (Annex1). The latter also criminalizes "reckless" acts accessed on July 20th , 2024.. 32 . Section 7 of the 1999 Stanford

Content Related Offenses

The content related offences captured under the Act, include child pornography and related offences[68], and racist and xenophobic Offences[69].

Child Pornography

Child pornography offences have a harmful repercussion in society and specifically for minor victims as a vulnerable sector in these matters.[70] No doubt, the provisions of section 23 are in line with international best practice as offences in this regard are universally recognized as criminal acts.[71] The offences here can only be committed with requisite intention. This section seeks to modernize child pornography laws and to attach consequences to the conduct of each participant in the chain creating offences of production, offering/making available, distributing/ transmitting, procuring and possessing.

However, the challenges here have to do with the fact that countries may differ on the appropriate age of consent, whether „simple" possession should be criminalized and whether the definition of child pornography should include „materials that visually depicts" as contained in our Section 23, or not Another problem associated with the

Racist And Xenophobic Offences

Going by the provision of section 26 of the Act, intentional distribution and making available of xenophobic material to the public through a computer system, is an offence. One of the 50

shortcomings of the Nigerian law is that it does not define what constitutes a "racist and xenophobic material".

---

[70] Section 23 of the Act. ." It provides in part: Any person who intentionally uses any computer system or networking in or for:- (a) Producing child pornography; (b) offering or making available child pornography (c) distributing or transmitting child pornography; (d) procuring child pornography for oneself or for another person. (e) possessing child pornography in a computer system or on a computer data storage medium: commits an offence under the Act and…."

Section 26 of the Act. It provides in part: "Any person who with intent – (a) distributes or otherwise makes available, any racist or xenophobic material to the public through a computer system or network; (b) threatens through a computer system or network – (i) persons for the reasons that they belong to a group distinguished by race, colour, descent, national or ethnic origin….."

Comprehensive Study on Cybercrime, United Nations Office on Drugs and Crime (UNDO), (February 2013) accessed 22nd July 2024.

[71] Ibid

However, it can be inferred from the wordings of section 26, that a racist and xenophobic material will include any material which advocates, promotes or incites hatred, discrimination or violence against persons for the reason that they belong to a group based on race, colour, descent, national or ethnic origin, as well as, religion, if used as a pretext for any of these factors; or a group of persons which is distinguished by any of these characteristics.

Also section 26 (i) (c), criminalizes insults made "publicly through a computer system or network to persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors" [72] This particular provision, obviously excludes insults made through private communication e.g. e-mail as that would not qualify as insult made publicly.

enforcement of section 23 is succinctly captured by Prof. carcon Gercke when he observes thus[73]:

> The legal challenges are complex, as information made available by one computer user in one country can be accessed from nearly anywhere in the world. If offenders create content that is illegal in some countries, but not in the country they are operating from, prosecution of the offenders is difficult or impossible. There is much lack of agreement regarding the content of material and to what degree specific acts should be criminalized.

---

[72] See Section 26(i)© of the Act.

carco Gercke, hUnderstanding Cybercrime: Phenomena, Challenges and Legal response', (2012), www.itu.int/ITUD/Cybersecurity/legislation/html.page accessed on 18th July 2024. [78] Sogunle(n 45)4

carco Gercke, hUnderstanding Cybercrime: Phenomena, Challenges and Legal response', (2012), www.itu.int/ITUD/Cybersecurity/legislation/html.page accessed on 18th July 2024. [78] Sogunle(n 45)4

Ibid

Ibid

Ibid

See section 7 of the 1999 Stanford Draft International Convention, https:// media,hoover.org/documents/0871999825 249.pdf.,accessed on 20th July, 2024.

Draft International Convention available at http:// media,hoover.org/documents/0871999825 249.pdf, accessed on 20th July 2024

[73] Gercke(n 54)

Similar to the above position is the vexed issue of how to enforce section 23 without interfering with the right to freedom of expression.
However, the Act fails to define what constitutes "insult." If the word "insults" is understood to refer to any offensive or invective expression which prejudices the dignity of a person and is directly connected with the insulted person's belonging to the group, then there is the need

for caution here to ensure that the sanctity of the principles of freedom of speech as guaranteed under the Constitution is not violated.[74] Obviously, in order to safeguard the principles of freedom of expression guaranteed under the constitution, there would be the need for the court to interpret the act of insult envisaged under section 26 of the Act narrowly.[75]

Computer Related Offences

Computer related offences, refer to a wide ranch of offences involving a computer and a network.[76] In other words, these are offences where the computer is used to facilitate the commission of an offence. Included in this category under the Cybercrime Act are Computer related forgery[87], computer related fraud[77] and identity theft and impersonation[78].

Computer Related Forgery[79]

Computer related forgery involves impersonation of legitimate individuals, authorities, agencies, and other entities online for fraudulent purposes.[80] From the clear reading of section 13 of the Act, computer related forgery seeks to protect data. Clearly, the provision does not only refer to computer data as the object of one of the acts mentioned, it is also necessary that the acts result in inauthentic data.[81]

---

[74] Sogunle(n 45)

[75] Ibid

[76] 'Computer Related offences and Crimes', https://www.jasperforgery.com. , accessed 20th July 2024. [87] See section 13 of the Act.

[77] See section 14 of the Act.

[78] See section 22 of the act.

[79] Section 13 of the Act provides "A person who knowingly accesses any computer or network and inputs, alters, delete, or suppresses any data resulting in inauthentic data with the intention that such inauthentic data will be considered or acted upon as if it were authentic or genuine, regardless of whether or not such data is directly readable or intelligible commits an offence and is liable on conviction to imprisonment for a term of not less than 3 years or to a fine of not less that N7,000,000 or both"

[80] 'Computer Related Offences', United Nations Office on Drugs and Crimes (UNODC), https://www.unodc.org>cybercrime>computer related-offences, accessed 22nd July 2o24.

[81] Sogunle(n 45)8

Computer Related Fraud[82]

Fraud is one of the most common forms of cybercrime. Computer fraud, can take many different forms, from phishing attacks, where a user is tricked into providing their personal information, to malware attacks, where malicious software is installed on the user's computer in order to gain access to sensitive information. It can also involve the unauthorized use of an individual's computer system or network for the purpose of stealing money or other assets.[104] Examples of computer related fraud include fraudulent online sales, advance fee schemes (otherwise known as 419), fraudulent investment opportunities and fraudulent electronic transfer of funds.

Section 40 of the Act, criminalizes an undue manipulation in the course of data processing with the intent to effect an illegal transfer of property.[94]However, for offences listed under section 14 (1) - (5) of the Act, the offender must have acted "intentionally".[83] The intent here has to do with the "manipulation" as well as the "financial loss."

Identity Theft And Impersonation

Identity theft and impersonation online can manifest in different forms, including: fake social media profiles, phishing emails, spoofed websites, scam ads, tech support scams, business email compromise, fake customer support accounts, celebrity impersonations, fabricated product or service reviews. [84] It refers to the criminal act of fraudulently obtaining and using another person's identity. The inclusion of section 22 in the Act is commendable in this regard.

---

[82] Section 14 of the Act. "Section 14 (1) Any person who knowingly and without authority or in excess of authority causes any loss of property to another by altering, erasing, inputting or suppressing any data held in any computer, whether or not for the purpose of conferring economic benefits on himself or another person, commits an offence and shall be liable on conviction to imprisonment for a term not less than 3 years, or to a fine of not less than N7,000,000.00 or to both fine and imprisonment." [104] 'Computer Fraud', https: //www.foundershield.com>Insurance Terms, accessed 22nd July 2024.

[94] See section 40 of the Act.

[83] See section 14 of the Act.

[84] What is Identity Theft and Online Impersonation? Understanding and Mitigating Cyber Threats, https://www.smartprotection.com>articles , accessed 23rd July 2024.

Jurisdiction[85]

The criminal jurisdiction of computer cybercrime is different from the traditional crime.[86] The typical one is "abstract cross border" behavior. Since the criminal acts involve many countries, it is difficult for this illegal computer cybercrime to point to a certain area of criminal jurisdiction. [87] This issue of abstract "cross border, has formed a great challenge to the traditional theory of criminal jurisdiction of computer cybercrime [88] .This explains the provisions of section 50 of the Act. Section 50 provides in part:

> 50 (1) The Federal High Court located in any part of Nigeria regardless of the location where the offence is committed shall have jurisdiction to dry offences under this Act, if committed -in Nigeria or in a ship or aircraft registered in Nigeria; or by a citizen or resident in Nigeria if the persons conduct would also constitute an offence under a law of the country where the offence was committed; or outside
> Nigeria, where -the victims of the offence is a citizen or resident in Nigeria; or the alleged offender is in Nigeria and not extradited to any other country for presentation…

A careful reading of section 50 [89]of the Act, clearly shows that there is no iota of doubt that section 50 (1) (a) (b) and (c) is a codification of the principle of territoriality[90]. The fact that jurisdiction in general only makes sense if it can be enforced, and enforcement of law requires control, explains the relevance of the principle in computer cybercrime matters.

It is submitted however, that the problem with section 50 (1) (a) - (c) has to do with a situation where neither the offender nor victim, is located within the country but only the infrastructure within a country was used for the commission of a crime. For example, if an e-mail with illegal content was sent out by using an e-mail provider in another country or a website with illegal content is stored on the server of a hosting provider to the country. To tackle a challenge such as this, it is suggested that a provision similar to the Singapore Act,[91]be included in the Nigerian legislation.

---

[85] See section 50 of the Act

[86] Sogunle (n 45)

[87] Ibid

[88] Ibid

[89] Article 22 of the European Convention on Computer Cybercrime, 2001 provides: Each party shall adopt such legislations and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Article 2 through 11 of this convention, when the offence is committed: (a) In its territory; or (b) On board a ship flying the flag of that party; or (c) On board an aircraft registered under the laws of that party; or (d) By one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any state.

[90] Sogunle(see note 45 above)9

[91] See Section 11 (3) (b) Singapore Computer Misuse Act, 2007

Challenges Of Cybercrime In Nigeria

The following are the major causes of cybercrimes in Nigeria: **Unemployment:** The rate of unemployment in Nigeria is alarming and growing by the day. Companies are folding up and financial institutions are going bankrupt. The government of Nigeria at all levels, and financial institutions have put unreasonable age barriers on who is eligible to apply for jobs. This has pushed the army of

unemployed Nigerians to go into cybercrimes and other conventional crimes for the purposes of survival.

Poverty Rate: The rate of poverty in Nigeria is alarming. In general, the incidences of monetary poverty are lower than the incidences of multidimensional poverty across most states in the country.[92] In Nigeria, 40.1% of people are poor according to the 2018/19 national monetary poverty line, and 63% are multidimensionally poor according to the National cPI 2022.[93] cultidimensional poverty is higher in rural areas, where 72% of people are poor, compared to 42% of people in urban areas.[94].

Two-thirds (67.5%) of children (0–17) are multidimensionally poor according to the National cPI, and half (51%) of all poor people are children. The highest deprivations are in the indicator of child engagements – where over half of poor children lack the intellectual stimulation that is pivotal to early childhood development.[107]On the global scale, Nigeria is regarded as a third world country. The poverty rate is ever increasing. The rich are getting richer and the poor are getting poorer. Insufficient basic amenities and an epileptic power supply, have grounded small scale industries.

Domestic And International Law Enforcement

One of the challenges of cybercrime is the fact that a hostile party using an Internet connected computer thousands of miles away can attack internet- connected computers in Nigeria as easily as if he were next door. It is often difficult to identify the perpetrator of such an attack,

---

[92] National Bureau of Statistics(NBS), 'Nigeria Launches its most Extensive National Measure of its MultiDimensional Poverty'(2022) https://www.nigerianstat.gov. nig, accessed 22nd July 2024.

[93] Ibid

[94] Ibid

and even when a perpetrator is identified, criminal prosecution across national boundaries is problematic.

Corruption: According to Transparency International, Nigeria is the 145 least corrupt nation out of 180 countries, according to the 2023 Corruption Perceptions Index.[95] Corruption Rank in Nigeria averaged 126.36 from 1996 until 2023, reaching an all time high of 154.00 in 2021 and a record low of 52.00 in 1997.[96]

Lack Of Standards And National Central Control: Emeruwa, a consultant to Nigeria Cyber Crime Working Group (NCCWG), said lack of regulations, standards and computer security and protection act are hampering true e-business in Nigeria.[97]

Lack Of Infrastructure: Nigeria as a country lacks a proper monitoring and arrest calls for sophisticated state of the art Information and Communication Technology devices.

Lack Of National Functional Data Bases: Lack of a functional National database could serve as a means of tracking down the perpetrators of cybercrimes by checking into past individual records and tracing their movements.

Proliferation Of Cyber Cafes: As a means of making ends meet, many entrepreneurs have taken to establishment of cybercafés that serve as blissful havens for the syndicates to practice their acts

through night browsing service, they provide to prospective customers without being guided or monitored.[111]

Porous Nature Of The Internet: The Internet is free for all with no central control, hence, the state of anarchy presently experienced.[98]

---

[95] Nigeria Corruption Rank, https://tradingeconomics.com>Nigeria, accessed 2nd August 2024.

[96] Ibid

[97] Ibid

111

[98] Ibid

Effects Of Cybercrime In Nigeria

Financial Loss: According to the Nigerian Communications Commission (NCC), Nigeria losses $500,000,000(Five Hundred cillion Dollars) annually to all forms of cybercrime including hacking, identity theft, cyber terrorism, harassment and internet fraud. [99] Perpetrators of cybercrime are like terrorists or metal thieves in that their activities impose disproportionate costs on society and individuals.

Loss Of Reputation: Cybercriminals have damaged the reputation of Nigeria in the eyes of the global community by defrauding individuals, companies, financial institutions of their financial resources and valuable data. It is submitted that most companies that have been defrauded or reported, to have been faced with cybercriminal activities complaint of clients losing faith in them.

Reduced Productivity: This is due to awareness and more concentration and attention being focused on preventing cybercrime and not productivity.

Solutions To Cybercrime In Nigeria

Education: Cybercrime in Nigeria, is difficult to prove as it lacks the traditional paper audit trail, which requires the knowledge of specialists in computer technology and internet protocols; hence Nigeria need to educate citizens that if they are going to use the internet, they need to continually maintain and update the security on their system. There is also need to educate corporations and organizations in the best practice for effective security management.[114] For example, some large organizations now, have a policy that all systems in their purview must meet strict security guidelines. [115]

Employment Opportunities: The government should consider it a duty to create job opportunities for the army of unemployed youths in Nigeria, considering the fact that out of 10 Nigerian students, (majority of which are youths), engage in internet fraud. [100] The job opportunities may include office jobs, IT Laboratories/ Forums and vocational training. Government should also bring out policies that encourage the private sector to collaborate and thrive with them. The private sector, through their private entities should complement

---

[99] Tope Omogbolagun, Senate Laments Nigeria's loss of $500m to cybercrime, *Punch* (Lagos, 22nd November 2023) https://punchng.com>senate-laments-nigerias-loss-of accessed 23rd July 2024. [114] Makeri(see note 29 above) 320

[115]

[100] Taiwo Okanlawon, 7 out of 10 Nigerian Students engage in internet fraud-EFCC, *Punch*(Lagos, 6th December 2023) https://punchng.com>senate-laments-nigerias-loss-of accessed 23rd July 2024.

government's efforts by providing job opportunities for the Nigerian youths. This will go a long way in reducing the unemployment and cybercrime rate in the country.

Provision Of Internet Protocol (IP) Address Tracking Software: Government and Private organizations should provide Software that could track the IP address of orders could be designed. This software could then be used to check that the IP address of an order is from the same country included in the billing and shipping addresses in the orders.

Provision Of Antivirus And Anti-Spyware Software: Antivirus software, consists of computer programmes that attempt to identify, thwart and eliminate computer viruses and other malicious software. Anti-spy wares are used to restrict backdoor program, Trojans and other spy wares to be installed on the computer.[101]

Cryptography: Cryptography is the science of encrypting and decrypting information. Encryption is like sending a postal mail to another party with a lock code on the envelope which is known only to the sender and the recipient.[102]A number of cryptographic methods have been developed and some of them are still not cracked.

Conclusion And Recommendations

As the global community continues to embrace and make use of the internet/cyberspace, the tendency is that there will be increase in cybercrime, particularly as it relates to Nigeria. Currently, Nigeria is rated the 5th country in the world with high rate of cybercrime after Russia, Ukraine, China, and the United States of America[103], respectively. Consequently, Nigerian government must address the high rate of cybercrime in Nigeria by seriously implementing the novel provisions Cybercrimes Act (Prohibition, Prevention, etc) (Amendment) Act 2024, the Cybercrimes (Prohibition, Prevention, etc) Act, 2015. This will go a long way in strengthening cyber security in Nigeria. The provision of job opportunities for the army of unemployed youths will keep them engaged and further discourage them from going into cybercrime, thereby showcasing Nigeria in good light in the eyes of global community. Furthermore, it is important that all hands (parents, teachers, community leaders, religious leaders, government,

---

[101] Makeri(n 29)

[102] Ibid

[103] Nigeria Ranks 5th in Global Cybercrime Index-Nairametrics, https://nairametrics.com>Sectors, accessed 25th July 2024.

through their various organs and agencies, e.t.c) must be on deck by working in synergy to aggressively tackle and ultimately stamp out the menace of cybercrimes in Nigeria.