ISSN: 3064-8378

Public Policy and Administration Studies Journal

Research Article

THE LEGAL BATTLE AGAINST CYBERCRIME IN NIGERIA: AN ASSESSMENT OF CURRENT LAWS

Aisha Oluwakemi Balogun

Senior Lecturer, Faculty of Law (Oleh Campus), Delta State University, Abraka, Nigeria.

DOI: 10.5281/zenodo.14892555

Abstract

Cybercrime, in the era of advanced technology, poses a significant threat to individuals and organizations, disrupting the fabric of global security and economic stability. The abstract examines the rise of cybercrime in the digital age, where criminals exploit the vulnerabilities of cyberspace to commit a wide range of offenses. The evolution of information technology has created a parallel world in cyberspace, offering opportunities and convenience to users, but it has also paved the way for malicious actors to exploit this interconnected network.

With the proliferation of netizens, the misuse of technology has led to a surge in cybercrime, both at domestic and international levels. In contrast to traditional physical crimes, modern cybercriminals can cause extensive damage and financial losses with the click of a button. These abstract highlights the economic toll of cybercrime, emphasizing the impact on individuals and businesses as criminals exploit vulnerabilities to steal, defraud, and compromise sensitive data. Cybersecurity measures have become crucial in safeguarding against these digital threats, protecting the global economy from this evolving challenge.

Keywords: Cybercrime, Information Technology, Cyberspace, Economic Impact, Cybersecurity.

1. Introduction

As the computer usage became more popular, there arose an expansion in the growth of technology. The evolution of information technology (IT) gave birth to cyber space wherein internet provides equal opportunity to everyone to access any information, store data, etcetera with the use of high technology.

Owing to the rise in the number of netizens, misuse of technology in the cyberspace increased and this in turn gave birth to different forms of cybercrime at the domestic and international level. In the past, some forms of crimes such as stealing, armed robbery, which were usually committed against physical property were more common. However, with the advent of Information Technology, the trend has changed. The modern thief can steal more from a computer than with a gun and tomorrow's terrorist may do more damage using a keyboard than with a bomb. Criminals will generally not commit armed robbery at a branch of a bank these days when they can hack into e-mails and access bank accounts from the relative comfort, safety and anonymity of their computer. Cybercrime is a clog in the wheel of economic progress the world over. Perpetrators of cybercrime care less about the economic well-being of their victims. For instance, once a cyber-criminal hacks into a bank account; he does not stop making withdrawals from the said account until he drains it of all funds.

ISSN: 3064-8378

Public Policy and Administration Studies Journal

Research Article

Law enforcement agencies and Consultancies around the world report that incidences of cybercrime are on the rise. Nigeria is not immune from cybercrime and its ugly effects. The Nigerian experience of cybercrime and computer related offences assumed a terrifying dimension in the late 90s and early 2000 and is still on the rise with the advent of GSM phones, sophisticated computers and an influx of network providers which affords everyone equal opportunity to access the internet.

The Nigeria Deposit Insurance Corporation (NDIC) 2014 Annual Report shows that between year 2013 and 2014, fraud on the e-payment platform of the Nigerian Banking sector increased by 183 percent. Cybercrime in this interconnected world has become pervasive and requires an adequate legislation at the national and international level. Many countries make laws and develop strategies towards fighting cybercrime by preventing, detecting and containing the threat associated with it. These strategies comprise legal and regulatory frameworks. Also at the international scene, there is the Budapest Convention on the control of cybercrime which Convention has been ratified by some States.

In Nigeria, there exist some local legislation which though were not directly made for the control of cybercrimes, but had some provisions which if properly enforced will lead to the control of some types of cybercrimes. These provisions can be found in some laws such as the Economic and Financial Crimes Commission (EFCC) Act, 2004, Advanced Fee Fraud Act, The Criminal Code Act, the Evidence Act, etcetera. The inadequacies in these laws and the proliferation of cybercrimes in Nigeria prompted the Nigeria National Assembly to pass a bill for the Prohibition and Prevention of Cybercrime and other Related Offences. This bill was signed into law by the immediate past President of the Federal Republic of Nigeria, Dr. Goodluck Ebele Jonathan on the 15th day of May, 2015. This law is the ―Cybercrime (Prohibition and Prevention etc) Act, 2015‖ (the cybercrime Act).

With the enactment of this law, the nation's socio-economic environment ought to heave a sigh of relief. Regrettably however, this principal legislation made solely for the purpose of fighting cybercrime in Nigeria is marred with shortcomings which if not checked will vitiate the purpose of the enactment with respect to its implementation.

This paper seeks to address the issue of cybercrime, cybercrime laws as well as the effects of cybercrime in Nigeria. The paper will critically examine the provisions of the Cybercrime Act and the other laws enumerated above to determine how well suited they are to deal with the menace of cybercrime in Nigeria.

2. Definition of Cybercrime Et Al

The different types of cybercrime committed in Nigeria ranges from the following:[14] Identity theft and invasion of privacy, Internet fraud, ATM Fraud, File sharing and piracy, Counterfeiting and forgery, Child pornography, Hacking, Cyber terrorism and a host of others. Sackson defines cybercrime ―as a crime that is committed with the use of a computer through a communication device or a transmission media called the cyberspace and global network called the internet.‖ Clay on his part, states that it is ―a crime that is enabled by or targets computers.‖

ISSN: 3064-8378

Public Policy and Administration Studies Journal

Research Article

In the Encyclopedia Britannica, the word cyber crime is defined as ―the use of computer as an instrument to further illegal ends such as committing fraud, trafficking in child, etc‖

The writers of this paper define cybercrime ―as the commission of clandestine and criminal activities in a cyberspace using a computer which is connected to a type of network as enabled by network providers‖. Okonigene et al in looking at cybercrime in Nigeria examined cybercrime vis-à-vis the Economic and Financial Crimes Commission Act, 2004 and the Criminal Code as laws available in combating cybercrime in Nigeria. The author restricted his work to two Laws whereas there are numerous others such as the Advanced Fee Fraud and other Related Offences Act, the money Laundering (Prohibition) Act, the Nigerian Evidence Act etc. which indirectly ensures the control of cybercrime.

On his part, Babafemi while looking at the legal framework on cybercrime in Nigeria analysed in detail the legal and institutional framework for cybercrime control in Nigeria. The author examines extensively, the causes and effects as well as the history of cybercrime and cybercrime laws with particular reference to Nigerian circumstance in chapter two. Sekav discussed the legal and institutional frameworks relevant for International Corporation against cybercrime in Nigeria. Although the work is very elaborate on the laws and enforcement agencies, it dwells more on international laws and frameworks for combating cybercrime.

Succinctly, Adejoke discusses the impacts and challenges of Information and Communication Technology in the fields of Commerce, Banking and other businesses in Nigeria. The author opined that there is a need for legislative intervention but the fragmented ICT laws and multi-layered regulatory institutions

Ibrahim et al[1] in their article examined sections 52(4) (b) and 52(2) of the Cyber Crimes (Prohibition, Prevention Etc) Act, 2015, to the effect that the Act provides for international corporation by the Attorney-General of the Federal Republic of Nigeria and other countries without the existing multilateral or bilateral agreement for this collaboration as well as the provision for extradition orders in laws of the other countries. According to the author, when one country's law criminalises high tech and computer related crimes and another country's law does not, cooperation to solve or eradicate such crimes may not be possible. Where there is no extradition treaty between Nigeria and a foreign country, offenders may not be extradited to Nigeria for the purpose of prosecution and this in turn will vitiate the provision of section 51 which provides that offences under the Act shall be extraditable under the Act.

[1] Ibrahim, A; Miriam, M. Cybercrime (Prohibition, Prevention Etc) Act,2015: Issues and Challenges in Nigeria. (Draft Paper Presented at the 49th Annual Nigerian Law Teachers' Conference at Nasarawa State University, Keffi on behalf of Usman Danfodio University Sokoto, 22nd -27th May, 2016) pg. 15-16.

ISSN: 3064-8378

Public Policy and Administration Studies Journal

Research Article

Specifically, Gbenga et al[2] in a Report for the Cyber Steward Network discusses the effect of cybercrime on the Nigerian economy, efforts of the National Assembly to provide laws to fight cybercrime and the need to fight cybercrime to encourage e-trade and salvage the nation's battered image.

Ani[3] in her work, ―Cybercrime and the National Security in Nigeria‖ is of the opinion that enforcement officials cannot effectively pursue cybercriminals unless they have the legal tools necessary to do so.

From all the literature discussed above, the writers of this paper observe that cybercrime is a nefarious crime with attendant evils, and therefore all hands must be on deck to urgently combat it, that is, there should be synergy of energy or collaboration among all to combat it.

3. Brief Statistics of Cybercrime in Nigeria

Nigeria records about N127 Billion loss annually to cybercrime. This figure represents 0.8% of the country's Gross Domestic Product (GDP).[4] In 2015, the Information Security Society of Nigeria (ISSAN) revealed that 25 percent of cybercrime in Nigeria are unresolved and 7.5% of the world hackers are Nigerians.[5] The EFCC reported in 2014 alone that customers in Nigeria lost approximately six billion naira to cyber criminals. Similarly, the CBN in 2015 reported that 70 percent of attempted or successful fraud/forgery cases in Nigeria banking sector were perpetrated via the electronic channels. Banks in Nigeria have lost approximately 159 billion naira to electronic frauds and cyber criminals between year 2000 and 2013 and the impact on the nation's economy as well as cashless policy is significant.[29]

Activities of cybercriminals particularly hackers resulted in the loss of eighty billion dollars in the struggle of combating the crime globally and about one hundred and twenty seven billion naira was the estimated loss to cybercrime in Nigeria between 2015 and 2017 according to the National Communication Commission.[6]It has been estimated that cyber security spending will exceed one trillion dollars from 2017 to 2020 and that damage cost will hit six trillion dollars annually by 2021.[7]

---

[2] Gbenga, S ; Babatope S; and Bankole O. A Report for the Cyber Stewards Network Project of the Citizen Library, Munk School of Global Affairs, University of Toronto at 11.

[3] Ani ,L. Cybercrime and national Security, the Role of the Penal and Procdural Laws in Azinge, E, SAN, et al (eds), *Law and Security in Nigeria,* (Nigerian Institute of Advanced Legal Studies Press, 2011)197-234.

[4] *Ibid.*

[5] *Ibid.* [29]

Ibid.

[6] Mbachu G; and Nazeef B. Cybercrime: Nigeria's Losing Battle Against Unrelenting Enemies. https://leadership.ng>. accessed October 2 2019.

[7] *Ibid.*

ISSN: 3064-8378

Public Policy and Administration Studies Journal

Research Article

4. The Legal Framework For Cybercrime Control In Nigeria

Presently, the principal legislation for combating acts of cybercrime in Nigeria is the Cybercrime (Prohibition, Prevention, etc) Act, 2015. Before the enactment of the Cybercrime (Prohibition, Prevention, etc) Act, 2015, the Nigerian digital economy had carried on with the absence of a specific legal framework for cyber security, causing a glaring gap in law enforcement agencies which draw their powers from the law. With the advent of the Cybercrime Act in 2015, Nigeria became more equipped legally in the fight against cybercrime activities.

However, it may not be adequate to discuss the Cybercrime Act 2015 without throwing some light on the enabling laws which were in existence in controlling cybercrimes before the Cybercrime Act was enacted. These laws in the order of their analysis are the Economic and Financial Crimes Commission (Establishment) Act, 2004, the Advanced Fee Fraud and other Related Offences Act, 2006, Money Laundering (Prohibition) Act, 2011 as amended in 2013, the Nigerian Evidence Act ,The Criminal Code Act, The Penal Code Act, the Terrorism (Prevention) Act, 2013, the National Identity Management Commission Act, 2007 while the institutional frameworks discussed are the Nigerian Financial Intelligence Unit (NFIU), Special Control Unit against Money Laundering and the Nigerian Cyber Crime Working Group.

4.1 The Economic and Financial Crimes Commission (Establishment) EFCC Act.

Before the enactment of the Cybercrimes Act, 2015, the Economic and Financial Crimes Commission (EFCC) Act[8], (hereinafter referred to as the EFCC Act) was the main legislation used in the fight and prosecution of Cyber criminals as it has a wide range of provisions relating to cyber/internet crimes. The EFCC Act provides that:

The Commission (Economic and Financial Crimes Commission) Established under the EFCC Act shall have the responsibility of enforcement and due administration of the provisions of the Act, the investigation of all financial crimes, including advanced fee fraud, money laundering, counterfeiting, illegal charge transfers, futures market fraud, fraudulent encashment of negotiable instruments, computer credit card fraud, contract scam, etc.[9]

The EFCC Act appears to have made very elaborate provision towards cyber security by creating a wide scope of cyber and internet crimes to which the Act applies. This provision and powers to prosecute those crimes and many more, has helped the Commission in making some laudable achievements in the fight against various types of cybercrime.

This provision has been the basis of various cases involving the Commission including the celebrated case of Federal Republic of Nigeria v. Chief Emmanuel Nwude & ors [10] and another case discussed below under the EFCC as an agency for cyber security. In the case of FRN V. Emmanuel Nwude, the accused persons were

[8] CAP E10, LFN 2010.

[9] Section 6 (a) (b) EFCC Act..

[10] Suit No. CA/245/2005.

ISSN: 3064-8378

Public Policy and Administration Studies Journal

Research Article

charged for a 57 count charge including scamming to the tune of US $181.6 million. They were found guilty of all the charges and were sentenced accordingly; their assets were forfeited to the Federal Government and the proceeds of the scam were recovered and returned to their owners. The Act also clearly provides the offences to be prosecuted under it.[11] These are offences against economic and financial crimes.

From the foregoing, it is clear that the EFCC Act though not specifically made for cyber security has enormous provisions for that purpose. However, the Act is not without loopholes.

The Act provides that the Commission created under the Act shall have powers towards the coordination and enforcement of all economic and financial crimes laws and enforcement of functions conferred on any other person or authority.[12] A strict application of this provision will create an atmosphere of power tussle between the Commission and other Law enforcement agencies including the Nigerian Communication Commission an agency charged with enforcing the Cybercrime Act, 2015. Also, the Act is not elaborate in enumerating acts and activities that constitute cybercrimes.

4.2 Advanced Fee Fraud and other Related Offences Act, 2006.

The Advanced Fee Fraud and other Related Offences Act[13] (hereinafter referred as AFF Act) was enacted in 2006 for the purpose of prohibiting and punishing certain offences relating to advanced fee fraud and other fraud related offences and to repeal other Acts related therewith. The Act generally provides for ways of fighting fraud including but not limited to internet fraud, cybercrime and other frauds such as obtaining property by false pretence, use of premises for fraudulent purposes, fraudulent invitations, laundering of fund obtained through unlawful activities, conspiracy, aiding among others[14].

The Act states that any person or entity providing an electronic communication service or remote computing service either by e-mail or any other form shall be required to obtain personal information of their customers.[15]

The Act makes it an offence to commit fraud by false pretence.[16] This provision would always come handy in prosecution of most cybercrimes especially those related to identity theft, phishing and spoofing and a host of others whose perpetrators are usually anonymous and hiding under false pretence.

The AFF Act also provides that:

[11] Section 14, 15, 16, 17 & 18 of the EFCC Act.

[12] Section 6 (c), EFCC Act.

[13] CAP A6 LFN, 2010.

[14] Tomilehun, B. An Appraisal of the Legal Framework of Cybercrime in Nigeria. Available on: https://www.info@clrwc.com. accessed on October 8 2019.

[15] Section 11 A (1) AFF Act.

[16] Section 2.

ISSN: 3064-8378

Public Policy and Administration Studies Journal

Research Article

a person who conducts or attempts to conduct a financial transaction which involves the proceed of a specified unlawful activity with the intent to promote the carrying on of a specified unlawful activity ; or where the transaction is designed to conceal or disguise the nature, location, source or ownership or the control of proceed of a specified unlawful activity is liable on conviction to a fine of one million Naira and in the case of a Director, Secretary or other official of a financial institution or corporate body or any other person to imprisonment for a term not more than ten years and not less than five years.[17]

This is a laudable position particularly the aspect of going after the main operators of the fraudulent act where a company is involved. The AFF Act also prohibits accepting an internet user as anonymous. That is to say that by virtue of the Act, every internet user must have an identity. The Act enjoins business owners such as financial institutions, Internet Service Providers and Cyber café owners to do well to obtain necessary information about their customers.[18] The AFF Act stipulates that providers of internet services shall be registered with Economic and Financial Crimes Commission and together with GSM service providers, provide information on demand to EFCC.

All these are in a bid to trace them or their customers if it is discovered that they are carrying on fraudulent activities online.

However, the following are some areas which in the opinion of the writers need to be reviewed. The Act vests the power and responsibility of surveillance on the operators such as Corporations as well as internet service providers. Although, this approach may seem a welcome development especially as these operators relate with the customers/criminals on daily basis, the fact that some of the employees of these operators have criminal tendencies and may assist these criminals should not be ruled out. For instance, despite the security and anti-fraud measures placed by banks and other financial institutions such as the Know Your Customer (KYC) schemes, frauds especially phishing keep rising on daily basis. It appears to be the case that the banks data base is continuously hacked on daily basis because an insider is assisting these criminals with information on customers' account status. This power of surveillance should have been shared between the operators and the relevant Law enforcement agencies.

4.3 Money Laundering (Prohibition) Act 2011

The Money Laundering (Prohibition) Act[19] (hereinafter referred to as the ML Act) is an Act that prohibits the laundering of proceeds of crime or an illegal act. The ML Act provides that no person or body corporate shall except in a transaction through a financial institution, make or receive cash payment of a sum exceeding

[17] Section 7 *ibid.*

[18] Section 12 AFF Act.

[19] CAP, M18, LFN 2018.

ISSN: 3064-8378

Public Policy and Administration Studies Journal

Research Article

#5,000,000.00 (five million naira) or its equivalent in case of an individual or #10,000,000.00 (ten million) or its equivalent in case of a body corporate.

By virtue of this provision, all banks and financial institutions in Nigeria are charged to always report any such transaction of a sum exceeding US $10, 000.00 (ten thousand dollars) or its equivalent to the Central Bank of Nigeria, the Securities and Exchange Commission or the Commission (EFCC in this case) in writing within 7 days from the date of the transaction.[20] The purpose of this requirement is to ensure that banks and financial institutions are not used as a conduit pipe by the cyber criminals to facilitate online crimes. Transportation of cash or negotiable instruments in excess of US $ 10,000.00(ten thousand dollars) or its equivalent by individuals or by any corporate body in or out of the country shall be declared to the Nigerian Customs Service.[21]

From the above provisions, it is very clear that the Act provides elaborately for cyber security and measures to guard against cybercrimes especially in the financial institutions. However, the Act fails to create its own agency for the enforcement of its provisions. Rather the provisions are to be enforced by the Economic and Financial Crimes Commission.[22] The writers are of the opinion that this may constitute a clog in the wheel of speedy enforcement of the provisions of the ML Act. The EFCC Act should be amended to remove the enforcement of provisions of the Money Laundering Act from it. Also, the ML Act should be amended to create an agency for the enforcement of its provisions. However, this situation is already being addressed in the new Money Laundering (Prevention and Prohibition) Bill pending before the National Assembly.[23] The bill seeks to repeal the existing Money Laundering Act among others. The bill also seeks to set up an agency, Bureau for Money Laundering Control (BMLC) as an independent agency for the enforcement of the provisions of the Money Laundering Act and related cases.

4.4 The Nigerian Evidence Act, 2011

The Evidence Act of 2011 which repealed the old Evidence Act of 2004 by provides for admissibility of computer and internet generated evidence among other things. Before the enactment of this new Evidence Act, electronically generated evidence was not admissible in our courts thereby creating an impediment in the admissibility of internet generated evidence.

This position, no doubt was a clog in the wheel of the nation's justice system up till 2011 when it was repealed. Prior to 2011, the courts were aware of the computer generated evidence as reflected in the case of Esso West

[20] Section 2 (1) *Ibid.*

[21] Section 2(3), *Ibid.*

[22] Section 7 EFCC Act.

[23] Chido, O. The Money Laundering Act and its Discontents. Available on: https://www.thisdayonline.com> 2016/02/15>mon... accessed November 5 2019.

ISSN: 3064-8378

Public Policy and Administration Studies Journal

Research Article

Africa Inc. v. T. Oyegbola,[24] but the hand of the courts were tied. In this case, the Supreme Court said that the law is not and cannot be ignorant of the modern business methods and must not shut its eyes to the mysteries of the computer.

This old position has been remedied in the new Evidence Act. The new Act provides that ―in any proceedings, a statement contained in a document produced by computer shall be admissible as evidence of any fact stated in it of which direct oral evidence would be admissible.‖[25] Thus, the Evidence Act haven made an inroad towards the admissibility of computer generated evidence, information obtained online could be applied to convict cyber criminals. Also, the Evidence Act in the interpretation section defines a document to include ―…any disc, tape, sound track or other device in which sound or other data are embodied so as to be capable of being reproduced from it and any device by means of which information is recorded, stored or retrievable including computer output‖[26]. This definition is wide enough to accommodate information from computer networks and online activities.

Laudable as this position may seem in prosecution of crimes especially cybercrimes, the Act laid down some conditions for admissibility of such evidence. The Act provides that evidence generated through a computer is admissible if:

a) That the document containing the statement was produced by the computer during a period over which the computer was used regularly to store or process information for the purpose of any activity regularly carried on over that period of time whether for profit or not by anybody whether corporate or not or by any individual;

b) That over that period , there was regularly supplied to the computer in the ordinary course of those activities, information of the kind from which the information so contained is derived;

c) That throughout the material part of that period, the computer was operating properly or, if not, that in respect of which it was not operating properly or was or out of operation during that part of that period was not such as to affect the production of the document or the accuracy of its contents; and

d) That the information contained in the statement reproduces or is derived from information supplied to the computer in the ordinary course of those activities.[27]

In the case of Kubor v. Dickson &Ors[28], the Supreme Court held that ―a party seeking to tender in evidence computer generated documents need to do more than just tendering same from the bar. Evidence in relation to the use of computer must be called to establish the conditions set out under section 84 (2)‖. These conditions may

[24] (1969) 1 NMLR, pt. 194 at 198.
[25] Section 84 (1) Evidence Act.
[26] Section 258, *Ibid.*
[27] Section 84 (2) (a—d).
[28] (2014) SC 193.

ISSN: 3064-8378

Public Policy and Administration Studies Journal

Research Article

pose some difficulty to the law enforcement agents. as most of these law enforcement agencies are under- funded. Even, when they are adequately funded, most of the agents may not be knowledgeable enough to know how to pass through the rigorous process of calling an expert through whom the evidence will be tendered. In such circumstance, the case may be lost for want of proof.

4.5 The Criminal Code Act

The Criminal Code Act[29] criminalizes any type of stealing as well as false pretences in Nigeria.[30] The Act provides that:

Any person who by any false pretence, and with the intent to defraud, obtains from any other person anything capable of being stolen or induces any other person to deliver anything capable of being stolen is guilty of a felony and is liable to imprisonment for three years[57].

The Criminal Code also provides that:

Any person who by means of any fraudulent trick or device, obtains from any 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 paid for or would have been delivered but for such trick or device is guilty of a misdemeanor and is liable to imprisonment for two years.

These provisions appear very useful in the prosecution of cyber criminals who thrive on false pretences such as pretending to be the Directors of companies, or presenting a false account as that of a corporate body with the intent of defrauding persons who deal with them on the strength of such representation.

Unfortunately, the Criminal Code is a legacy of British colonial era; it predates the internet era and understandably does not specifically address internet scams[31] under the section dealing with false pretences. The archaic nature of the Criminal Code is seen in section 419 which provides that unless the criminal is caught in the act; such criminal cannot be arrested without warrant. Cyber criminals are very smart and can delete all traces of the crime and transaction before a warrant of arrest is obtained by the law enforcement agents. Again, it is only in exceptional cases that a cyber criminal can be caught in the act. Online crimes are usually detected or felt after its commission. Furthermore, the punishment for criminals under the Criminal Code which is three years imprisonment or seven years imprisonment if the value of the stolen property exceeds one thousand naira is a clear indication that the law was not intended to apply to the modern day crimes such as cybercrime. The sum of

[29] CAP C38, LFN 2004.

[30] Section 1 Criminal Code. [57]
Section 419.

[31] Chawki, M. Nigeria Tackles Advanced Fee Fraud. (2009), Vol. 1 Journal of Information, Law and Technology at .8.

ISSN: 3064-8378

Public Policy and Administration Studies Journal

Research Article

one thousand naira is meagre and ridiculous compared to what these criminals steal on daily basis which usually run into millions of dollars.[32] Another unpleasant aspect of our criminal justice system is that the State is the complainant and in most cases, nothing goes to the victims at the end of the day.[33] Thus, the victims of cybercrimes may not be willing to bring complaints about cybercrime activities even when they are affected.

4.6 The Penal Code Act

The following are some provisions of the Penal Code Act[34] which are cybercrime related and may be employed towards fighting cybercrime:

Section 320 states that whosoever by deceiving a person:

a) fraudulently or dishonestly induces the person so deceived to deliver any property to a person or consent that any person shall retain any property; or

b) Intentionally induces the person deceived to do or omit to do anything which he would not do or omit to do if he were not so deceived and which act or omission causes or is likely to cause damage to that person in body, mind, reputation or property is said to cheat[35]. This provision could be used as a tool in the fight against cybercrime which thrives on deception. The element of inducement as contained in this section is seen most especially in the cyber-crime of cyber terrorism and phishing.

The Act under section 362 further provides that:

a person who dishonestly makes, signs, seals or executes a document or part of it with the intent of making others to believe that the document is made by the authority authorized to so make; or without lawful authority, alters a document or part of it with the intent of deceiving others to believe that the document emanates from a lawful authority commits forgery

This is yet another section of the Act which may be employed toward prosecuting cyber criminals in the area of forgery and counterfeiting. However, the Penal Code Act is an old legislation and only applies to the Northern part of the country.

4.7 The Terrorism (Prevention) (Amendment) Act, 2013

This Act repealed the Terrorism (Prevention Act) of 2011 and made provisions for extra territorial application of the Act as well as strengthening the regulation of Terrorist financing Offences.[36]

Section 1 (b) of the Act provides that:

---

[32] Oriole, T. Advanced Fee Fraud on the Internet (2005) Vol. 21 Computer Law and Security Report at 241.

[33] *Ibid.*

[34] CAP P3, LFN 2004.

[35] Section 320 (a) & (b) Penal Code Act.

[36] Ibrahim, A An Appraisal of the Legal and Administrative Framework for Combating Terrorist Financing (2013) Vol. 19 Journal of Law, Policy and Globalization, at 32. [65] Section 1(a)of the Terrorism (Prevention) Act 2013.

ISSN: 3064-8378

Public Policy and Administration Studies Journal

Research Article

any person or body corporate who knowingly in or outside Nigeria, directly or indirectly deals or attempts or threatens any act of terrorism,[65] commits an act preparatory to or in furtherance of an act of terrorism, omits to do anything that is reasonably necessary to prevent an act of terrorism,[37] assists or facilitates the activities of persons engaged in an act of terrorism or is an accessory to any offence under this Act,[38]participates as an accomplice in or contributes to the omission of any act of terrorism or offence under this Act,[39] assists, facilitates, organizes or directs the activities of persons or organizations engaged in an act of terrorism,[40] is an accessory to any act of terrorism or incites, promotes, or induces any other person by any means whatsoever to commit any act of terrorism[41] or any other offence referred to in this Act commits an offence and is liable on conviction to maximum of death sentence.

The Act, although not specifically made for cyber security is a handy tool in prosecuting an aspect of cybercrime dealing with cyber terrorism having made an all-encompassing provisions which may include but not limited to act of terrorism committed online or by the use of a computer network.

The Act vests the power of prosecution of offences on the following agencies: (a) the Nigerian Police Force, (b) the Economic and Financial Crimes Commission, (c) the Department of State Security Services. This may seem a welcome development especially in considering that the Government has zero tolerance for acts of terrorism. However, the number of agencies involved in prosecuting these offences are too many as this may lead to power tussle and duplication of functions in the prosecution of the offences under this law; this development will rather mar than make for achieving the modest intentions of the Act. A single well equipped agency can do the job.

4.8 The National Identity Management Commission Act

The National Identity Management Commission Act,[42] 2007 (hereinafter referred to as the NIMC Act) is an Act that repealed the National Civic Registration Act[43] and established a national database for the country and the National Identity Management Commission[44] as the statutory body charged with the responsibility of the database, the registration of individuals, issuance of general purpose identity cards among other things.

The objective of the Database as provided for in the Act is:

[37] Section 1 (c).
[38] Section 1 (d).
[39] Section 1 (e).
[40] Section 1 (f) .
[41] Section 1 (g).
[42] No. 23, 2007.
[43] CAP C 240, LFN 2004.
[44] Section 1 NIMC Act.

ISSN: 3064-8378

Public Policy and Administration Studies Journal

Research Article

to use fingerprints and other biometric information as unique and unambiguous features of identifying registerable persons,[45] enable the Commission using the information contained in the Database to issue a Multipurpose Identity Card with a unique Identification Number to registrable persons[46], enable the harmonization of existing identity card schemes in Nigeria[78], provide a medium for the identification, verification and authentication of citizens of Nigeria and other registerable persons entitled to the multipurpose identity cards

Facilitate the provision of a secured and reliable method of ascertaining, obtaining, maintaining and preserving information and facts about registerable persons in accordance with the provisions of the Act and whenever same is necessary or adjudged necessary in the public interest, provide such information to a designated and specified judicial or police authority[47],

Facilitate th provision of a convenient method for individuals who have been issued with the multipurpose Identity Card to provide proof of facts entered about themselves in the Database to other persons who reasonable requires such proof.[48] The Act provides for some transactions that the use of National Identity card is mandatory.[49] [50]And failure to furnish the information on such occasion is an offence under the Act.

The provision of the NIMC Act as enumerated above is a vital tool in fighting cybercrime relating to identity theft as it will ensure that information is provided about every Nigerian or non – Nigerian who is registrable, especially their finger prints. This will ensure that such registered persons can easily be if involved in crime. However, these cyber criminals are very smart and can go to any length at shielding their identity. Most times, these criminals knowing that they may be nabbed with the NIMC card may go the extra mile of going to the court to swear to an affidavit to the effect that they have lost the National Identity Cards to enable them perpetrate their evil deeds. Also, theft of identity is a watchword of these criminals. They may disguise themselves using modern photographic techniques to look different from who they really are.

4.9 The Cybercrimes (Prohibition, Prevention Etc) Act, 2015

The Nigerian Cybercrime Act, 2015 is a novel piece of legislation in that it is the first Nigerian Federal legislation specifically enacted to deal with crimes, commissions, omissions and threats faced in the digital world in this digital age[83]. The Cybercrime Act 2015 is an Act that provides for the Prohibition, Prevention, Detection and Prosecution of Cybercrime and other related matters in Nigeria. The Act is made up of 58 chapters and is divided

[45] Section 15 (a) NIMC Act.

[46] Section 15 (b). [78]
Section 15 (c).

[47] Section 15 (e).

[48] Section 15 (f).

[49] Section 27 (a-k).

[50] Controversial Aspects of the Nigerian Cybercrime Act 2015 Available on:. https://www.lawpadi.com.. acccessed October 23 2019.

ISSN: 3064-8378

Public Policy and Administration Studies Journal

Research Article

into eight parts. Part 1 provides for the objectives and application of the Act. Part 11 provides for the protection of Critical National Infrastructure. Part 111 provides for offences and penalties. Part 1V provides for duties of Service Providers. Part V provides for administration and enforcement. Part V1 provides for search, arrest and prosecution. Part V11 provides for jurisdiction and International Corporation and part V111 provides for miscellaneous. The Act provides for Cybercrime Advisory Council.

By virtue of section 1, the Act has the following objectives:

a. To provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria,[51]

b. Ensure the protection of critical national infrastructure[52]

c. Provide cyber security and protection of computer systems and networks, electronic communication, data and computer programs, intellectual property and privacy rights.[53]

The provisions of the Act are made to apply throughout the Federal Republic of Nigeria.[88] although the passage of the Act brought with it some innumerable gains to the Nigerian justice System, the Act is also bedeviled with some shortcomings. We humbly point out some of these shortcomings with a view of proposing a further and better development of the law.

The Act provides that:

The President may on the recommendation of the National Security Adviser, by order published in the Federal Gazette, designate certain computer systems, and or networks whether physical or virtual and or the computer programs, computer data and / or traffic data vital to this country that the incapacity or destruction of or interference with such system and assets would have a debilitating on the security, national or economic security, national public health and safety, or any combination of those matters as constituting Critical National Information Infrastructure.[54] The crime against such Critical National Infrastructure is punishable under section 5.[55] The Act goes further in the interpretation section to define Critical Infrastructure as systems and assets, which are so vital to the country that destruction of such systems and assets would have an impact on the security, national economic security, national public health and safety of the country;‖[56] The implication of this provision is that for a matter to be deemed as a Critical National Information Infrastructure, such matter shall be ―so vital‖ to the

[51] Section 1 (a) the Act.

[52] Section 1 (b).

[53] Section 1 (a-c). [88]
Section 2.

[54] Section 3.

[55] Cybercrime (Prohibition, Prevention, etc) Act, 2015.

[56] Section 58, the Act.

ISSN: 3064-8378

Public Policy and Administration Studies Journal

Research Article

circumstances and matters stated in the section.[57] The phrase ―so vital‖ is a subjective clause and this is a very dangerous situation especially as the Act makes no provision for checks and balances from the Executive. The President may designate a matter not so vital as ―so vital‖ or may overlook a matter ―so vital‖ without designating same as such.

Unauthorized access to a computer for fraudulent purpose and for obtaining data vital to national security is an offence punishable with a term of five years imprisonment or a fine of not more than N5, 000.000.00 (five million naira) or to both fine and imprisonment.[58] Where such offence is committed with the intent of securing access to classified information relating to commercial or industrial secret, the offence is punishable with imprisonment for a term not more than seven years or a fine of not more than five million naira or 7 years imprisonment or to both fine and imprisonment.[59] The Act in this section raises the issue of ―intent‖ to commit a crime. Intention to commit crime is a fact very difficult to prove. The position of the Evidence Act on facts bearing on question whether an act was accidental or intentional[60] could not be very useful in this circumstance considering the type of crime which this Act refers to. A smart cybercriminal may escape liability by showing that the crime he is being prosecuted for is not intended by him. Also the law enforcement agencies may not have the wherewithal to categorically pin the accused to the crime as it may be difficult to prove intention in cyber activities wherein punching a button may lead to various results. It would have been better if strict liability is prescribed for such offences.

Under the Act, connivance between a cyber-criminal and an owner of a cyber café to perpetrate an electronic fraud or online fraud using a cyber café is an offence. Where such connivance is proven, the owner of the cyber café shall be liable for an imprisonment for three years or a fine of N2,000,000.00 (two million naira) or both fine and imprisonment.[61] The burden of proving such connivance rests on the prosecutor.[62]

The writers are of the opinion that this burden of proof on the prosecution is an onerous task which may vitiate the smooth working of the core aim of this Act. There are instances where the prosecution is not computer literate. Even when they have some knowledge of the computer, they may not possess the enabling forensic knowledge to tackle the crime. In some other cases, the judge before whom the matter may be brought may not be literate on the workings of computer systems and the network to satisfy himself of connivance even when the prosecution is

[57] *Ibid.*

[58] Section 6 (1)

[59] Section 6(2)

[60] Section 12 Evidence Act.

[61] Section 7 (3) the Act.

[62] Section 7 (4) .

ISSN: 3064-8378

Public Policy and Administration Studies Journal

Research Article

striving to prove its case. This situation may create a soft landing for the cyber café owners to escape liability. The liability in this instance ought to be strict so as to deter intending offenders.

Under the Act, the relationship between financial institutions and their customers is such that where there is a fraud affecting a customer, the onus of proving negligence on the part of the financial institution rest on the affected customer once the financial institutions shows that they put in place, counter fraud measures to safeguard their information.[63]

Sometimes, the burden of proof appears to rest on the computers and systems through which these acts of cybercrime are committed since the bank has done all that is required of it to ensure that occurrence of fraud is ruled out. This could seem so in the instance of an Automated Teller Machine (ATM) and Point Of Service Machines (POS) which are operated and accessed at any time of the day including weekends and public holidays within and outside the bank, in the absence of the affected bank and its staff as the case may be. One may conclude that the bank should not be held responsible for any crime committed in the process of using these computer systems by a customer especially when the bank or her staff is not present and the bank management has placed all counter fraud measures in place.

This line of argument may appear credible on the face of it. However, it is worthy of note that a machine and or a computer is a programmed system which displays or functions according to an instruction or command. Again, in other civilized countries where banking systems are computerized, banking programmes are frequently checked to detect interference or attack and when such is detected, it is blocked and the existing programme changed immediately. Also, computers in such civilized nations are programmed to detect foreign bodies and interference. This is to ensure that perpetrators of cybercrime do not have their way into customers' accounts and is for any reason it happens, then it is detected on time before greater harm is done.

Allowing the banks to escape liability once it is proven that all counter fraud measures are put in place without more could be an onerous one on the customer who may not have the requisite technological expertise or the financial power to engage an expert to prove that the financial institution is actually negligent even when it is clear that it is negligent. The writers are of the opinion that the Act would be better if there is strict liability on the part of the financial institutions since they are the custodians of this leaked information. They should be made to prove that they are actually not liable.

5. The Institutional Framework for the Control of Cybercrimes in Nigeria.

The following are some of the institutions and agencies charged with enforcing, investigating and prosecuting offences relating to cybercrime in Nigeria.

5.1 Special Control Unit against Money Laundering (SCUML)

[63] Section 19, the Act.

ISSN: 3064-8378

Public Policy and Administration Studies Journal

Research Article

The Special Control Unit against Money Laundering (SCUML) was established by the Federal Ministry of Industry, Trade and Investment to work closely with the Economic and Financial Crimes Commission (EFCC) in the battle against money laundering.[64] This is in a bid to ensure that financial crimes in cyber space are curtailed.[65] The SCUML is domiciled in the Federal Ministry of Commerce and Industry. The Money Laundering Act which this Unit seek to administer made provisions for Financial Institutions and Designated Non Financial Institutions.[66] These include businesses such as dealers in jewelry, cars and luxury goods, chattered accountants, audit firms, tax consultant etc.[67] The Minister for Commerce and Industry is charged to make regulations in respect of and to govern some businesses and professions known as the Designated Non Financial Businesses and Professions to protect the sector against any form of money laundering and combating the finance of terrorism.[68] To this end, the minister can make regulations to include or remove a particular trade, business or profession from the Designated Non Financial Businesses and Professions, DNFBPs. The Money Laundering Act includes the legal profession as a trade in the list of Designated Non Financial Institutions. As a result of this, the Unit will be at liberty to request for information from owners of law firm to check money laundering and financing of terrorism. This led to some court cases such as the case of the Registered Trustees of the Nigerian Bar Association v. the Attorney General of the Federation & the Central Bank of
Nigeria.[69]

The NBA relied heavily on the provisions of section 192 Evidence Act 2011 which forbids and prohibits legal practitioner from divulging to any party, the secret of transaction or communication between them and their clients. The prayers were granted as prayed.

The SCUML has the mandate to supervise, monitor and regulate the activities of all Designated Non Financial Institutions (DNFIs)[70] in consonance with the country's Anti-Money Laundering and Combating of Financing of Terrorism regime.[71] Its mandate is statutory in nature.[72] The SCUML as an agency of the federal government is established for the sole purpose of combating money and financial crimes in the cyber space. The Unit is not

[64] Timothy, G. Special Control Unit Against Money Laundering: Powers and Limitations. Available on: https://www.britishcouncil.org.ng accessed November 11 2019.

[65] Dzever, *Op. Cit.* 59.

[66] Section 3 Money Laundering Act.

[67] Section 25 Money Laundering Act.

[68] Section 5 (4) .

[69] Suit No. FHC/ABJ/CS/173/2013. In the originating summons dated the 15th day of March, 2013, the NBA, inter alia asked the court to declare that the provision of section 5 of the MLPA in so far as it purport to apply to legal practitioners is invalid, null and void.

[70] Section 25 MLPA, 2011 (as amended).

[71] Timothy, *Op. Cit.*.

[72] *Ibid.*

ISSN: 3064-8378

Public Policy and Administration Studies Journal

Research Article

without some shortcomings especially with that relating to the Unit's powers of demanding information from DNFIs. The MLA provides that: the Commission, Agency, Central Bank of Nigeria or other regulatory authorities pursuant to order of a

Federal High Court obtained upon an ex parte application supported by a sworn declaration made by chairman of the Commission or an authorized officer of the Central Bank of Nigeria or other regulatory authorities justifying the request, may in order to identify and locate proceeds, properties, objects or other things related to the commission of an offence under this Act, the Economic and Financial Crimes Commission (Establishment) Act or any other law,[73] place any bank account or any other account comparable to a bank account under surveillance;[74]Obtain access into any suspected computer system,[75] Obtain Communication of any authentic instrument or private contract, together with all bank, financial and commercial records when the account, the telephone line or computer system is used by any person suspected of taking part in a transaction involving a financial or other crime.[76]

This implies that the SCUML cannot obtain information or access into a DNFIs financial or bank accounts, telephone line and records on its own without first applying to the Federal High Court judge.

5.2 The Nigerian Cybercrime Working Group (NCWG)

The Nigerian Cybercrime Working Group was set up by the Nigerian Federal Government in 2004 in a bid to realize the objectives of the National Cyber security Initiative (NCI).[77] The NCWG was set up to enhance public enlightenment of the Nigerian population on the nature and danger of cybercrime, criminalization through new legislation of all online vices, establishment of legal and technical framework to secure computer systems and networks and protection of critical national infrastructure for the country.[78] The Group was created to deliberate on and propose ways of tackling the malaise of internet fraud in Nigeria.[79] The Nigerian Cybercrime Working Group came up with a draft Cyber crime Bill which later gave birth to the Nigerian Cyber Crime (Prohibition, Prevention, etc) Act, 2015.

5.3 The Nigerian Financial Intelligence Unit (NFIU)

[73] Section 13 Money Laundering Act.

[74] Section 13 (a).

[75] Section 13(b).

[76] Section 23 (c).

[77] Maka, M. Building National Cybersecurity Capacity in Nigeria: The Journey So Far. (2009) Regional Cybersecurity Forum for Africa and Arab States.

[78] *Ibid.*

[79] *Ibid.*

ISSN: 3064-8378

Public Policy and Administration Studies Journal

Research Article

The EFCC by virtue of the powers conferred on it under the Act has many departments and sectors. One of the departments is the Nigerian Financial Intelligence Unit (NFIU): This is an operative unit of the EFCC and was established under the EFCC Act 2004,[80] and Money Laundering (Prohibition) Act, 2004 as amended.[81]

The rationale behind the establishment of the NFIU is to safeguard the Nigerian Financial system and contribute to the global fight against money laundering, terrorism financing and related crimes through the provision of credible financial intelligence[82]as one of the requirements of the Egmont Group[83]. The Unit complements EFCC's Directorate of Investigation but does not carry out its investigation.[84]

The Unit's central purpose is to receive and analyze financial disclosures relating to currency transactions report and suspicious transaction. All financial institutions and designated non-financial institutions are required by law to furnish the NFIU with details of their financial transactions.[85] The NFIU is operationally autonomous and independent in carrying out its core and distinct functions and are free from any undue political, government or industry influence or interference which might compromise its operational independence.[121] accordingly, the NFIU is the Nigerian arm of the global financial intelligence Units in Nigeria. It is domiciled with the EFCC as an autonomous unit operating in the African region.[86] The establishment of the NFIU is in tandem with the requirement of the Financial Action Task Force (FATF) standards and Article 14 of United Nations Convention against corruption (UNCAC).[87] Since its establishment, the NFIU has sought to develop standards and procedures for the receipt, analysis and dissemination of financial intelligence to law enforcement agencies, perform on-site and off-site examination of financial institutions, enhance compliance with the legal and regulatory regimes on Anti-Money Laundering and combating the financing of Terrorism (AML/CFT) in Nigeria as well as respond to the Global trends by collaborating with other FIUs worldwide.[124]

In discharging its function, the NFIU works directly and closely with the following as reporting institutions the Central Bank of Nigeria, (CBN), the National Insurance Commission (NAICOM), Securities and Exchange

---

[80] Section 1 (2)(c), EFCC Act.

[81] Saulawa, M. Marshall, J. Cyberterrorism: A Comparative Legal Perspective (2015) Vol. 33 Journal of Law, Policy and Globalization at 5.

[82] Sekav,*op.cit.*

[83] The EGMONT Group of Financial Intelligence Units began in 1995 as a small group of national entities today referred to as financial intelligence Units (FIUs).

[84] Chawki *Op. Cit.* 65.

[85] Tomilehun, B. An Appraisal of the Legal Framework of Cybercrime in Nigeria Available on: https://www.info@clrwc.com. accessed on October 14 2019. [121]
Sekav, *Op. cit.*

[86] *Ibid.*

[87] *Ibid.* [124]
Ibid.

Commission (SEC) and the Special Control Unit against Money Laundering (SCUML). in receiving the following reports:

NFIU was created solely to guard against suspicious financial and monetary transactions and ensure that all transactions (financial) meet with the international best practices on the fight against financial crime. This understandably is in the bid to ensure that persons especially politicians do not indulge in the habit of laundering the nation's currency to outside countries which practice may lead to economic recession in the country.

However, the agency is not without some shortcomings. One of such is that the NFIU is faced with a plethora of reporting authorities. The writers are of the opinion that all these bodies are too many. A single and well equipped reporting authority can do the job to avoid duplication of functions.

Another challenge facing the unit is that the NFIU does not have full autonomy. Presently, NFIU as a body is domiciled with the Economic and Financial Crimes Commission (EFCC) unlike its counterparts in other countries such as the United Kingdom,[88] and the United States.[89] This is the reason for suspending the NFIU from the Egmont[90] group until a full autonomy is granted. The core functions of a Financial Intelligence Unit (FIU) call for professionalism and objectivity in decision making, the timely processing of information, dissemination to appropriate authorities and strict protection of confidential data.[91] This may not be achieved if the NFIU is placed under the EFCC.

6. The Budapest Convention and Cybercrime Laws in Other Jurisdictions

In the preceding paragraphs, the legal regime and institutional framework governing cybercrime and cyber security in Nigeria were appraised and the inadequacies of these laws were highlighted.. Consequent upon this, it will be necessary to examine some of these laws by way of comparative analysis vis-a-viz the Nigerian laws. Also, the Budapest Convention, an international instrument aimed at combating some forms of crimes committed at the international scene by the instrumentality of the computer network will be examined. The Budapest Convention and Cybercrime laws in some selected jurisdictions of the United States of America and Canada will be examined and compared with the Nigerian position.

6.1 The Budapest Convention on the Control of Cybercrime

[88] Where the Financial Intelligence Unit (FIU) is headed by the Assistant Director in National Crime Agency.The Assistant Director reports to the Deputy Director, Economic Crimes Command.

[89] Where the FIU is placed in the United States Department of Treasury.

[90] The Egmont Group of Financial Intelligence is an informal network of 156 Financial Intelligence Unit.

[91] Yakubu, U. The Unending Battle for the Nigerian Intelligence Unit. Available on: https://www.opinion.premiumtimesng.com> accessed October 31 2019.

ISSN: 3064-8378

Public Policy and Administration Studies Journal

Research Article

The Convention on Cybercrime also known as the Budapest Convention[92] on Cybercrime or the Budapest Convention is the first international treaty seeking to address internet and computer crime by harmonizing national and regional laws, improving investigative technique and increasing cooperation among nations.

The Budapest Convention is the first and the only existing Global Convention on cybercrime today. The Convention was drawn up by the Council of Europe in Strasbourg, France with the active participation of the Council of Europe's observer states i.e that is Canada, Japan, South Africa and the United States[93]. The Convention was signed on the 23rd of November, 2001 in Budapest and became effective from the 1st day of July, 2004. At present, the number of signatories stands at 56.[131] An additional Protocol to the Convention was made on the 1st day of March, 2006. The Budapest Convention is a widely recognized decisive document on international best practice in combating cybercrime and enjoins even non signatory States to comply with its provisions.[94]

According to the preamble to the convention, its main objective is to pursue a common criminal policy aimed at protection of the global society against cybercrime, especially by adopting legislation and fostering international cooperation.[95] The Convention comprises of four main chapters with several articles. The first chapter takes care of definition of terms normally used in cyber world, cyber space and cyber technology. Chapter two deals with the substantive crimes and legislations a ratifying country is expected to adopt in order to combat cyber crimes. Chapter three provides for mutual prosecution of cybercrimes as well as extradition rules, treaty reciprocation obligations among the ratifying countries. Chapter four takes care of the final clauses and articles pertaining to the signing of the Convention, territorial application of the Convention, declarations, amendments, withdrawals, and federalism. The Budapest Convention provides for the offences related to the illegal access or access to a computer system without right or authorisation.[134] Illegal access covers the basic offence of dangerous threats and attacks against the security of computer systems and data. The cybercrime offences of illegal access are likened to hacking, one of the oldest computer-related crimes which involves operations that exploit computer systems in ways that are unusual, illegal and without the consent or authorisation of the owner.[96]

Some commendable features of the Budapest Convention are as follows:

---

[92] Budapest Convention on Cybercrime. Available on: https://www.coe.int accessed October 30 2019.

[93] *Ibid.* [131]

Ibid.

[94] Shalini, S. Budapest Convention on Cybercrime: an Overview Available on: https://ccgnludelhi.word press.com accessed October 20 2019.

[95] Budapest Convention on Cybercrime. Available on: https://www.coe.int accessed October 27 2019 [134] Article 2 of Budapest Convention.

[96] Online-Community Hacker Watch, available at : http://www.hackerwatch.org/about/ accessed October 12 2019.

ISSN: 3064-8378

Public Policy and Administration Studies Journal

Research Article

i. The Convention is aimed at providing a unified and a common criminal policy aimed at protection of the global society against cybercrime. This feature, the convention shares with the Nigerian Cybercrime Act, 2015. The Cybercrime Act of Nigeria serves as a unified instrument for all States in Nigeria in the fight against cyber crime.

ii. The Convention is a global best practice measures towards the fight against cybercrime. iii. It serves as a guideline after which nations can carve their cybercrime laws. iv. The convention is flexible in nature, allowing rooms for more and future protocols.

v. The convention makes room for extradition among signatory countries. This feature is also present in the Nigerian Cybercrime Act, 2015. However, the Cybercrime Act of Nigeria failed to take into consideration the rules of extradition and the need for a mutual bilateral agreement between States before the extradition process can take place.

vi. The Convention also makes room for public/private co-operation in the fight against cybercrime. This feature is provided for in the Nigerian Cybercrime Act, 2015; however, it has never been tested or implemented. For example, it has been suggested that for a better and smooth implementation of the Nigerian Cybercrime Act, 2015, there is a need for a public-private partnership and corporation.[97]

6.2 Cybercrime Laws in the United States of America

Cybercrime is a top concern of the American Legal community. Despite greater consumer awareness and advanced counter measures, cybercrime statistics continue to rise in the United States.[98]Thirty years ago, law enforcement agencies faced the emerging threat of cybercrime without the aid of any criminal statutes designed to deal with it. Wire fraud and mail fraud laws were employed where possible but were often a poor fit for the conduct of the issue.[138] The Congress enacted a statute known as the 18 U.S.C 1030. The subsequent Congressional deliberations on the law culminated into passing of the Computer Fraud and Abuse Act 1986. The Computer Misuse Act used to be the major item of the Federal Legislation dealing with computer crime in the United States. The Act criminalises various conducts relating to the use of computers in criminal behaviour, including conduct relating to the obtaining and communicating of restricted information; unauthorized accessing of information from financial institutions, United States government, and ―protected computers‖; unauthorized

[97] B Udotai Esq. Technology Times Outlokk, Lagos, August 21 2015.

[98] A.Kelly Cybercrime www.aaronkenkellylaw.com>cybercrime-la... accessed October 12 2019. [138] Winmill, BL. Cybercrime: Issues and Challenges in the United States (2010) Vol. 7 Digital Evidence and Electronic Signature Law Review, 24.

ISSN: 3064-8378

Public Policy and Administration Studies Journal

Research Article

accessing of a government computer; fraud; damaging of a protected computer resulting in certain types of specified harm; trafficking in passwords; and extortionate threats to cause damage to a ―protected computer‖[99]. Presently, the United States Justice Department prosecutes computer crimes or cybercrime under different U.S Federal laws.[100] [101]

The second legislation is the Wiretap Act also known as Title 111. This deals with the use of wiretaps while investigating crime and prohibits any person including a law enforcement officer from making an illegal interception or disclosing or using illegally intercepted material. It covers three different offences:

a. Intercepting communications.
b. Disclosing an intercepted communication.
c. Using an intercepted communication.

A violation of any of the provisions of the Wiretap Act is a class D felony[102] and attracts a term of imprisonment not more than 5 years and a fine not more than $250 for individual and $500,000 for an organization unless there is a substantial loss. Though the punishment under this section may look paltry, it is adequate enough to checkmate the activities of law enforcement agencies towards ensuring that they do not exceed their power in intercepting information. There is no provision in the Cybercrime (Prohibition, Prevention, etc) Act, 2015 dealing with liability of law enforcement agents in excess use of their powers to intercept suspicious traffic data information as provided for under section 39(2) of the Act.

The third federal legislation of the United States on cybercrime is known as the Other Network Crime Statutes which provides for penalties for offences such as:

a. Unlawful access to stored communications[143].
b. Identity theft.[144]
c. Aggravated Identity theft.[145]
d. Access Device Fraud.[103]
e. CAN-SPAM [104]

---

[99] Ibekwe, C. The Legal Aspect of Cybercrime in Nigeria: An Analysis with the UK Provisions (Unpublished thesis work), July 2015, at 40.

[100] John F. A Guide to Cyber Crime Laws . Available on: https://www.quora.com>what-are-the-c... accessed October 12 2019.

[101] U.S.C Sec. 2511.

[102] A class D felony is the least serious grouping of felonies. Class D felonies are generally not associated with being violent or dangerous as they usually do not involve victims. However, because it is still a felony, it is still associated with all the penalties of a felony. Available on: https://www.legalmatch.com>article>cl... accessed October 12 2019. [143] 18 U.S.C Sec. 2701. [144] Sec. 1028.

[103] Sec. 1029.

[104] Sec. 1037. [148]
Sec. 1343.

ISSN: 3064-8378

Public Policy and Administration Studies Journal

Research Article

f. Wire Fraud.

The United States Government in an effort to strengthen its cyber security has introduced some new Federal legislations and also amended some older ones.[105] These are :

i. The Cyber security Enhancement Act, 2014: this law provides an ongoing public-private partnership to improve cyber security and strengthen cyber security research and development, etc. ii. The Cyber security Information Sharing Act (CISA) 2015. The objective of CISA is to improve cyber security in the United States through enhanced sharing of information about cyber security threats, and for other purposes. The Act allows the sharing of internet traffic information between the United States Government and Technology manufacturing companies.

iii. The Federal Exchange Data Breach Notification Act, 2015. This Act requires a health insurance Exchange to notify each individual whose personal information is known to have been acquired or accessed as a result of a breach of security of any system maintained by the exchange as soon as possible but not later than 60 days after the discovery of the breach.

iv. The Nation Cyber Security Protection Advancement Act, 2015. This law amends the Homeland Security Act, 2002 and introduced a provision to enable the Department of Homeland Securities (DHS's) national cyber security and Communication Integration Centre (NCCIC) to include tribal governments, information sharing and analysis centres and private entities among its non-federal representatives.

Some States in the United States have also taken steps to enact decisive cyber security laws to ensure their law enforcement agencies are better equipped at fighting cybercrimes. For instance, in 2003, the State of California passed a law known as the ―Notice of Security Breach Act‖ which requires that any company that maintain personal information of citizens and has a security breach must disclose the details of the event leading to the breach. This is a welcome development in the United States. The Nigerian State should emulate same.

6.3 Cybercrime Laws in Canada

Like her contemporaries, Canada is not immune from the acts of cybercrime. Canada has different laws dealing with different forms of cybercrime. The government of Canada is committed to protecting Canadians against cybercrime. Many Canadian government departments including the Department of Justice, the Royal Canadian Mounted Police (RCMP), Public Safety Canada and Global affairs Canada work together to protect Canadians against cybercrime.[106] Partnerships have also been developed between international, federal and provincial law enforcement agencies. For example, there is a Canadian Anti-Fraud Centre, a joint effort of the RCMP, the

[105] A Glance at the United States Cyber Security Laws. Available on: https://www.linkedin.com>pulse>glance... ... accessed October 14 2019.

[106] Cybercrime: Global Affairs Canada / Affairs Mondiales Canada. Available on: https//www.international.

.gc.ca>crime>cyber… accessed October 14 2019.

ISSN: 3064-8378

Public Policy and Administration Studies Journal

Research Article

Ontario Provincial Police (OPP) and the Competition Bureau of Canada to combat internet and mass marketing fraud.[107]

On October 3, 2010, the Federal Government of Canada launched the Canadian Cyber Security Strategy. The strategy is geared towards protecting individuals, industries and government from cyber threats.

On March, 10 2015, the Protecting Canadians from Online Crime Act was enacted. This Act empowers the law enforcement agencies to take action against exploitation of children and organized crime via the internet. The enactment of this Act necessitates the amendment of some key Canadian legislation such as the Criminal Code Act of Canada which among other things was amended to include the power of a law enforcement agency to make preservation demands and orders to compel the preservation of electronic evidence; the Canadian Evidence Act, the Competition Act, the Mutual Legal Assistance in Criminal Matters Act.

There is also a forum known as the Global Affairs Canada which coordinates and ensures active participation in international initiatives to combat cybercrime. This forum funds capacity building initiatives to help other countries in better protecting themselves and the internet from criminality that easily transcends borders and often threaten Canadians from abroad.

Canada has ratified and is a strong supporter of the Budapest Convention.

Looking at the Canadian's law on cybercrime and the Nigerian Cybercrime Act, there is lot to be emulated. Canada not only has many specific laws in different areas of cyber security, the Canadian government also forms public and private partnership in fighting cybercrime.

7 Lessons for Nigeria

Generally, Nigeria is not faring too poorly in the area of cyber security and the fight against cybercrime. Nigeria has been ranked the 15th in Information Communication Technology development in Africa and 143rd globally among 176 countries[108].

To achieve the desired end and restore Nigeria's cyberspace to the full cyber security, there are a lot of lessons to be learnt from the the Budapest Convention and cybercrime laws in the jurisdictions examined above. Some of the lessons are as follows:

a. The Budapest Convention is the international convention for controlling cybercrimes in the cyberspace. Ratifying and domesticating the provisions of the Budapest convention will not only aid Nigeria in amending her cybercrime laws to the World's best standard. This will enable the country to fight cybercrime not only at the local level but also at the international scene.

---

[107] *Ibid.* [152]
Ibid.

[108] Cybersecurity: Understanding the Threat, Landscape and Lessons From the GDPR For Nigerian Entities. Available on: https://www.lexology .com>library>detail. accessed November 23 2019.

ISSN: 3064-8378

Public Policy and Administration Studies Journal

Research Article

b. In the United States and Canada, there are many federal legislations geared towards achieving cyber security and eradicating cyber crime. In the United States, they are laws such as the Wiretap Act, Computer Fraud and Abuse Act, Other Network Crime Statutes, etcetera. This is a welcome development as the concerned agency will always be equipped with a handy legislation in any form of cybercrime. As such, there is need to enact other federal legislations on cyber security in Nigeria in addition to the Cybercrime Act, 2015.

c. In the United States, the different federating States have their cybercrime laws and are enjoined to apply the provision of these laws towards cyber security in their domain. In Nigeria, it will be apt if the different States are enjoined to make their own individual cybercrime laws. Combating cybercrime should not be the sole responsibility of the federal government but should be decentralised.

d. In Canada, there are many government departments charged with the control of cybercrime. Nigeria should learn from this. Also strategies should be earmarked, forums should also be created to educate people on the need to fight cybercrime collectively both at the public and private sector.

e. The Nigerian Police should be trained and well equipped with what is needed to fight cybercrime.

8. Conclusion

Strict liability should be imposed on financial institutions to prove that they are not negligent when a cyber-criminal becomes privy of a customer's information in their possession despite their having put up counter fraud measures. There is a need to amend both the Criminal Code and the Penal Code to be in ttune with the modern day realities and technology. The NFIU should also be given full autonomy, separate from the EFCC. This will go a long way to ensure that the NFIU regains its position in the Egmont Group. The Unit should also receive direct funding from the nation's yearly budget. Different States of the federation should also create their own laws of cyber security just as it obtains in the United States. The Nigerian government should strive to create more jobs and employment for the teeming Nigerian youths. This will go a long way in curbing acts of cybercrime in the polity.

References

A Glance at the United States Cyber Security Laws. Available on: https://www.linkedin.com>pulse>glance... ... accessed October 14 2019. .

A. Kelly Cybercrime www.aaronkenkellylaw.com>cybercrime-la... accessed October 12 2019.

Adejoke, O. The ICT Revolution and Commercial Sectors in Nigeria: Impacts and Legal Interventions British Journal of Arts and Social Sciences, (British Journal Publishing Inc; 2012), Vol.5 at No.2 at 54.

Ani ,L. Cybercrime and National Security, the Role of the Penal and Procdural Laws in Azinge, E, SAN, et al (eds), Law and Security in Nigeria, (Nigerian Institute of Advanced Legal Studies Press, 2011)197-234.

Udotai Esq. Technology Times Outlokk, Lagos, August 21 2015.

Babafemi ,T. An Appraisal of the Legal Framework of Cybercrime In Nigeria. Available on: clrwc.com>anappraisalof-thelegal-fra… accessed October 23 2019.

Budapest Convention on Cybercrime. Available on: https://www.coe.int accessed October 27 2019

Chawki, M. Nigeria Tackles Advanced Fee Fraud. (2009), Vol. 1 Journal of Information, Law and Technology at .8.

Chido, O. The Money Laundering Act and its Discontents. Available on: https://www.thisdayonline.com>2016/02/15>mon... accessed November 5 2019.

Clay, W. Botnets, Cybercrime and Cyberterrorism: Vulnerabilities and Policy Issues for Congress (CRS Report for Congress 2007)7.

Cyber Crime Law Available on: www.britannica.com>topic>cybercrime. accessed December 5 2019.

Cybercrime: Global Affairs Canada / Affairs Mondiales Canada. Available on: https//www.international. .gc.ca>crime>cyber… accessed October 14 2019.

Cybersecurity: Understanding the Threat, Landscape and Lessons From the GDPR For Nigerian Entities.‖ https://www.lexology .com>library>detail.. … accessed October 26 2019

Dhawesh, P. Cyber Crime and the Law Available on: www.legalindia.com>cyber-crimes-and-... accessed October 17 2019.

Daramola, A. Nigeria Losses N127b Annually to Cyber Crime. Available on; https://www.dailypost.ng. . accessed October 29 2019.

Dzever, S An Appraisal of the Legal Framework for Combating Cybercrime in International Law. (2011), unpublished thesis at 94.

Gbenga, S ; Babatope S; and Bankole O. A Report for the Cyber Stewards Network Project of the Citizen Library, Munk School of Global Affairs, University of Toronto at 11.

Hudson, A. The Fight Against Cyber Crime Available on: www.legalindia.com>cyber-crimes-and-... accessed October 23 2019.

Ibrahim, A. An Appraisal of the Legal and Administrative Framework for Combating Terrorist Financing (2013) Vol. 19 Journal of Law, Policy and Globalization, at 32.

Ibekwe, C. The Legal Aspect of Cybercrime in Nigeria: An Analysis with the UK Provisions (Unpublished thesis work), July 2015, at 40.

Ibrahim, A; Miriam, M. Cybercrime (Prohibition, Prevention Etc) Act,2015: Issues and Challenges in Nigeria. (Draft Paper Presented at the 49th Annual Nigerian Law Teachers' Conference at Nasarawa State University, Keffi on behalf of Usman Danfodio University Sokoto, 22nd -27th May, 2016) pg. 15-16.

John F. A Guide to Cyber Crime Laws . Available on: https://www.quora.com>what-are-the-c... accessed October 12 2019.

Johnson, O. Automated Teller Machiune (ATM) Frauds in Nigeria: The Way Out. (2011),UNILJ, Vol 5 at

Maka, M. Building National Cybersecurity Capacity in Nigeria: The Journey So Far. (2009) Regional Cybersecurity Forum for Africa and Arab States.

Michael, Aaron, Dennis, ―Cybercrime Definition, Statistics and Examples.‖ Available on: https://www.britanicacom>topics>cyber... accessed accessed October 21 2019.

Mrabure KO. Lack of Centralized Data Base as an Impediment in Curtailing Cyber Crimes in Nigeria in Eboibi FE (ed) Handbook on Nigerian CyberCrime Law Justice Jenco Printing and Publishing Global, 2018, Nigeria at 498-499.

Munguno, B. (rtd), during the inauguration of the Cyber Crime Advisory Council in Abuja. (Thisday Newspaper of April 19, 2016)15.

Okonoigne, R; Adekanle, R. Cybercrime in Nigeria available on: www.saycocorporativo.com/saycoUK/BIJ/jOURNAL/Vol.13 No.1/Article_7. accessed October 30 2019.

Online-Community Hacker Watch, available at : http://www.hackerwatch.org/about/ accessed October 12 2019. Oriole, T. Advanced Fee Fraud on the Internet (2005) Vol. 21 Computer Law and Security Report at 241.

Pahuja, D. Cyber Crime and the Law. Available on: www.legalindia.com>cyber-crimes-and-..accessed December 5 2019.

Sackson, M., Computer Ethics: Are Students Concerned? First Annual Ethics Conference,1996.

Saulawa, M. Marshall, J. Cyberterrorism: A Comparative Legal Perspective (2015) Vol. 33 Journal of Law, Policy and Globalization at 5.

Sekav, S. An Appraisal of the Legal Framework for Combating Cybercrime in International Law (Masters Dissertation, School of Postgraduste Studies, Ahmadu Bello University, Zaria, May, 2016), chapter three.

Shalini, S. Budapest Convention on Cybercrime: an Overview Available on: https://ccgnludelhi.word press.com accessed October 20 2019.

Timothy, G. Special Control Unit Against Money Laundering: Powers and Limitations. Available on: https://www.britishcouncil.org.ng accessed November 11 2019.

Tomilehun, B. An Appraisal of the Legal Framework of Cybercrime in Nigeria. Available on: https://www.info@clrwc.com. accessed on October 8 2019. 5 Controversial Aspects of the Nigerian Cybercrime Act 2015 Available on:. https://www.lawpadi.com.. acccessed October 23 2019.

Winmill, BL. Cybercrime: Issues and Challenges in the United States (2010) Vol. 7 Digital Evidence and Electronic Signature Law Review, 24.

Yakubu, U. The Unending Battle for the Nigerian Intelligence Unit." Available on: https://www.opinion.premiumtimesng.com> accessed October 31 2019.