LEGAL DESIGN AND IMPLEMENTATION OF CYBER CRIME MONITORING SYSTEM IN NIGERIA

Abstract
The paper examines the plans made to show the appearance or workings of cybercrime monitoring system under the Nigerian laws; to ascertaining the effective strategies for reducing cybercrimes among the youths and the society at large. The study is aimed at designing and implementing cybercrime monitoring system in Nigeria, the specific objective are to identify the factors responsible for cybercrime among the youths and the society find out the consequences of cybercrime in the Nigerian economy and to find how the economy is affected by high rate of cybercrime in Nigeria among others. The researcher adopted the doctrinal method in obtaining information. This entailed the collection of relevant materials on the topic and carrying out critical analysis and description of the data. Reliance was placed on both primary and secondary sources of obtaining data such as constitution, case law, law books, law journals, laws report, conference papers, treaties and conventions, etcetera. The study found Nigeria to be among top countries where cybercrime records are high. Another finding of this work is that internet technology in Nigeria has led to the modernization of fraud among the youth. Cyber fraud seems to have become accepted as a means of living for the Nigerian youth. We made necessary recommendation after our conclusion in urging the government to develop political will by making available technical facilities to Law Enforcement Agencies towards proper prosecution of Cybercriminals so that the country will be comfortable to the citizens, create awareness against cybercrimes and make the crime a strict liability offence.

Keywords: Legal design, implementation, cybercrime monitoring system and Nigeria.

1. Introduction

The world today is fast evolving into a global village. This is due to the dynamism of the internet and technology. Virtually every aspect of our human lives including economic growth, commerce, governance, communication, exchange of ideas, education, research and development, banking and financial transactions currently runs in the cyberspace. However, the activities of cyber-thieves or hackers are increasingly becoming more and more sophisticated everyday and their activities pose an enormous security threats to the internet and information abound in the cyberspace.[337]The abuse orchestrated by the users of these internet

***Livinus I. Nwokike**, OND, HND, PGD, MBA, FNIM. LLB (Hons), BL, LLM, PhD , Justice of Peace, Notary Public & Lecturer, Department of International Law and Jurisprudence, Faculty of Law, Nnamdi Azikiwe University, Awka, Anambra State, Nigeria, Email: *li.nwokike@unizik.edu.ng, tolerancefocus@gmail.com,* website: http://*www.geci.org.ng*. Phone Number: 08033521034, 09073018015

services and technologies (cyber) to underdevelop rather that develop the society including Nigeria to criminize these acts, hence, cybercrime. Cybercrime otherwise called computer crime is a crime involving the use of a computer, such as sabotaging or stealing electronically stored data[338]. In Nigeria, so many of them are not aware that the internet super high way has been invaded by criminals and deviants who luck around desperately looking for targets. Often times, the unguarded, naïve and causal internet user full prey to their antics. The problem of cybercrime victims is made worst by the seeming inability of law enforcement agents to effectively prosecute offenders. Clearly, law enforcement has not been able to keep up with technological advances to prevent cybercrime.[339]

The advent of the internet technology in Nigeria has led to the modernization of fraud among the youth. Cyber fraud seems to have become accepted as a means of living for the Nigerian youth. He argued that this is more so far those who are of college age.[340]Cyber crime has led to both prosecution and enforcement problems too. According to Johnson and Post, cyberspace radically undermines the relationship between legally significant (on line) phenomenon and physical location.[341] The practice of conducting operations via cyberspace has become irresistible and unstoppable. Because activities on the internet can have transboundary effect in every state in a nation and also every state on earth, there arises the issue of where exactly a person who has a cause of action based upon such activities may sue before a court or an agency can enforce a cybercrime case, it must be clothed with the necessary jurisdiction. Thus, a central and difficult legal issue in fighting cyber criminality is the problem of jurisdiction. This is particularly true as it is hard to territorially locate conduct in cyberspace because of the dispersed and amoeboid nature of the network that makes up the internet.[342]

---

[337]A Lucas, 'How prepared is Nigeria for Cyber-attacks'? The Nation Newspaper, 20 September, 2017

[338]B A Garner, Blacks Law Dictionary (Texas: 10th ed. Thomson Reuters, 2014)

[339]K Jaishakar, 'Establishing a theory of cybercrime (Editorial)', International Journal of Cyber Criminology 1(2) 2007 *http://wwwcybercrimejournal.com* accessed 19th July, 2019

[340]A Adeniran, 'Café culture and heresy of yahooboyism in Nigeria in Jaishankar (ed), Cyber criminology: Exploring internet crimes and criminal behaviour. Boca Raton, *FL* (*USA*: *CRC* Press), pp 3-12

[341]R J David and D David, 'Law and Borders – The Rise of Law in Cyberspace (1996) 48 Standard Law Review 1367, 1370

[342]Ikenga K E Oraegbunam, 'Jurisdictional challenges in fighting cybercrimes: Any panacea from international Law?', *Nnamdi Azikiwe University Journal of International Law and Jurisprudence* Vol 6, 2015 p. 57

2. Clarification of Terms

In Nigeria, some of the common cybercrimes in Nigeria include 419 – frauds, Romance scam, phishing or spoofing, hacking, denial of service, cyber terrorism, cyber-smearing/bullying and online visa application fraud.

Cybercrime is described as any criminal activity which involves the computer or the internet network.[343]

Cybercrime is also defined as a computer crime, which involves the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities or violating piracy.[344] Cybercrime is the use of a computer or other electronic device to perpetrate criminal acts. Cyber cafes have to register with the EFCC so that the Commission can monitor their operations and enforce operating standards that eliminate internet crimes.[345]

Crime can be defined as a illegal act for which someone can be punished by the government especially; a gross violation of law. It is also defined as an act that the law makes punishable - the breach of a legal duty treated as the subject matter or a criminal proceeding.[346]

Strict liability crime is defined as an offence for which the action alone is enough to warrant a conviction with no need to prove a mental state; a crime that does not require a mens rea element, such as traffic offences and illegal sale of introxicating liquor.[347]

Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offence (child pornography, late crimes)[348] Network is defined as a complicated system of roads, lines, tubes, nerves, etc that cross each other and are convicted to each other. It is a number of computers and other devices that are connected together so that equipment and other devices that are connected together so that equipment and information can be shared.[349] Internet is an international computer network connecting other networks and computers from companies, universities etc.[350]Hacking on the other hand is defined as the action of secretly finding a way

---

[343]Op.cit

[344]A D Michael, 'Defining cybercrime, accessed *http://www.britannica.com/cybercrime* accessed 19th July, 2019

[345] L I Nwokike, 'Security Education for Junior Secondary Schools (with workbook) JSS 1, (Awka: Arise and Shine Press, 2019) p 23

[346] *Op.cit,* 13

[347] B A Garner, Black's Law Dictionary, *Ibid*, 453

[348]Techopedia, 'What does cybercrime mean?"
http://www.techopedia.com/definition/2387/cybercrime accessed on 19th July, 2019

[349]A S Hornby, Oxford Advanced Learner's Dictionary of Current English (United Kingdom: 9th edn. Oxford University Press, 2015) 1039

[350]Ibid at 823

of looking at and/or changing information on somebody else's computer system without permission: The government tax website is vulnerable to hacking, putting taxpayer's information at risk,[351] Hacker, therefore, is a person who secretly finds a way of looking at and/or changing information on somebody else's computer system without permission.[352]

3. Types of Cybercrime

Fraud

Computer fraud are conducts which involve the manipulation of a computer, by whatever method, in order dishonestly to obtain money, property or some other advantage of value or to cause loss.[353] Fraud or fraudulent misrepresentation or misstatement involves an act where a false statement is made to a person upon whom that person relies on; and as a result or consequence of relying on that statement suffers some damages.[354] Fraud can take the form of abuse of position, or false representation, or prejudicing someone's rights for personal gain.[355] An estimated £139.6 million of card fraud took place over the internet in 2011; which is an increase of 3 per cent from 2010 when e-commerce fraud losses were £135.1 million, which now accounts for 63 per cent of card-not-present losses – slightly up from 59 per cent in 2010.[356] Article 8 of the Council of Europe's Convention on cybercrime enjoins member states to adopt such legislative and other measures as may be necessary to establish as criminal offences under their various domestic law, when committed intentionally and without right, the causing of a loss of property to another person by any input, alteration, deletion or suppression of computer data; and any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, and leading or resulting to economic benefit for oneself or for another person. The provisions of Article 8 aim to criminalise any undue manipulation in the course of data processing with the intention to affect an illegal transfer of property.[357]

---

[351]Ibid at 703

[352] Ibid at 703

[353] The Law Commission, Report No 186, Criminal Law-Computer Misuse, 1989, England, is available at: *http://www.official-documents.gov.uk/document/hc9495/hc00/0011/.pdf* accessed on 30 September 2019

[354] T A Oriola, 'Advance free fraud on the Internet: Nigeria's regulatory response' (2005) Computer Law & Security Report, Vol 21, Issue 3, 237

[355] D Bainbridge, 'Criminal law tackles computer fraud and misuse' (2007) Computer Law & Security Review, 23(3), 276-281

[356] The *UK* Card association Report is available at: <http://www.theukcardsassociation.org.uk/wm_documents/Fraud_The_Facts_2012.pdf > accessed on 7 April 2013

[357] Paragraph 86 (*Supra*)

These crimes consist mainly of input manipulations, where incorrect data is fed into the computer, or by programme manipulations and other interferences in the course of data processing.[358] A survey of about 160 companies revealed that electronic business fraud is twelve times higher than traditional fraud from retailer sales.[359] This involves deceptive behaviors conducted through the Internet in an illegal manner, with financial and personal benefits as its major motivations, and includes acts like credit card fraud, fraudulent Internet banking sites and advance fee fraud.[360] The offender must have committed the offence here intentionally, and with fraudulent or dishonest intent, without right, and with an economic benefit for himself/herself or for another person.

In the words of Lord Hardwicke in 1759, "…fraud is infinite, and was a court once to... define strictly the species of evidences of it; the jurisdiction would be cramped, and perpetually eluded by new schemes which the fertility of man's invention would contrive."[361] The general criminal offence of fraud can include the following elements: deception whereby someone knowingly makes false representation; or they fail to disclose information; or they abuse a position of authority. A civil claim for fraudulent misrepresentation can also lie in tort against a defendant under an action for deceit to provide a civil remedy for an individual who had relied on a false representation to their detriment.

In the UK, the law governing the 'traditional fraud' was governed by The Theft Act 1968. Section 15 of the Act provides as follows:

> A person who by any deception dishonestly obtains property belonging to another, with the intention of permanently depriving the other of it? For the purposes of this section 'deception' means any deception (whether deliberate or reckless) by words or conduct as to fact or as to law, including a deception as to the present intentions of the person using the deception or any other person.

---

[358] Paragraph 86 of the explanatory report

[359] Harry Tan, 'E-fraud: Current trends and international developments' (2002) Journal of Financial Crime 9.4

[360] Wingyan Chun, Hsinchun Chen, Weiping Chan, Schichich Chow, "Fighting Cybercrime: A Review and the Taiwan Experience", (2006) Decision Support Systems, 41, 669-682, pp. 670; See also Reich Pauline, 'Advance fee scams in-country and Across Border, (2004) Cybercrime & Security, *IF*-1, page 1, <http://www.acc.au/conferences/2004/index.html> accessed on 13 June 2015.

[361] The Law Commission Fraud (Report No. 276), of July 2002 is available at: <http://www.lawcom.gov.uk/lc_reports.htm#2002> accessed 9 June 2015

The case of *R v Sunderland*[362] illustrates the vulnerability of computer systems to criminal activities, and shows that the greatest threats of fraud comes from within an organization; and employees are responsible for a great deal of ICT fraud, or attempted ICT fraud ranging from small amounts of money to very large sums indeed.[363] Another problem faced by the Theft Act 1968 and the Theft Act 1978 in the UK was the position of offences against intangible property which has no physical existence. However, it has been held that confidential information does not constitute property for the purposes of the Theft Act. In *Oxford v Moss,*[364] the defendant, a student of engineering, took an exam paper with the intention of returning the paper having used the information gained in order to cheat in his exam. It was held that the information cannot be regarded as property and so cannot be stolen for the purposes of the Theft Act 1968. As stated by the Law Commission,[365]

> "…computer-enabled fraud is not new… it just takes 'real world' frauds and uses the Internet as a means of reaching the victim. These crimes consist mainly of input manipulations, where incorrect data is fed into the computer or by programme manipulations and other interferences with the course of data processing"[366].

The Fraud Act 2006, took effect in January 2007, and deals with some of the deficiencies, at least as far as information and communications technology fraud is concerned, of the Theft Act 1968 and the Theft Act 1978. It introduces a completely new general offence of fraud in section 1, and other offences which could be committed by false representation,[367] failure to disclose information[368] and by abuse of position.[369] Arguably, the key reason for the introduction of the Fraud Act was the history of complexity and uncertainty concerning offences

---

[362] (Unreported) 20 June, 1983. In *R v Sunderland*, an employee of Barclays Bank used bank's computer to find a dormant account, and then forged the holder's signature to withdraw £2,100. He was sentenced to 2 years imprisonment, which was later reversed on appeal to the Lord Chief Justice who suspended 18 months of the sentence taking into account the fact that the appellant's had previously been of good character

[363] David I. Bainbridge, Introduction to Information Technology law, (6th edn, Oxford University Press, 2007) 422

[364] (1979) 68 Cr App Rep 183

[365] Paragraph 8.42; Law Commission Consultation Paper No 155 is available at <http://www.lawcom.gov.uk/library/lib-crim.htm> accessed on 24 March 2013

[366] Paragraph 86 of the *COE* Convention explanatory report

[367] Section 2

[368] Section 3

[369] Section 4

involving deception, and the introduction of these general offences.[370] It has also been argued that this intended to provide a substantial scope to ensure that cyber-crime can be targeted by this provision.[371] This makes provisions for offences such as phishing and spoofing that were not provided for in of the Theft Act 1968 and the Theft Act 1978. The Police and Justice Act 2006 (the "PJA") was later introduced to make some amendments to the CMA.[372] According to Bainbridge, the prosecution has most often appeared to prefer more general legislation, like the Theft Act 1968, when dealing with issues of fraud involving computers; as such legislation is regarded as having "*inherent flexibility and freedom from the technicalities of the Computer Misuse Act*."[373]

On the other hand, Article 29(d) of the African Union Convention also urged member states to take necessary legislative and/or regulatory measures to make it a criminal offence to fraudulently procure, for oneself or for another person, any benefit by inputting, altering, deleting or suppressing computerized data or any other form of interference with the functioning of a computer system. This provision was also restated in Article 10 of the ECOWAS Directives on Cybercrime which show similarities to Articles 8 of the Budapest Convention and section 8 of the ITU Toolkit for Cybercrime Legislation. These regional provisions are ratified by section 14 of the Nigerian Cybercrime Act, which makes two different provisions on computer related fraud. The first provision in

---

[370] K M Rogers, 'The Internet and the Law' (Palgrave Macmillan, 2011) 240.

[371] M Johnson, K M Rogers, 'The Fraud Act 2006: The E-Crime Prosecutor's Champion or the Creator of a New Inchoate Offence?', (2007) International Review of Law, Computers & Technology, Volume 21, Number 3, 295-304; In *R. v Ekajeh* (2012) *EWCA* Crim 3125, the accused was part of three persons who were all Department of Work and Pensions employees who carried out a series of frauds in which a large number of false benefit claims were submitted using identities and sensitive personal data illegally accessed from departmental databases. The judge identified as aggravating features necessitating deterrent sentences the gross breach of trust involved over a prolonged period of time; that these were multiple frauds, targeting very large sums of public money intended for the neediest members of society; that the victims included the individuals whose identities had been stolen and whose right to privacy in sensitive data had been violated; and that it was a matter of public concern that personal data could be illegally accessed and misused in this way, undermining public confidence in the public bodies to which such data was entrusted. On appeal it was held that a total sentence of 10 years' imprisonment imposed for three counts of conspiracy to defraud was not excessive where the offender had breached the trust placed in him as a Department of Work and Pensions employee in carrying out a series of frauds involving a large number of false benefit claims utilizing identities and sensitive personal data illegally accessed from departmental databases.

[372] The Report of the Computer Misuse Act is available at: <www.cullen-international.com/cullen/multi/national/uk/.../cmareport.pdf> accessed on 8 September 2013

[373] David I Bainbridge, Introduction to Computer Law (4th edn, Pearson Education, 2000) Ch. 24, Computer Fraud at p 300.

section 14(1) provides for fraudulent acts on the computer system,[374] while the second provision provides for computer related fraud by false representation.[375]

Section 14(1) makes it an offence for 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 any economic benefits for himself or another person.[376] A very interesting aspect of this legislation is the provision regarding the resultant effect of the offence, which states that it is immaterial whether the purpose of the criminal act was to confer any economic benefit to the offender or another person.[377] The offence here is completed when the victims suffers a loss a result of the offender's criminal act on the data held on the computer system.[378]

Section 14(2) of the Act goes further to make it an offence for any person with the intent to defraud to send electronic message to a recipient, where such electronic message materially misrepresents any fact or set of facts upon which reliance the recipient or another person is caused to suffer any damage or loss. This provision, like the preceding provision in section 14(1), considers the offence completed on the proof that the victim suffered loss upon reliance on the misrepresentation made by the offender.[379] The provision of section 14(2) of the 2015 Act bears utmost resemblance to the provisions of section 1 of the Nigeria Advance Fee Fraud and other Fraud Related Offences Act, 2006.[380] One striking

---

[374] J M Adams, 'Controlling cyberspace: applying the computer fraud and abuse act to the internet' (1996) Santa Clara Computer & High Tech. LJ 12, 403; See also Christine S Davik, 'Access denied: Improper use of the Computer Fraud and Abuse Act to control information on publicly accessible Internet Websites' (2004) Maryland Law Review 63

[375] Nnabuihe, S Nwachukwu, S Nwaneri and N Ogbuehi, 'Critical Analysis of Electronic Banking in Nigeria' (2015) European Scientific Journal 11.10; See also C Mohamed, et al, '419 Scam: An Evaluation of Cybercrime and Criminal Code in Nigeria' (2015) Cybercrime, Digital Forensics and Jurisdiction, 129-144

[376] Idowu Abiola, and Adedokun Taiwo Oyewole, 'Internal Control System on Fraud Detection: Nigeria Experience' (2013) Journal of Accounting and Finance, 13(5), 141-152.

[377] Anah Bijik Hassan, D. L., Funmi, and Julius Makinde, 'Cybercrime in Nigeria: Causes, Effects and the Way Out' (2012) ARPN Journal of Science and Technology, 2(7), 626-631. See also N. H. A Aziz, et al, 'Financial fraud: Data mining application and detection' (2013) Innovation, Communication and Engineering, 341

[378] Kehinde Oladipo Williams and Kolawole Ojo Adekunle, 'Information and Communication Technology in Banking Sector: Nigeria and United Kingdom Comparative Study' (2013) International Journal of Advanced Research in Computer Science, 4(11).

[379] Orji Uchenna Jerome, Cybersecurity Law & Regulation (1st edn, Wolf Legal Publishers, 2012)

[380] Mohamed Chawki, et al, "419 Scam: An Evaluation of Cybercrime and Criminal Code in Nigeria", (2015) Cybercrime, Digital Forensics and Jurisdiction, 129-144; See also EIgbadon E Gregory and Adejuwon A. Grace, 'Psychodemographic Factors Predicting Internet Fraud Tendency among Youths in South-western, Nigeria' (2015) Journal of Educational and Social Research 5.2, 159

importance of the provision of the Advance Fee Fraud and other Fraud Related Offences Act, 2006 is the provision of section 1(1) which started with the phrase: '*Notwithstanding anything contained in any other enactment or law*'. This phrase is not contained in section 14 of the Cybercrime Act, and seems to give a subtle suggestion that the provisions contained in Advance Fee Fraud and other Fraud Related Offences Act, 2006, supersedes every other provision related to Fraud and other related activities. This suggestions is strengthened by the fact that section 1(3) which prescribes a harsher punishment of imprisonment for a term of not more than 20 years and not less than seven years *without the option of a fine,* for offenders convicted of any of the fraud-related offences.[381] This creates a situation where the prosecution are given options to pick and choose which legislation to use, and leaves no room for consistency.[382]

Section 419 of the Criminal Code Act (applicable in the Southern Nigeria) makes it a criminal felony punishable by 3 years imprisonment for any person who by any false pretence, and with intent to defraud, to obtain from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen.[383] A very interesting part of this provision is the use of the clause *'anything capable of being stolen'*. This provision except the use of the phrase 'anything capable of being stolen' bears utmost semblance to the provisions of section 1 of the Advance Fee Fraud and other Fraud Related Offences Act, 2006, and

section 14 of the Cybercrime Act 2015.[384] Under the Penal Code (as applicable to the Northern Nigeria), the offence is covered by the offences of cheating[385] and cheating by personation.[386]

---

[381] See Abiola Idowu and Kehinde A. Obasan, 'Anti-Money Laundering Policy and Its Effects on Bank Performance in Nigeria' (2012) Business Intelligence Journal, 6, 367-373

[382] E Inyang, Z Peter, and N Ejor, 'The Causes of the Ineffectiveness of Selected Statutory Anti-Corruption Establishments in Fraud Prevention and Control in the Nigerian Public Sector' (2014) Research Journal of Finance and Accounting, 5(5), 163-170

[383] Uche Onyebadi and Jiwoo Park, 'I'm Sister Maria. Please help me': A lexical study of 4-1-9 international advance fee fraud email communications (2012) International Communication Gazette, 74(2), 181-199

[384] The elements of the offence as enunciated in the case of *Alake v. The state* (1991) 7 *NWLR* Pt 205 pg. 567 at 591, and reiterated in *Onwudiwe v. FRN* (2006) 10 *NWLR* Pt 988 pg. 382 at 429-430 are as follows: "There is a pretence; The pretence emanated from the accused person; The pretence was false; The accused person knew of its falsity or did not believe in its truth; There was an intention to defraud; The things is capable of being stolen; and the accused person induced the owner to transfer his whole interest in the property" Maitanmi Olusola, et al, 'Cybercrimes and cyber laws in Nigeria", (2013) The International Journal of Engineering and Science (IJES), 2(4), 19-25

[385] Section 320 of the Penal Code. See also Timothy Yerima and Olubayo Oluduro, 'Criminal law protection of property: A Comparative Critique of the Offences of Stealing and Theft in Nigeria' (2012) Jorn of Pol & L, 5, 167; Akeem Olajide Bello, 'United Nations and African Union

An offender could alternately be charged under section 421 of the Nigerian Criminal Code Act[387] which provides that:

> Any person who by means of any fraudulent trick or device obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen or to pay or deliver to any person any money or goods, or any greater sum of money or greater quantity of goods than he would have paid or delivered but for such trick or device, is guilty of a misdemeanour, and is liable to imprisonment for two years. A person found committing the offence may be arrested without warrant.

Brenner (2010) vividly described this type of cybercrime which his very common in Nigeria, when she said "this type of fraud is known as 419 because many of the scams originate in Nigeria and section 419 of the Nigerian Criminal Code criminalizes fraud. A 419 scam begins with an e-mail, the subject line of which will be something such as 'From the Desk of Mr. [X]' or 'Your assistance is needed.' The e-mail will say that its author knows of: a large amount of unclaimed money or gold which he cannot access directly, usually because he has no right to it… The money could be… bullion [or]… a bank account… The sums involved are usually in the millions of dollars, and the investor is promised a large share, typically ten to forty percent, if they will assist… in retrieving the money." Brenner further explained how this 419 Fraud was used to defraud Janelia Spears, a registered nurse from a small town in Oregon, USA, who lost $400,000.00 to a Nigerian con man in 2008 "It began with an e-mail promising her $20 million left by her grandfather, with whom her family had lost touch years earlier.[388] Spears said the fact that the e-mailer knew her grandfather's name piqued her interest and convinced her there must be something to the story. She started by sending $100 but kept responding to the scam emailer's escalating demands for money. By the time she was done, she had mortgaged the house in while; she and her husband lived, put a lien on their car, and spent her husband's retirement money."

Conventions on Corruption and Anti-corruption Legislations in Nigeria: A Comparative Analysis' (2014) Afr J Int'l & Comp L, 22, 308

[386] Section 321 of the Penal Code. See also Akeem Olajide Bello, 'Criminal Law in Nigeria in the last 53 Years: Trends and Prospects for the Future' (2013) Acta Universitatis Danubius, Juridica, (1), 15-37

[387] See Okay Benedict Agu, 'Economic Crimes and National Security: Nigerian Perspective' (2012), Law and Security in Nigeria, 3; See also John O Odumesi, 'Combating the Menace of Cybercrime' (2014) IJCSMC, Vol 3, Issue 6, June 2014, 980–991

[388] S W Brenner, Cybercrime: Criminal Threats from Cyberspace. (Santa-Barbara, CA: ABC-CLIO LLC, 2010) p.84

Romance Scam

These schemes involve scammers pretending to seek companionship or romance online. Victims of these scams believe they are in a relationship with someone who is honest and trustworthy without meeting them in person. Cybercriminals search dating websites, chat rooms, and social media websites for personally identifiable information, and use well rehearsed scripts to attract potential victims. The criminals present convincing scenarios involving family tragedies, severe life circumstances, and other hardships in an attempt to solicit money[389]. Ironically, a good number of Nigerian cybercriminals involved in this are young boys and men, who simply morph the faces or simply use the pictures of innocent beautiful ladies, who may not even be aware that their faces or pictures have been used for such cybercrimes.

Phishing and Spoofing

This involves the duplication of the Websites of reputed institutions in order to win over the confidence of genuine customers, thereafter inducing them to part with confidential information, such as account numbers or passwords. The perpetrators can then gain access to the victims' online banking accounts.[390] According to,[391] "many Nigerians who have lost money through online banking fraud and related scams have been victims of spear phishing attacks. These attacks are becoming more sophisticated as the criminals device more ways to circumvent security measures put in place by deposit money banks (DMBs) in the country. The criminals have also latched onto ongoing bank verification number (BVN) scheme of the Central Bank of Nigeria (CBN). They capitalize on the 'fire brigade' mentality of the populace…." He further provided an example of a typical phishing scam e-mail "Dear Customer, The online registration for your Unique Identification Number (BVN) is incomplete. Failure to complete this process will result in permanent account termination as directed by CBN. http://bit.ly/1IFsHda."

Hacking

This involves cybercriminals having unauthorized access to persons' confidential information, restricted information belonging to large corporations or government

---

[389] Internet Crime Complaint Centre (*IC3*) (2014). Internet fraud-crime report. National White Collar Crime Centre and the Federal Bureau of investigation.
http://www.ic3.gov/media/annualreports.aspx

[390] R K Raghavan, 'Cybercrime: problems and prospects.' in G T Kuria, (ed.) World Encyclopedia of Police Forces and Correctional Systems (2nd ed.) (New York: Thomson Gale, 2006).

[391] L Ajanaku, Cyber crooks prowl on social media sites: How to stay ahead of them. The Nation, 2015 p 13-14

departments, and using the information to cause harm, damage, injury, destruction, evaluation or losses.[392] Cybercriminals in Nigeria are involved in 'massive hacking business' and it is for this reason that Semantic Corporation, maker of Norton Computer Security Software in 2011 rated Nigeria as the 59th country in the world for malicious activities.[393] In the same year (2011), Cybercrime watch report ranked Nigeria 3rd in hacking in the world after United Kingdom – 2nd and USA – 1st.[394] Some cybercriminals in Nigeria do hack into their victims' information and thereafter, phone their victims instead of using email. They usually pretend to be from a bank, and try to convince the victim to share sensitive information such as passwords.[395]

4. Objective and Application

The objectives of this Act are to –

(a) Provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrime in Nigeria;
(b) Ensure the protection of national information infrastructure; and
(c) Promote cyber security and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights.

The provisions of this Act shall apply throughout the Federal Republic of Nigeria.[396]

5. Protection of Critical National Information Infrastructure

(1) The President may, on the recommendation of the National Security Adviser, by Order published in the Federal Gazette designate certain computer systems or networks, whether physical or virtual, the computer programs, computer data or traffic data vital to this country that the incapacity or interference with such system and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters as constituting Critical National Information Infrastructure.

---

[392] *Ibid*

[393] Symantic Corporation, Internet security threat report (Vol. 18). (New York, 2012)

[394] Cybercrime Watch, Cybercrime report. Retrieved available online: www.myfinancialintelligence-nigeria-eye-cybercrime accessed 10the November, 2019

[395] *Op.cit*

[396] See section 1 & 2 of the Cybercrime (Prohibition Prevention, ETC) Act, 2015

(2) The Presidential Order made under subsection (1) of this section may prescribe minimum standards, guidelines, rules or procedure in respect of –

(a) the protection or preservation of critical information infrastructure;
(b) the general management of critical information infrastructure;
(c) access to, transfer and control of data in any critical information infrastructure;
(d) infrastructural or procedural rules and requirements for securing the integrity and authenticity of data or information contained in any designated critical national information infrastructure;
(e) the storage or arching of data or information designated as critical national information infrastructure;
(f) recovery plans in the event of disaster, breach or less of the critical national information infrastructure or any part of it; and
(g) any other matter required for the adequate protection management and control of data and other resources in any critical national information infrastructure.[397]

The Presidential Order made under section 3 of this Act may require the Office of the National Security Adviser to audit and inspect any critical national information infrastructure at any time to ensure compliance with the provisions of this Act.[398]

(1) A person who, with intent, commits any offence punishable under this Act against any critical national information infrastructure, designated under section 3 of this Act, is liable on conviction to imprisonment for a term of not more than 10 years without option of fine.

(2) Where the offence committed under subsection (1) of this section results in grievous bodily harm to any person, the offender is liable on conviction to imprisonment for a term of not more than 15 years without option of fine.

(3) Where the offence committed under subsection (1) of this section results in the death of a person, the offender is liable on conviction to life imprisonment.[399]

(1) A person, who, without authorization, intentionally accesses, in whole or in part, a computer system or network for fraudulent purposes and obtains data that are vital to national security, commits an offence and is liable on

[397] See Section 3, *ibid*
[398] See Section 4, *ibid*
[399] See Section 5, *ibid*

conviction to imprisonment for a term of not more than 5 years or to a fine of not more than ₦5,000,000.00 or both.[400]

(1) The Council shall

(a) Create an enabling environment for members to share knowledge, experience, intelligence and information on a regular basis and shall provide recommendations on issues relating to the prevention and combating of cybercrimes and the promotion of cyber security in Nigeria;

(b) Formulate and provide general policy guidelines for the implementation of the provisions of this Act;

(c) Advice on measures to prevent and combat computer related offences, cybercrimes, threats to national cyberspace and other cyber security related issues.

(d) establish a program to award grants to institutions of higher education to establish cyber security Research centres to support the development of new cyber security defense; techniques and processes in the real-world environment and

(e) Promote Graduate Traineeships in cyber security and computer and network security research and development.

(2) The Council shall have power to regulate its proceedings and make standing orders with respect to the holding of its meetings, notices to be given, the keeping of minutes of its proceedings and such other matters as the Council may, from time to time, determine.[401]

6. Arrest, Search, Seizure and Prosecution

(1) A law enforcement officer may apply exparse to a judge in Chambers for the issuance of a warrant for the purpose of obtaining electronic evidence in related crime investigation.

(2) The Judge may issue a warrant authorizing a law enforcement officer to –

(i) An offence under this Act is being committed; or

(ii) There is evidence of the commission of an offence under this Act, or

(iii) There is an urgent need to prevent the commission of an offence under this Act;

(b) search any person or conveyance found on any premises or place which such authorized officers who are empowered to enter and search under paragraph (a) of this subsection;

---

[400] See Section 6, *ibid*

[401] See Section 43, *ibid*

(c) Stop, board and search any conveyance where there is evidence of the commission of an offence under this Act;
(d) Seize, remove and detain anything which is, or contains, evidence of the commission of an offence under this Act;
(e) Use or cause to use a computer or any device to search any data contained in or available to any computer system or computer network;
(f) Use any technology to decode or decrypt any coded or encrypted data contained in a computer into readable text or comprehensible format; or
(g) Require any person having charge of or otherwise concerned with the operation of any computer or electronic device in connection with an offence under this Act to produce such computer or electronic device.
(3) The court shall issue a warrant under subsection (2) of this section where it is satisfied that –
(a) The warrant is sought to prevent the commission of an offence under this act or to prevent the interference with investigative process under this Act.
(b) The warrant is for the purpose of investigating cybercrime, cyber security breach, computer related offences or obtaining electronic evidence;
(c) There are reasonable grounds for believing that the person or material on the premises or conveyance may be relevant to the cybercrime or computer related offences under investigation; or
(d) The person named in the warrant is preparing to commit an offence under this Act.[402]

(1) Subject to the powers of the Attorney General relevant law enforcement agencies shall have power to prosecute offences under this Act.
(2) In the case of offence committed under section 19 and 21 of this Act, the approval of the Attorney General must be obtained before prosecution.[403]

(1) In addition to any other penalty prescribed under this Act, the Court shall order a person convicted of an offence under this Act to make restitution to the victim of the false pretense or fraud by directing the person, where

[402] See Section 45, *ibid*
[403] See Section 47, *ibid*

the property involved is money, to pay to the victim an amount equivalent to the loss sustained by the victim and in any other case to –

(a) Return the property to the victim or to a person designated by him; or

(b) Pay an amount equal to the value of the property, where the return of the property is impossible or impracticable.

(2) An order of restitution may be enforced by the victim or by the prosecutor on behalf of the victim in the same manner as a judgment in a civil action.[404]

7. Conclusion and Recommendations

There is no doubt that cybercrime is a type of crime in Nigeria. It is a menace that should be eradicated, if not reduced to a very minimal level for our great nation to develop. Our government should make the welfare and well being of the citizens of paramount importance so as to lessen the burden of individuals by providing good paying jobs and other basic amenities. The extant legislation on cybercrime – Cybercrimes (Prohibition Prevention, ETC) Act, 2015 should be quickly amended to make the Cybercrime Advisory Council (otherwise in this Act referred to as "The Council" to be a body corporate and fully independent and to proscribe any offence committed under section 19 and 21 of this Act without seeking the consent and approval of the Attorney General of the Federation. The Federal Legislature should in fact amend sections 42, 43 and 47 of the Act; to this extent and make cybercrime in Nigeria to be a strict liability crime. The Federal Government of Nigeria should put technological facilities in place to enable law enforcement agents in Nigeria to effectively prosecute offenders; as crimes are presently been committed in the world using advanced technical means.

[404] See Section 49, *ibid*